PLN-i09-OSS

(I)SN09 OSS Guide

Advance Feature Guide

(I)SN09 Standard 01.04 January 2006

NORTEL NETWORKS

How the world shares ideas.

(I)SN09 OSS Guide

Advance Feature Guide

Publication number: PLN-i09-OSS
Product release: (I)SN09
Document release: Standard 01.04
Date: January 2006

Publication History

January 2006

Re-release of the Standard version of this document for (I)SN09 at FVS. The document covers ATM solutions, IP solutions (Chapters 1-3), and International features (Chapter 4). The following features have been added since the previousStandard release because they were not previously identified by content primes as OSS-impacting:

- A00009515--Out-of-Band interop with MCS
- A00011740--Packet Cable Multimedia for CS2K

The following feature has been deferred to a later release, so it has been removed from this version of the document: A00009610, IEMS Calix Integration.

September 2005

Re-release of the Standard version of this document for (I)SN09 at FCS. The document covers ATM solutions, IP solutions (Chapters 1-3), and International features (Chapter 4). The following features have been added since the initial Standard release because they were not previously identified by content primes as OSS-impacting:

- A89007819--QoS Reporting: QoS Collector Application (QCA)
- A00007269--NGSS Backup and Restore
- A00008090 -- SBA: Alternate Scheduled Closure of Billing Files
- A00008724 -- OMDD Enhancements and Robustness
- A00009129-- Controlled Hot SWACT
- A00009153-- H.323 RLT Development
- A00009207 -- DPT Trunk Testing Support

- A00009332 -- P-Time and Codec Negotiation Selection Policy
- A00009364 -- CICM End-of-Call QoS Reporting
- A00009375 & 9376 -- CICM Third-party Corrective Content Patching & CICM Selective Binary Component Patching
- A00009514 -- CS2K-MCS Interop for SN09
- A00009520 -- Trunk blocking tools for MG4K and GWC on SN09
- A00009530 -- H248 and xUA NAT traversal for CPE Gateways
- A00009839 -- Ability to apply patches during ESUP upgrade
- A00009840 -- CBM IPSec Northbound Interface
- A00012001 -- IEMS Call Server 2000 SIP Integration
- A00012210 -- Geo OA&M Automatic Backup and Accelerated Restore

June 2005

Standard release of this document for (I)SN09. The document covers ATM solutions, IP solutions (Chapters 1-3), and International features (Chapter 4). The following features have been added since the Preliminary release:

- A00008629 -- GEM-II AAL2 IW-SPM SN09 Core Preparation Work
- A00009028 -- PHX SIP Lines OAM Support
- A00009043 -- PHX SIP Lines Provisioning Support
- A00009036 -- Table HOMELRN Option SITE Expansion
- A00009190 -- Universal Carrier Protocol (UCP) C7UPTMR Enhancements
- A00009235 -- TLS for SIP
- A00009292 -- IEMS: UserID-based Partitioning by NE
- A00009353 -- GWCUnit Availability/ Health Monitoring
- A00011167 -- MG9KEM Central Userid and Password Support
- A00011746 --Addition of LGRP_TYPE field to GW profiles (Corrective)

The following features have been removed from this document because they have been deferred to release SN09.1

- A00007269 -- NGSS Backup and Restore
- A00009530 -- H248 & xUA NAT Traversal for CPE Gateways

April 2005

Preliminary release of this document for (I)SN09. The document now covers ATM solutions, IP solutions (Chapters 1-3), and International features Chapter 4). The following sections are updated for this release:

- Mapping tables (ACTID-to-solutions; ACTID-to-OAM&P impacts). Two new reference lists have been added:
  - Features for IP solutions
  - Features for ATM solutions
- New or changed per release for both IP and ATM features
- IEMS Functionality for (I)SN09
- Feature descriptions by product/network element for both IP and ATM features
- International Features information, including the following:
  - Mapping tables (ACTID-to-solutions; ACTID-to-OAM&P impacts). Anew reference list has been added: International Features List, which shows both International-only features as well as features that apply to the International and North American markets
  - New and changed for ISN09
  - ISN09 Feature descriptions for CS2K International and World Trade
- Baseline information for Logs/Faults
- Baseline information for OMs/PMs
- Appendices

Table of Contents

Appendices for Logs/Faults and OMs/PMs

Appendix J: MCS Operational Measurements

About this document

When to use this document

This document supports the (I)SN09 release of Carrier VoIP Solutions. It provides (I)SN09 design documents that contain Operations Support Systems (OSS) information. It also provides information on what is new and changed in (I)SN09, related to the following areas:

- Logs/faults
- Data schema tables/MIBs
- Commands/User Interface
- Service Orders
- Office Parameters
- Operational/performance measurements (OMs/PMs)
- AMA/billing
- Software optionality control (SOC)

In addition, it provides a baseline of the Logs/Alarms and Operational Measurements (OMs)/Performance Measurements (PMs) that are available in Carrier VoIP, organized by network element.

Information in this document is believed to be accurate at the time of publication, but it is subject to change. Use of this document should be restricted to resource planning and estimating for (I)SN09. **Do not use this document to make changes to existing software.**

How this document is organized

This document is divided into the following sections:

- Mapping tables and Feature Lists
  - — Mapping network elements to ACTIDs to solutions
  - — Mapping network elements to ACTIDs to OAM&P documentation elements
  - — Features for IP solutions
  - — Features for ATM solutions
- New/changed information for (I)SN09
  - — Logs and faults
  - — Data Schema/MIBs
  - — Commands/User Interface
  - — Service Order
  - — Office Parameters
  - — Operational Measurements/Performance Measurements
  - — AMA/Billing
  - — Software Optionality Control (SOC)
- (I)SN09 features for IP and ATM solutions, organized by network element
- ISN09 International features information, including the following:
  - — Mapping tables (ACTID-to-solutions; ACTID-to-OAM&P impacts). Anew reference list has been added: International Features List, which shows both International-only features as well as features that apply to the International and North American markets.
  - — New and changed for ISN09
  - — ISN09 Feature descriptions for CS2K International and World Trade
- Baseline information
  - — Logs/faults available, organized by network element
  - — OMs/PMs available, organized by network element
- Appendix A: Ethernet Routing Switch 8600 Performance Metrics
- Appendix B: MG9000 MIB OMs/PMs
- Appendix C: Media Gateway 15000 and MDM Alarm Log Summary
- Appendix D: USP OMs/PMs
- Appendix E: MG9000 Alarms, Event Logs, Audit Logs

- Appendix F: CICM Logs and Alarms
- Appendix G: Ethernet Routing Switch 8600 Trap List
- Appendix H: IEMS Fault Transparency with SDM/CBM
- Appendix I: MCS Alarms and Logs
- Appendix J: MCS Operational Measurements

Audience

This document is intended for Nortel Networks personnel, third-party OSS vendors, and customers who need to plan resources and estimate network impacts for this release.

How to check the version and issue of this document

The document release information on the title page and the footers of this document indicate the version and issue, for example, 01.01.

The first two digits indicate the version. The version number increases each time the document is updated to support a new software release. For example, the first release of a document is 01.01. In the next software release cycle, the first release of the same document is 02.01.

The second two digits indicate the issue. The issue number increases each time a document is revised but re-released in the same software release cycle. For example, the second release of a document in the same software release cycle would be 01.02.

Writing conventions

Descriptions of commands, parameters, and responses in this document use the following conventions:

Input prompt

An input prompt (> or #) indicates that the information that follows is a command:

```
>LIST
```

Commands and fixed parameters

Commands and fixed parameters that are entered at the MAP terminal are shown in uppercase letters:

```
>LIST ALL
```

Variables

Variables that are entered at a MAP terminal are shown in lowercase letters:

>TABLE table_name

References in this document

This document may refer to the following Nortel Networks publications:

- 297-8001-840, *NA DMS-100 Log Report Reference Manual*
- 297-2621-840, *DMS-250 Logs Reference Manual*
- NN10021-111, *cCS 2000 Product and Technology Fundamentals*
- NN10408-900, *ATM/IP Solution-level Fault Management*
- NN10409-500, *ATM/IP Solution-level Configuration Management*
- NN10401-700, *ATM/IP Solution-level Performance Management*
- NN10334-911, *IEMS Fault Management*
- NN10330-511, *IEMS Configuration Management*
- NN10327-711, *IEMS Performance Management*
- NN10324-509, *Carrier Voice over IP Operational Configuration: Data Schema Reference*
- NN10264-709, *Carrier VoIP Performance Management Operational Measurements Reference*
- NN10025-111, *SAM21 Product and Technology Fundamentals*
- NN10089-911, *SAM21 Fault Management*
- NN10111-511, *SAM21 Configuration Management*
- NN10155-711, *SAM21 Performance Management*
- NN10083-911, *CS 2000 Fault Management*
- NN10188-511, *CS 2000 Configuration Management*
- NN10149-711, *CS 2000 Performance Management*
- NN10275-909, *Carrier Voice over IP Fault Management: Logs Reference*
- NN10090-911, *GWC Fault Management*
- NN10012-111, *SPM Product and Technology Fundamentals*
- NN10075-911, *SPM Fault Management*
- NN10097-511, *SPM Configuration Management*
- NN10141-711, *SPM Performance Management*
- NN10079-911, *DPT-SPM (IP) Fault Management*
- NN10078-911, *IW-SPM (IP) Fault Management*
- NN10073-911, *UAS Fault Management*

- NN10139-711, *UAS Performance Management*
- NN10085-911, *cCS 2000 Fault Management*
- NN10082-911, *CS 2000 Core Manager Fault Management*
- NN10104-511, *CS 2000 Core Manager Configuration Management*
- NN10148-711, *CS 2000 Core Manager Performance Management*
- NN10300-100, *CS 2000 Management Tools IP Solutions Basics*
- NN10325-900, *CS 2000 Management Tools ATM/IP Fault Management*
- NN10276-500, *CS 2000 Management Tools ATM/IP Configuration Management*
- NN10149-711, *CS 2000 Performance*
- NN10088-911, *STORM Fault Management*
- NN10110-511, *STORM Configuration Management*
- NN10154-711, *STORM PerformanceManagement*
- NN10074-911, *MG 9000 Fault Management*
- NN10096-511, *MG 9000 Configuration Management*
- NN10140-711, *MG 9000 PerformanceManagement*
- NN10087-911, *Call Agent Fault Management*
- NN10109-511, *Call Agent ConfigurationManagement*
- NN10153-711, *Call Agent PerformanceManagement*
- NN10202-911, *Gateway Controller Fault Management*
- NN10205-511, *Gateway Controller ConfigurationManagement*
- NN10208-711, *Gateway Controller PerformanceManagement*
- NN10145-711, *DPT-SPM (IP) Performance*
- NN10144-711, *IW-SPM (IP) Performance*
- NN10071-911, *USP Fault Management*
- NN10137-711, *USP Performance Management*
- NN10351-911, *Core and Billing Manager 850 Fault Management*
- NN10361-711, *Core and Billing Manager 850 Performance Management*
- NN10076-911, *MG 4000 Fault Management*
- NN10142-711, *MG 4000 Performance Management*
- NN10080-911, *DPT SPM-ATM Fault Management*
- NN10146-711, *DPT SPM-ATM Performance Management*

- NN10077-911, *IW SPM-ATM Fault Management*
- NN10143-711, *IW SPM-ATM Performance Management*
- NN10328-911, *Media Server 2000 Series Fault Management*
- NN10331-711, *Media Server 2000 Performance Management*
- NN10438-911, *Policy Controller Fault Management*
- NN10439-711, *Policy Controller Performance Management*
- NN10332-911, *Session Server Fault Management*
- NN10342-711, *Session Server Performance Management*

In order to find informtion about the Multiserver Data Manager (MDM), refer to the following documents:

- 241-6001-011, *MDM Fault Management User Guide*
- 241-6001-501, *MDM Proxy Alarms Reference Guide*
- 241-6001-801, *MDM Overview*

Introduction and Mapping Tables

Overview

This document supports Nortel's Carrier VoIP Solutions ISN09 release for North American and International markets. The features described in Chapter 4 apply to International solutions only. This document describes ISN09 features that affect inputs to or outputs from the solutions. These changes, therefore, affect the use of the Operations Support System (OSS) for ISN09. The document includes copies of feature descriptions used in software design.

Information in this document is believed to be accurate at the time of publication, but it is subject to change. Use of this document should be restricted to resource planning and estimating for ISN09. DO NOT use this document to make changes to existing software.

How the North American section is organized

This portion of the document is divided into the following areas:

- *North American activities mapping tables*. These tables relate the activity identifier associated with each feature to:
  - the product/application/network element affected
  - affected software object types (data schema, for example)
- *North American features lists by solution type*. This part has two lists:
  - Features for IP solutions. This list includes all IP-solutions-related features. Features asssociated with the following solutions may be found here: PT-IP, UA-IP, IAC, IAW, CHS, MCS, and DMS. It also identifies features associated with the PT-AAL2 solution. (The main difference between IP solutions and the ATM AAL2 solution is that the Media Gateways are se tup to transport the bearer path using ATM AAL2 instead of IP.)
  - Features for ATM solutions. This list includes all ATM-solutions-related features. Features asssociated with the following solutions may be found here: PT-AAL1, UA-AAL1.

- *Chapter 1, New and changed* for (I)SN09 (North American). This section provides a table for each software object type, as follows:
  - Logs and alarms
  - Data Schema tables or MIBs
  - User Interface (commands)
  - Service Orders (Servord+)
  - Office parameters
  - Operational and Performance Measurements (OMs and PMs)
  - AMA/billing
  - Software Optionality Control (SOC)

Each table gives a summary of the changes caused per feature. Within each table, features are arrranged by product/application, network element and then in numeric order by the ACTID of the feature which creates new information or causes the change.

- *Chapter 2, IEMS Functionality for (I)SN09*. This chapter provides information on fault management and performance management for all network elements regarding their interaction with IEMS.
- *Chapter 3, Feature descriptions (North American and some International)*. This section provides feature descriptions, based on design documents. These are organized by product/application/network element and then in numeric order by ACTID.
  The features that apply to both North American and International markets are located in this chapter, while the International-only features are located in Chapter 4.

ISN09 Activity mapping tables

Introduction

This document contains advance information about differences in operations, administration, maintenance, and provisioning (OAM&P) for (I)SN09. The purpose of this document is to provide early information about new, modified or deleted items related to OSS-impacting areas.

The table below shows the mapping from the activity identifier (ACTID) associated with each new feature to the following:

- the associated product, application, or network element

- the solution that the feature affects, of the following:
  - PT-IP
  - UA-IP
  - IAW
  - IAC
  - DMS
  - MCS
  - CHS
  - AAL2
  - UA-AAL1
  - PT-AAL1
- the software object type or area that the feature affects, of the following:
  - Logs/faults
  - Data schema tables/MIBs
  - Office parameters
  - Service orders (ServOrd)
  - User interface/human-machine interface
  - Operational and performance measurements (OMs/PMs)
  - Automatic Message Accounting (AMA)/billing
  - Software Optionality Control (SOC)

Activity Mapping Table: Solutions Affected

		(I)SN09 Solutions									
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	DMS	MCS	CHS	AAL2	UA-AAL1	PT-AAL1
CS 20000	A89007819	X		X	X						
CS 20000	A00007217							X			
CS 2000	A00007269	X									
CS 2000	A00007544	X						X			
CS 2000	A00007547							X			
CS 2000	A00008043				X						
CS 2000	A00008090										X
CS 2000	A00008556							X			
CS 2000	A00008601	X									
CS 2000	A00008629	X									X
CS 2000	A00008724										X
CS 2000	A00009036		X								
CS 2000	A00009078		X			X				X	
CS 2000	A00009085		X			X				X	
CS 2000	A00009091		X								
CS 2000	A00009120		X								
CS 2000	A00009129	X									
CS 2000	A00009153							X			
CS 2000	A00009190		X								
CS 2000	A00009200	X									
CS 2000	A00009204	X							X		
CS 2000	A00009207										X
CS 2000	A00009208		X	X	X						
CS 2000	A00009235	X			X						
CS 2000	A00009252		X								
CS 2000	A00009311		X						X		
CS 2000	A00009313		X						X		
CS 2000	A00009315		X						X		
CS 2000	A00009332	X	X								X
CS 2000	A00009353	X									
CS 2000	A00009364							X			
CS 2000	A00009375 & 9376							X			
CS 2000	A00009443	X						X			
CS 2000	A00009463	X				X			X		X
CS 2000	A00009470	X							X		X
CS 2000	A00009508							X			
CS 2000	A00009514	X			X			X			

		(I)SN09 Solutions									
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	DMS	MCS	CHS	AAL2	UA-AAL1	PT-AAL1
CS 2000	A00009515							X			
CS 2000	A00009520		X								X
CS 2000	A00009530							X			
CS 2000	A00009550	X				X			X	X	
CS 2000	A00009822	X	X						X	X	X
CS 2000	A00009839										X
CS 2000	A00009840										X
CS 2000	A00009893	X							X		
CS 2000	A00010303					X			X		
CS 2000	A00012001		X								
CS 2000	A00012210		X								
IEMS	A00009289		X						X		
IEMS	A00009292										
IEMS	A00009320		X							X	
IEMS	A00009532		X						X	X	
IEMS	A00009611		X								
IEMS	A00009612		X								
IEMS	A00009614		X								
IEMS	A00009777		X						X		
IEMS	A00009823		X								
MCS	A00009028						X				
MCS	A00009043						X				
MCS	A00009045						X				
MCS	A00009092						X				
MCS	A00009241							X			
MCS	A00009651						X				
MCS	A00009655						X				
MCS	A00011740				X						
MG 9000	A00008858		X							X	
MG 9000	A00008969		X							X	
MG 9000	A00009218		X							X	
MG 9000	A00011167		X							X	
CS2K Mgmnt Tools	A00008522		X				X				
CS2K Mgmnt Tools	A00008916	X	X	X	X				X		
CS2K Mgmnt Tools	A00009189			X	X						
CS2K Mgmnt Tools	A00009310		X								
CS2K Mgmnt Tools	A00009339				X						
CS2K Mgmnt Tools	A00009890							X			
CS2K Mgmnt Tools	A00010617			X	X						

		(I)SN09 Solutions									
PRODUCT or APPLICATION	ACTID	PT-IP	UA-IP	IAW	IAC	DMS	MCS	CHS	AAL2	UA-AAL1	PT-AAL1
CS2K Mgmnt Tools	A00011746			X	X						
Network Patch Mgr.	A00009227	X	X	X	X				X	X	
CS 2000-TOPS	A00009011	X				X					X
CS 2000-TOPS	A00009012	X				X					X
CS 2000-TOPS	A00009013	X				X					

Activity Mapping Table: Software object types or areas impacted

(I)SN09 Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Parms	Service Orders	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
CS 20000	A89007819	X							
CS 20000	A00007217					X			
CS 2000	A00007269					X			
CS 2000	A00007544		X			X			X
CS 2000	A00007547	X		X			X		
CS 2000	A00008043	(See A00009189-CS2M)							
CS 2000	A00008090							X	
CS 2000	A00008556		X		X	X			X
CS 2000	A00008601		X						
CS 2000	A00008629		X	X		X			
CS 2000	A00008724						X		
CS 2000	A00009036		X						
CS 2000	A00009078		X						X
CS 2000	A00009085		X	X	X				X
CS 2000	A00009091		X						X
CS 2000	A00009120	X							
CS 2000	A00009129					X			
CS 2000	A00009153		X						
CS 2000	A00009190		X						
CS 2000	A00009200					X			
CS 2000	A00009204					X			

(I)SN09 Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Parms	Service Orders	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
CS 2000	A00009207			X					
CS 2000	A00009208			X					
CS 2000	A00009235	X				X			
CS 2000	A00009252							X	
CS 2000	A00009311					X			
CS 2000	A00009313					X			
CS 2000	A00009315	X							
CS 2000	A00009332					X			
CS 2000	A00009353	X							
CS 2000	A00009364	X					X		
CS 2000	A00009375 & 9376		X						
CS 2000	A00009443					X			
CS 2000	A00009463					X			
CS 2000	A00009470					X			
CS 2000	A00009508							X	
CS 2000	A00009514					X			
CS 2000	A00009515	X							
CS 2000	A00009520					X			
CS 2000	A00009530					X			
CS 2000	A00009550					X			
CS 2000	A00009822	X				X			
CS 2000	A00009839					X			
CS 2000	A00009840					X			
CS 2000	A00009893	X					X		
CS 2000	A00010303					X			X
CS 2000	A00012001					X			
CS 2000	A00012210					X			
IEMS	A00009289					X			
IEMS	A00009292					X			
IEMS	A00009320					X			
IEMS	A00009532	X				X			
IEMS	A00009611	X				X			
IEMS	A00009612					X			
IEMS	A00009614	X							

(I)SN09 Solutions		Documentation Elements							
PRODUCT	ACTID	Logs/Faults	Data Schema	Office Parms	Service Orders	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
IEMS	A00009777	X				X	X		
IEMS	A00009823	X							
MCS	A00009028					X			
MCS	A00009043					X			
MCS	A00009045	X					X		
MCS	A00009092					X			
MCS	A00009241					X			
MCS	A00009651					X			
MCS	A00009655					X			
MCS	A00011740						X		
MG 9000	A00008858					X			
MG 9000	A00008969					X			
MG 9000	A00009218					X			
MG 9000	A00011167					X			
CS2K Mgmnt Tools	A00008522		X		X	X			
CS2K Mgmnt Tools	A00008916					X			
CS2K Mgmnt Tools	A00009189		X			X			
CS2K Mgmnt Tools	A00009310					X			
CS2K Mgmnt Tools	A00009339					X			
CS2K Mgmnt Tools	A00009890					X			
CS2K Mgmnt Tools	A00010617					X			
CS2K Mgmnt Tools	A00011746		X						
Network Patch Mgr.	A00009227	X							
CS 2000-TOPS	A00009011		X	X					
CS 2000-TOPS	A00009012		X			X			
CS 2000-TOPS	A00009013	X	X						

IP and ATM Features Lists

Introduction

This section consists of two tables: Features for IP solution, and Features fror ATM solutions. The first table shows all features in numeric order by ACTID that are applicable to the various VoIP solutions:

- PT-IP
- UA-IP
- IAW
- IAC
- DMS
- MCS
- CHS

Features for IP solutions

ACTID	Feature Title	IP Solution
A89007819	QoS Reporting: QoS Collector Application (QCA)	PT-IP, IAW, IAC
A00007217	ITRANS Media Proxy Selection	CHS
A00007269	NGSS Backup and Restore	PT-IP
A00007544	NCAS Link & SIP NMS Support	PT-IP, CHS
A00007547	SIP Lines Core Call Processing Support	CHS
A00008043	CS2K Support for 64 Character FQDN (in 9189)	IAC
A00008522	SESM Support for SIP Lines	UA-IP, MCS
A00008556	SIP Lines Core OAMP Support	CHS
A00008601	IW-SPM-IP Fully Provisionable Codec Lists for G.711/G.729	PT-IP
A00008629	GEM-II AAL2 IW-SPM SN09 Core Preparation Work	PT-IP, PT-AAL1
A00008858	CS2M & MG9K EM - User Inactivity Time-out	UA-IP
A00008916	Increase Port Density	PT-IP, UA-IP, IAC
A00008969	MG9000 ATM50 SSI Monitoring	UA-IP,
A00009011	TOPS IP Security Enhancements	PT-IP, DMS

ACTID	Feature Title	IP Solution
A00009012	TOPS OSSAIN Service Enhancements	PT-IP, DMS
A00009013	TOPS Announcements via UAS/AMS	PT-IP, DMS
A00009028	PHX SIP Lines OAM Support	MCS
A00009036	Table HOMELRN Option SITE Expansion	UA-IP
A00009043	PHX SIP Lines Provisioning Support	MCS
A00009045	CALLP Checkpointing Support	MCS
A00009078	ICM Dual CTI	UA-IP, DMS
A00009085	ACD & ICM Capacity Expansion	UA-IP, DMS
A00009091	EA LPIC Privilege Routing	UA-IP
A00009092	CS2K MSM SIP Lines Cisco 7960 Client Integration	MCS
A00009120	Multi Time Zone Enhancement	UA-IP
A00009129	Controlled Hot SWACT	PT-IP
A00009153	H.323 RLT Development	CHS
A00009189	SESM Support for 64 Character FQDN	IAW, IAC
A00009190	Universal Carrier Protocol (UCP) C7UPTMR Enhancements	UA-IP
A00009200	Packet Trunking Trunk Test: Milli-watt Tone Swap	PT-IP
A00009204	Call Agent Customer Visible Capacity Tools	PT-IP
A00009208	180K Lines Support	UA-IP, IAW,IAC
A00009218	MG9KEM Data Audit Robustness	UA-IP
A00009227	NPM Robustness	PT-IP, UA-IP, IAW, IAC
A00009235	TLS for SIP	PT-IP, IAC
A00009241	NCAS & QSIP Development on CS2K SS	CHS
A00009252	Multi-Time Zone AMA Enhancements	UA-IP
A00009289	IEMS - 10 Minute Default on User Inactivity Timer	UA-IP
A00009292	IEMS:UserID-based Partitioning byNE	UA-IP
A00009310	SSPFS CLUI Restricted Access	UA-IP
A00009311	SSPFS Dark Office Backup	UA-IP
A00009313	SSPFS SN09 Upgrades and ESD Support	UA-IP

ACTID	Feature Title	IP Solution
A00009315	SSPFS Detect Failures from Syslog and Generate Alarms	UA-IP
A00009320	IEMS - Remote Ping & Traceroute for GWC & SSPFS	UA-IP
A00009332	P-Time and Codec Negotiation Selection Policy	PT-IP, UA-IP
A00009339	Packet Cable 1.5 Support	IAC
A00009353	GWCUnit Availability/ Health Monitoring	PT-IP
A00009364	CICM End-of-Call QOS Reporting	CHS
A00009375 & A00009376	CICM Third-party Corrective Content Patching & CICM Selective Binary Component Patching	CHS
A00009443	T.38 Annex D for NGSS	PT-IP, CHS
A00009463	CBM to Support Centralized User Authentication	PT-IP, DMS
A00009470	SDM To Support SAML NNSSwitch Client	PT-IP
A00009508	AMA SIP Line Identification	CHS
A00009514	CS2K-MCS Interop for SN09	PT-IP, IAC, CHS
A00009515	Out-of-Band interop with MCS	CHS
A00009520	Trunk blocking tools for MG4K and GWC on SN09	UA-IP
A00009530	H248 and xUA NAT traversal for CPE Gateways	CHS
A00009532	IPSEC Host to Host Tunnels for Northbound OSS Connections	UA-IP
A00009550	CBM-NPM Patching Convergence	PT-IP, DMS
A00009611	IEMS - Keymile Integration	UA-IP
A00009612	IEMS - Restricted Access Shell	UA-IP
A00009614	IEMS - Provide Tamper Proof Key Storage	UA-IP
A00009651	Web Collaboration Multilingual Support	MCS
A00009653	Web - PROV/PA/Client Service	MCS
A00009655	BladeCenter-T RTP Media Portal	MCS
A00009777	IEMS - Mediant 2000 Integration	UA-IP
A00009822	SSPFS - General Security Log When the User Logs Out	PT-IP, UA-IP
A00009823	SSPFS - Security Logging	UA-IP

ACTID	Feature Title	IP Solution
A00009890	Provisioning for MP	CHS
A00009893	Session Server Call Processing Overload	PT-IP
A00010303	CS2K - CI Command	DMS
A00010617	Addition of Neura-BTX-4K	IAW, IAC
A00011167	MG9KEM - Central UserID and Password Support	UA-IP, UA-AAL1
A00011740	Packet Cable Multimedia for CS2K	IAC
A00011746	Addition of LGRP_TYPE field to GW profiles	UA-IP
A00012001	IEMS Call Server 2000 SIP Integration	UA-IP
A00012210	Geo OA&M Automatic Backup and Accelerated Restore	UA-IP

Features for ATM solutions

This table shows all features in numeric order by ACTID that are applicable to the various VoATM solutions:

- PT-AAL1
- UA-AAL1
- PT-AAL2

ACTID	Feature Title	ATM Solution
A00008090	SBA: Alternate Scheduled Closure of Billing Files	PT-AAL1
A00008858	CS2M & MG9K EM - User Inactivity Time-out	UA-AAL1
A00008629	GEM-II AAL2 IW-SPM SN09 Core Preparation Work	PT-AAL1
A00008724	OMDD Enhancements and Robustness	PT-AAL1
A00008969	MG9000 ATM50 SSI Monitoring	UA-AAL1
A00009011	TOPS IP Security Enhancement	PT-AAL1, DMS
A00009012	TOPS OSSAIN Service Enhancement	PT-AAL1, DMS
A00009013	TOPS Announcements	DMS
A00009078	ICM Dual CT	UA-AAL1, DMS
A00009085	ACD & ICM Capacity Expansion	UA-AAL1, DMS
A00009091	Equal Access (EA) LPIC Privilege Routing	PT-AAL1

ACTID	Feature Title	ATM Solution
A00009207	DPT Trunk Testing Support	PT-AAL1
A00009218	MG9KM Audit Robustness	UA-AAL1
A00009227	NPM Robustness	UA-AAL1
A00009280	MG9KEM Line Circuit Enhancements	UA-AAL1
A00009292	IEMS:UserID-based Partitioning byNE	UA-AAL1
A00009332	P-Time and Codec Negotiation Selection Policy	PT-AAL1
A00009463	CBM to Support Centralized User Authentication	PT-AAL1, DMS
A00009470	SDM To Support SAML NNSSwitch Client	PT-AAL1
A00009520	Trunk blocking tools for MG4K and GWC on SN09	PT-AAL1
A00009532	IPSEC Host to Host Tunnels for Northbound OSS Connections	UA-AAL1
A00009550	CBM-NPM Patching Convergence	UA-AAL1, DMS
A00009822	SSPFS - General Security Log When the User Logs Out	PT-AAL1, UA-AAL1
A00009839	Ability to apply patches during ESUP upgrade	PT-AAL1
A00009840	CBM IPSec Northbound Interface	PT-AAL1
A00009292	IEMS: UserID-based Partitioning by NE	UA-AAL1
A00010303	CS2K - CI Command	DMS
A00011167	MG9KEM - Central UserID and Password Support	UA-AAL1

Chapter 1: New and changed

New or changed for (I)SN09

This section of the document contains tables which give an overview of the feature-based changes occurring in the (I)SN09 release for the following categories:

- Logs/alarms
- Data Schema tables and MIBs
- User interface (Commands)
- Service order (Servord+)
- Office parameters
- Operational measurements (OMs) and performance measurements (PMs)
- AMA/Billing
- Software Optionality Control (SOC)

Within each table, the changes are arranged by associated product, and then in numeric order by the ACTID of the feature which creates new information or causes the change.

Solutions Application

This OSS Guide includes both IP solutions and ATM solutions. The ATM AAL2 solution differs from IP solutions in that the ATM AAL2 solution has Media Gateways set up to transport the bearer path using ATM AAL2 instead of IP. The signaling functionality for both ATM AAL2 and IP solutions is the same.

SSH Compatibility statement

Access to some functions requires the use of SSH compatible client software for access to secure telnet and ftp services (via the SSH standard). SSH clients are supplied bundled with some operating systems, but may need to be obtained separately. Sources for SSH clients include (but are not limited to):

- PUTTY - freeware
- OpenSSH - freeware
- SSH Inc. - commercial
- Secure CRT - commercial
- WinSCP - freeware

Nortel does not supply or recommend a particular supplier.

Logs/faults changes overview

The following logs/faults are new or changed for (I)SN09. They also appear in the logs-by-product tables in the Baseline section of this document with descriptions/cause for generation. This section also offers general log changes. Additional information is available in the Feature Deltas section of this document.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Product = CS 2000		
QCA logs (changed)	(refer to FN)	Feature A89007819 (PT-IP, IAW, IAC, Int'l PT-IP, Int'l IAW, Int'l IAC) is updated for SN09 to reflect changes in the QCA logs. See Appendix A of the feature for a complete list of QCA logs.
NMSS logs (new)	NMSS115 NMSS116 NMSS117 NMSS118	Feature A00007544 (PT-IP, CHS, Int'l PT-IP) creates the following logs. • NMSS115 - generated if an error occurs while sending NMS TCAP messages to SCTP. • NMSS116 - generated if an error occurs while receiving NMS TCAP messages from SCTP. • NMSS117 - generated if an error occurs while sending NMS REJ messages to SCTP. • NMSS118 - generated if an error occurs while receiving NMS REJ messages from SCTP.
NCAS logs (new)	NCAS325 NCAS601	Feature A00007544 (PT-IP, CHS, Int'l PT-IP) creates the following logs. • NCAS325 - an alarm log generated when a critical alarm is raised because the NCAS Link goes down. It is also generated when the alarm is cleared when the NCAS Link comes up. • NCAS601 - raised when a new NCAS Link is created.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
DPL logs (new)	DPL100 DPL101	Feature A00007547 (CHS) creates the following logs. • DPL100 indicates that reconstruction of the VID resource pool has started. • DPL101 indicates that reconstruction of the VID resource pool has completed.
SDM logs (new)	SDM338 SDM631 SDM638 SDM639	Feature A00007547 (CHS) creates the following logs. • SDM338 indicates that omdata file system usage exceeds 60% (Minor) or 80% (Major). • SDM631 indicates that a file in *closedNotSent* directory is deleted by audit to make morethan 80% available space in the omdata file system. • SDM638 indicates that the OMDD audit finds omdata file system usage goes below 80% or below 60%. • SDM639 indicates that the OMDD audit finds omdata file system usage exceeds 90%. All the OM files from the closedSent directory will be deleted.
Syslog alarm (new)	N/A	Feature A00009315 (UA-IP) creates a raise major alarm to indicate that the syslog system has failed to write logs, and a clear alarm to indicate that syslog has resumed writing logs. Both alarms are reported in log SPFS380.
LINE and MCT logs (changed)	LINE125 LINE126 MCT103 MCT105	A00009120 (UA-IP) modifies these logs by adding a new field, LOCAL TIME, to display the local time for that subscriber line based on the switch time modified by the value in table MUTITM if assigned to that line. This change is made to support the Multiple Time Zones feature.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
SIPS logs (new)	SIPS303 SIPS308 SIPS608 SIPS609	Feature A00009235 (PT-IP, IAC) creates the following logs. • SIPS303 - Certificate Mismatch in Server Certificate, generated if the two sets of files on the active and inactive sides do not match each other. An alarm is also raised. • SIPS308 - Failed Certificate Policy Check, generated when enough certificate policy failures have occurred to generate an alarm. An alarm is also raised. • SIPS608 - TLS Certificate Policy failure, generated when the remote side of the connection presents a certificate that does not conform to the selected local certificate policy. • SIPS609 - Security Parameter Changed, generated whenever a TLS Security Parameter is changed by the user.
SIPS logs (changed)	SIPS305 SIPS604	Feature A00009235 (PT-IP, IAC) creates the following logs. • SIPS305 - TLS Initialization Failure, generated during the initialization of the Call Processing application (i.e. during the unlock). If one of the critical logs come out, it means that there is a problem with the initialization, and the application is unable to start. An alarm is also raised. • SIPS604 - TLS Initialization Logs, originally implemented in SN08. The Certificate Effective Date log is the new content being documented here.
PreSwact Audit Failure alarm (new)	GWC317	Feature A00009353 (PT-IP) creates a new alarm which will be raised whenever PreSwact audit fails. An alarm will be raised with proper text which explains which component has led Preswact audit to fail. The specific problem displayed at the GWC level for the alarm raised will match with the swact failure reason at the SESM GUI.
CICM alarm and log (new)	CICM363	Feature A00009364 (CHS) creates an INFO alarm Subtract ConnectionAck Failed, raised when Subtract ConnectionAck cannot determine the destination for a message. Relates to log CICM363.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
NCAS log (new)	NCAS501 NCAS502	Feature A00009515 (CHS) creates the following logs: • NCAS501, generated when an Out-of-Band REFER Request that has been received by the Session Server does not validate and this the request can not be accepted. • NCAS502 indicates Unable to Establish Connection with SCPLite.
SIP Gateway application overload-related events on the Session Server (new)	STGW700 CPU Occupancy Alarms	Feature A00009893 (PT-IP) creates new logs and alarms to provide notification of SIP Gateway application overload-related events on the Session Server. • STGW700 is an INFO log that may indicate any one of these issues or problems: FCR Change, Babbling node detected, Babbling node timeout, All babbling node IPs re-enabled due to initialization, or CPU occupancy critical alarm. • Alarm CPU Occupancy Critical, generated when the CPU occupancy reaches 90%. • Alarm CPU Occupancy Major, generated when the CPU occupancy reaches 85%. • Alarm CPU Occupancy Minor, generated when the CPU occupancy reaches 80%.
GWC304 SNMP traps (changed)	GWC304	Per CR Q01148626-02, the GateWay information which is now the Specific Problem field of the event is populated in the nnExtAlarmActiveAdditionalText VarBind. Hence the OSS has to parse this VarBind additionally to extract the GateWay information.
GWC logs	(see list in next column)	Per CR Q01115352, Location and Component ID fields are added to GWC350, GWC400, GWC501, GWC502, GWC503, GWC506, GWC507, GWC600, and GWC 601
GWC log	GWC603 (new)	CR Q01221814 creates new log GWC603 to indicate that a netfail event occurred from the GW and was reported to the connection broker. The log shows on which GWC the problem occurred, the Gateway name, IP address of the GW, the Endpoint name, the terminal ID, and the reason for the netfail event.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
GWC log	GWC604 (new)	CR Q01221822 creates new log GWC604 to indicate that a connection broker exception occurred from the GW and was reported. The log shows on which GWC the problem occurred, the Gateway name, IP address of the GW, the Endpoint name, the terminal ID, and the reason for the exception.
SAM21 Event Traps (changed)	N/A	Per CR Q01140338-02, the VarBind related to the alarmActiveDescription (.1.3.6.1.2.1.118.1.2.2.1.11) will now have only the Reason field value. Also, the VarBind corresponding to nnExtAlarmActiveResourceDescription (.1.3.6.1.4.1.562.29.6.1.1.1.5) will have the componentId of the log.
MDM alarms (changed)	N/A	Per CR Q01141846, the FaultCode information which is now the Specific Problem field of the event is populated in the nnExtAlarmActiveAdditionalText VarBind. Hence the OSS has to parse this VarBind additionally to extract the FaultCode information. Also, the tag faultCode : will not be present in the VarBind value.
MCS-related logs (new)	refer to the next column	Per MCS design, the following alarm logs are new for SN09: • EMTC401 - A threshold has been crossed. The number of unreachable static clients has reached or exceeded the configured percentage of 100 % ... currently there are 20000 unreachable clients. Also functions as a Clear log. • NCAS101 - An NCAS link has been disconnected from a specified IP address. Also functions as a Clear log. • NED101 - Local communication with NED (Network Element Daemon) lost. This normally indicates NED has died, in which case it should automatically be restarted. Also functions as a Clear log. • NIF200 - The logical interface for a specified floating IP Address is not up. Also functions as a Clear log. • NIF201 - Failed to down logical interface for a specified floating IP Address. Also functions as a Clear log.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) MCS-related logs (new)	(continued) refer to the next column	(continued) Per MCS design, the following alarm logs are new for SN09: • RTP101 - Critical. Raised from alarm “Blade Out of Service.” Occurs when Managed IP or MCP Service network difficulties (communication problems) are encountered when attempting to communicate with the Media Blade specified by BladeName. • RTP102 - Critical or Major. Raised from alarm “RTP Media Portal Out of Service.” Occurs when timer activated event checks availability of Media Blades that are currently configured or when a OutOfServiceAlarm is raised. • RTP103 - Critical. Raised from alarm “Best Blade Selection.” Occurs during session setup when the host attempts to determine which media blade should handle the session. • RTP104 - Critical, Major, or Minor. Raised from alarm “Port Usage.” Occurs when timer activated event checks to see what percentage of the configured Managed IP Network ports are in use. Alarm severity is based on the percentages configured for the parameters: "Minor Port Usage Alarm Level," "Major Port Usage Alarm Level," and "Critical Port Usage Alarm Level." • RTP105 - Major. Raised from alarm “Host Interface Failure.” Occurs when a timer activated event checks the status of host network interfaces. • R6AS700 - R6AS configuration modified while instance is not offline. Also functions as a Clear log. • RTPB804 - An error occurred during initialization. test-string. The RTP Media Portal is NOT operational. Also functions as a Clear log. • RTPB805 - The RTP Media Portal Blade in slot 1 is in Standby. Also functions as a Clear log. • RTPB806 - Cluster is in a 1+0 configuration with 0 node(s) shutting down and should be in a 1+1 configuration. Also functions as a Clear log.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) MCS-related logs (new)	(continued) refer to the next column	(continued) Per MCS design, the following alarm logs are new for SN09: • RTPB815 - Live Update of Media Portal Cluster Configuration Parameters Data is NOT supported. Also functions as a Clear log. • RTPB816 - Live Update of Media Portal Cluster Fault Tolerance Data is NOT supported. Also functions as a Clear log. • RTPB817 - Live Update of Media Portal Cluster Gateway Controllers Data is NOT supported. Also functions as a Clear log. • RTPB818 - Live Update of Media Portal Cluster Session Managers Data is NOT supported. Also functions as a Clear log. • RTPB819 - Live Update of Media Portal Cluster Static Routes Data is NOT supported. Also functions as a Clear log. • RTPB820 - Live Update of Media Portal Cluster Service Instance Data is NOT supported. Also functions as a Clear log. • SIP401 - The number of 500 Server Internal Error responses to SIP 9273429374@47.102.244.146 requests in OM group SIP_Inbound_Response_Report exceeds the specified percentage of responses. Also functions as a Clear log. • SIP703 - Raise: Message received that contained bad syntax information. Bad headers will be discarded. Also functions as a Clear log. • SVCA801 - The System Manager service address has changed. Also functions as a Clear log. • SYS707 - A request to receive synchronization from peer is rejected. Also functions as a Clear log.
CICM alarm and log (new)	NoBootpResponse, CICM351	CR Q01103219 creates this alarm and log as a warning that, although started, the CICM/CICM-EM was unable to retrieve its basic configuration data. It then checks to see whether it has old configuration data stored from a previous boot, and it will use that instead. As a result,this log and alarm means that the CICM/CICM-EM is currently using old configuration data that may no longer be up to date

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Product = CS 2000 TOPS		
TOPS logs (changed)	TOPS113 TOPS104	Feature A00009013 (PT-IP, DMS) modifies the following logs: • TOPS113 changes the fixed string in the Event Label field from TOPS DRAM PLAY TRBL to ANNOUNCEMENT PLAY TRBL. • TOPS104 changes the TROUBLE CODE field, removing values NO_REPLY_FROM_ DRAM and MISC_DRAM_FAIL, and adding value MISC_ANNOUNCEMENT_FAIL. When this trouble code is generated, the TOPS104 log is most often accompanied by another log that provides more detailed information.
Product = IEMS		
IEMS north-bound NT STD log feed (changed)	All Logs in the SCC2 stream	CR Q01177244 - **IMPORTANT:** IEMS's northbound NT STD log feed to the fault OSS has changed with respect to the "Start of Log string" in SN09. Previously, the Start of Log string was just a carriage return character (0D in Hexidecimal, 13 in Decimal). With the implementation of this CR in SN09, the Start of Log string is now a line feed followed by a carriage return. (0A0D in Hexidecimal, 1013 in Decimal). Customer fault OSSs receiving the NT STD stream pre-SN09 should be prepared for the change prior to IEMS upgrade to SN09. At the time of writing, there are no plans to patch this change back to previous releases.
IEMS northbound SCC2 log feed (changed)	All Logs in the SCC2 stream	CR Q01091683 - **IMPORTANT:** The IEMS SCC2 northbound log stream to the OSS has changed in SN09. This change affects only the Start of Log delimiter. Previously, the Start of Log delimiter was just a carriage return (0D in hexidecimal). With this CR implementation, the Start of Log string has been changed to be a line feed followed by a carriage return. (0A0D in hexidecimal). This change has been patched back to SN08 via CR Q01091683-01 and to SN07 as well via CR Q01091683-02. OSSs receiving the SCC2 log stream pre-SN09 should be prepared for the change prior to IEMS upgrade to SN09.
IEMS logs (new)	IEMS601, IEMS602 (changed)	CR Q01151503 modifies these logs by adding the Component ID and Location fields, and by changing the Location field value structure.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
IEMS log (new)	IEMS614 (new)	CR Q01158203 creates new log IEMS614 when IEMS receives an OSI State Change SNMP Notification (nortelNMIneOSIstateChangeNortification) trap from the MCS Manager.
IEMS log (new)	IEMS615	CR Q01177066 creates new log IEMS615, generated whenever IEMS receives a Stateless Clear (Orphaned Clear), that is, whenever IEMS receives a Clear from the Southbound device, for which IEMS could not identify the matching raise from its database. Hence the OSS should use this log to identify some kind of misleading log information that is being sent from the Southbound devices. NOTE: This log is not generated for MDM devices since they send two clears for a single raise alarm (one normal clear and one explicit clear).
IKE failure messages (changed)	N/A	Feature A00009532 (UA-IP) enables host-to-host IPSec between SSPFS servers. As part of that functionality, Internet Key Exchange (IKE) generates failure messages to syslog. The FN lists 41 possible failure messages.
UNEM and UMUX Alarms and Logs (new)	UNEM or UMUX300 UNEM or UMUX301 UNEM or UMUX302 UNEM or UMUX303 UNEM or UMUX304 UNEM or UMUX500 UMUX501 UMUX502 UNEM or UMUX600	Feature A00009611 (UA-IP) creates the following UNEM and UMUX alarms and logs: • UNEM or UMUX300 is generated for a minor, major, or critical communication alarm. • UNEM or UMUX301 is generated for a minor, major, or critical equipment alarm. • UNEM or UMUX302 is generated for a minor, major, or critical environmental alarm. • UNEM or UMUX303 is generated for a minor, major, or critical processing error alarm. • UNEM or UMUX304 is generated for a minor, major, or critical quality of service alarm. • UNEM or UMUX500 is generated when a standing alarm condition has bee cleared. • UMUX501 INFO is generated to indicate a change in the operational state of a UMUX NE. • UMUX502 INFO is generated to indicate that the UNEM's polling status of the UMUX NE has been modified. • UNEM or UMUX600 INFO is generated when an alarm is acknowledged by the UNEM system.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
UNEM and UMUX Alarms and Logs (new)	(continued) UNEM or UMUX300 UNEM or UMUX301 UNEM or UMUX302 UNEM or UMUX303 UNEM or UMUX304 UNEM or UMUX500 UMUX501 UMUX502 UNEM or UMUX600 UMUX601 UMUX602 UMUX603 UMUX604 UMUX605	(continued) Feature A00009611 (UA-IP) creates the following UNEM and UMUX alarms and logs: • UNEM or UMUX300 is generated for a minor, major, or critical communication alarm. • UNEM or UMUX301 is generated for a minor, major, or critical equipment alarm. • UNEM or UMUX302 is generated for a minor, major, or critical environmental alarm. • UNEM or UMUX303 is generated for a minor, major, or critical processing error alarm. • UNEM or UMUX304 is generated for a minor, major, or critical quality of service alarm. • UNEM or UMUX500 is generated when a standing alarm condition has bee cleared. • UMUX501 INFO is generated to indicate a change in the operational state of a UMUX NE. • UMUX502 INFO is generated to indicate that the UNEM's polling status of the UMUX NE has been modified. • UNEM or UMUX600 INFO is generated when an alarm is acknowledged by the UNEM system. • UMUX601 INFO is generated when a UMUX NE has been added to the UNEM topology inventory. • UMUX602 INFO is generated when a UMUX NE has been deleted from the UNEM topology inventory. • UMUX603 INFO is generated when a UMUX NE name is changed in the UNEM. • UMUX604 INFO is generated when a card has been added to a managed UMUX inventory. • UMUX605 INFO is generated when a card has been deleted from a managed UMUX inventory.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
IEMS Security logs (new)	Refer to description column	Feature A00009614 (UA-IP) creates the following security logs: • Database password change logs: successful change, invalid user, and invalid machine used. • Certificate creation and change logs: fresh certificate installed, and certificate changed. • ssh Key creation and change logs: ssh key change, and invalid user for ssh key change. • IPSec IKE policy creation and deletion logs: — IKE rule added — IKE entry added — IKE rule deleted — IKE entry deleted — Problem occurred loading IPSec rules on other cluster unit — Could not Sync IPSec data — IKE rule could not be added — IKE configuration data could not be updated — IKE preshared key data could not be updated — IKE entry could not be added — IKE key could not be deleted — IKE rule could not be deleted — IKE rules could not be updated — IKE key could not be updated — IKE entry could not be deleted • IPSec Key Change logs: — Preshared key modified — Attempt to modify Preshared key — Could not change Preshared key

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
(continued) IEMS Security logs (new)	(continued) refer to description column	(continued) Feature A00009614 (UA-IP) creates the following security logs: • IPSec Key Change logs (contiinued): — IKE preshared key data could not be updated — Problem occurred loading IPSec rules on other cluster unit — Could not Sync IPSec data — Could not modify preshared key • IPSec IPSec Policy Creation and Deletion logs: (The same logs are created here as for IKE Policy Creation and Deletion.)
IEMS Security alarms (new)		Feature A00009614 (UA-IP) creates the following security alarms: • Password expiration warning alarm (Info), relates to SPFS350 log. • Password expiration alarm (Minor), relates to SPFS350 log. • Account expiration warning alarm (Info), relates to SPFS350 log. • Account expiration alarm (Minor), relates to SPFS350 log. • Certificate expiration alarm (Minor), relates to SPFS350 log. • Certificate expiration alarm clearing, relates to SPFS350 log.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
MG 3200 trap handling and MGTH logs (new)	MGTH300 MGTH301 MGTH302 MGTH303 MGTH307 MGTH309 MGTH312 MGTH313 MGTH314 MGTH500 MGTH501 MGTH600 MGTH601 MGTH800	Feature A00009777 (UA-IP) creates MG 3200 device trap handling in the IEMS as follows: • MGTH300--acBoardEvResettingBoard • MGTH301--acBoardFatalError • MGTH302--acBoardConfigurationError • MGTH303--acBoardTemperatureAlarm • MGTH307--acBoardEthernetLinkAlarm • MGTH309--acActiveAlarmTableOverflow • MGTH312--acOperationalStateChange • MGTH313--acKeepAlive • MGTH314--acNATTraversalAlarm • MGTH500--acBoardEvBoardStarted • MGTH501--acgwAdminStateChange • MGTH600--acEnhancedBITStatus • MGTH601--dsx1LineStatusChange • MGTH800--acPerformanceMonitoringThresholdCrossing
Client Session Monitor Security logs (new)	N/A	Feature A00009822 (PT-AAL1, PT-IP, UA-AAL1, UA-IP, PT-AAL2) logs the interaction with Client Session Monitor. The following security INFO logs are generated when the Client Session Monitor processes the notification of the authentication and client lifetime events: • User authenticated. • Successful session start. • Session stopped due to user exit. • Active session manually marked as done. • Client start or stop event is requested, but session ID is not valid.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Security logs on SSPFS	(refer to the next column)	Feature A00009823 (UA-IP) adds security logging to the SSPFS CLI scripts. Security logs are to be generated whenever any security affecting parameter is changed from the CLI. The following events are logged: • Login Retries Limit--whenever an MSAP access threshold is changed. • Login Session (User Inactivity) Timeout--whenever an MSAP time interval that controls keyboard lockout is changed. • User Termination Timeout--whenever an MSAP time interval that controls keyboard lockout is changed. • User Reauthentication Disable Timeout--whenever an MSAP time interval that controls keyboard lockout is changed. • Login Session Master Server--whenever an MSAP time interval that controls keyboard lockout is changed. • Socks Security Service--whenever changes to MSAP security profiles and attributes occurs. • IEMS Server IP address--whenever changes to MSAP security profiles and attributes occurs. • Default PAM--whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs. • Radius PAM--whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs.
IEMS northbound SCC2 log feed (changed)	All Logs in the SCC2 stream	CR Q01091683 in SN09 has changed the IEMS SCC2 northbound log stream to the OSS. This change affects only the Start of Log delimiter. Previously, the Start of Log delimiter was just a carriage return (0D in hexidecimal). With this CR implementation, the Start of Log string has been changed to be a line feed followed by a carriage return. (0A0D in hexidecimal). This change has been patched back to SN08 via CR Q01091683-01 and to SN07 as well via CR Q01091683-02.
IEMS logs (changed)	IEMS350 IEMS650	Per CR Q01137225, these logs are as follows: • IEMS350 indicates that an IEMS device is changed to an unmanaged state by the user. • IEMS650 indicates that an IEMS device is changed to a managed state by the user.

Summary of new or changed Logs/Faults for (I)SN09

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Product = MG 9000		
ATM50 alarm (changed) NE305 log	Hardware Port Unstable	Feature A00008969 (UA-AAL1, UA-IP) describes this alarm that is raised if the SSI (Signal State Interrupt) count gets too high. The alarm is reported as an NE305 log, which is changed to allow a new or additional reason code.
MG9K EM Line Circuit Enhancements (changed)	N/A	Feature A00009280 (UA-IP, UA-AAL1) provides the following enhancements. • adds a color indication for alarms on the port ilog of the Card Display. • allows the user to manually mark a port as faulty. • adds a color indication for a faulty port on the port ilog of the Card Display. • displays the directory number in the LineCircuit view. • displays the directory number at the Alarm Browser screen for alarms reported and adds the associated directory number in the line circuit alarm log. • adds Circuit Listing at the NE desktop level to list the faulty ports.
Product = Network Patch Manager (NPM)		
PATC log (new)	PATC300	Feature A00009227 (PT-IP, UA-IP, IAC, IAW, UA-AAL1) creates this new major alarm and log to indicate when a restart is required for a patch on a specific card. PATC300 is generated when a patchAlarmFault is received from an MG9000 DCC card. The PATCxxx alarm is viewed from the MG9000, not the NPM.
Product = SAM21		
SCU log (changed)	SCU350	Per CR Q01088284, the SCU350 log is changed so that the Category field correctly reflects the proper value of Environmental.

Data Schema/MIBs changes overview

The following Data Schema tables or MIBs are new or changed for (I)SN09. More complete descriptions will appear in the Feature Deltas section of this document.

Summary of new/changed Data Schema/MIBs information for (I)SN09

Table or MIB name	New or changed	Description
Product = Call Server 2000		
GWC-MIDDLE-BOX-MIB GWC-MEDIA-PROXY-MIB	Changed	Feature A00007217 (CHS) modifies the following MIBs: • GWC-MIDDLE-BOX-MIB adds two new fields: — The **MiddleBoxMPGroupId** field is used to identify the preferred MediaProxyGroup for the middle box. The value of this field is used to index into the MediaProxyGroup table on the GWC. — The **MiddleBoxVpnGID** field represents a global Identifier indicating the VPN that the MiddleBox is part of (applies to NATs only). • GWC-MEDIA-PROXY-MIB adds two new fields: — The **MediaProxyInGWCGroup** field is used to indicate whether or not the Media proxy has been provisioned as a media Proxy on the GWC. — **MediaProxyGlobalID**--This field represents a unique global ID for a specific MediaProxy within the system. — There is also a new table added to the GWC-MEDIA-PROXY-MIB. This is a new table to convey MediaProxy Group Data to the GWC.
IPAPPL	Changed	Feature A00007544 (PT-IP, CHS, Int'l PT-IP) modifies table IPAPPL by adding entry NMS under subfield SERVICE in the OPT field.
MSGRTE	Changed	Feature A00007544 (PT-IP, CHS, Int'l PT-IP) modifies table MSGRTE by adding new selector SCTP under subfield MSGRTE_SEL in the MSGRTRES field.

Summary of new/changed Data Schema/MIBs information for (I)SN09

Table or MIB name	New or changed	Description
SERVRINV LGRPINV	Changed	Feature A00008522 (UA-IP, MCS) modifies the following tables: • SERVRINV--In SN09, the field TERM_EXEC_TC_TAB of the table SERVRINV includes DPLEX with a DLP termtype for GWCs defined with Large_LineNA_v2 and Large_LineINTL_v2 GWC profiles. • LGRPINV--In SN09, the field GRPTYPE of the table LGRPINV is set to “SSDPL” for SIP; logical groups will be used to indicate that the logical group is assigned to a CS2K SS gateway.
SERVRINV LGRPINV IPAPPL IBNFEAT	Changed	A00008556 (CHS) modifies the following tables: • LGRPINV adds new entry SSDPL in field GRPTYPE to support DPL agents. • IPAPPL adds new entry SIPMTC to the option list under Subfield Application in field OPTS. • IBNFEAT is enhanced as follows to support a new feature DPL which will convert the IBN line into a DPL line: — Fields DF and Feature add a new entry, DPL, to be assigned to an IBN line. — The DATA field adds new subfield SIP with a Y/N entry to identify a SIP line. — The DATA field adds new subfield MAX_NUM_ CALLS to specify the maximum simultaneous call appearances. — The DATA field adds new subfield ALLOW_BSY_ TERM to determine whether or not a busy SIP line can take an additional call termination.
MNIPPARM	Changed	Feature A00008601 (PT-IP) modifies table MNIPPARM as follows: • Field DFCODEC adds entry G729. • Field PRFCODEC adds entries G711ALAW and G711ULAW.

Summary of new/changed Data Schema/MIBs information for (I)SN09

Table or MIB name	New or changed	Description
NETBRDGE MNCKTPAK MNATMIF	Changed	Feature A00008629 (PT-IP,PT-AAL1) modifies the following tables: • NETBRDGE modifies field BEARNETS to allow selection of the two interfacing network types. For AAL2 IW-SPM, this would be TDM_ENET to NET_AAL2. • MNCKTPAK modifies the PEC field to specify the new GEM-II pack that can operate as AAL2 (for ATM RM) or IP (for GEM RM). It also modifies field LOAD to select a valid tuple from table PMLOADS. New AL2nnnn load for AAL2 ATM, or new GM2nnnn load for IP GEM. • MNATMIF adds AAL2 ATM protocol parameters: — CIDPRSVC specifies the maximum number of AAL2 CIDs that may be allocated on an AAL2 SVC. — PRECREAT specifies whether Pre-creation of SVCs is enabled. — TIMERCU sets the maximum period of time in usec (micro seconds) before a partially filled AAL2 packet is scheduled for transmission. — SVCHOLD sets the length of time that an AAL2 SVC is kept up after the last narrowband call to use it has been deleted. — SRVCAT is the ATM Service Category for SVC. Default is VBR. — PKCLRT sets the peak cell rate of the ATM connection on a per SVC basis. — SUSTCR sets the sustained cell rate of the ATM connection on a per SVC basis. — MAXBURSZ sets the maximum burst size of the ATM connection on a per SVC basis. — REMADDR is the ATM address of the node that may be reached. — CODEC sets the type of on-board CODEC in-use. — SILSUP enables silence suppression. — MAXBRI sets the max number of bridges provided by an AAL2 IW.

Summary of new/changed Data Schema/MIBs information for (I)SN09

Table or MIB name	New or changed	Description
(continued) MNMGPIP MNIPPARM	Changed	(continued) Feature A00008629 (PT-IP,PT-AAL1) modifies the following tables: • MNMGPIP modifies the GEMSIGIP, SIGMASK, and SIGGWIP fields to allow those fields for AAL2 IW-SPM. • MNIPPARM modifies the DIFFSERV field to allow this field for AAL2 IW-SPM.
HOMELRN	Changed	Feature A00009036 (UA-IP) enhances the maximum limit for SITE names per HOMELRN entry from 10 to 256.
SCAICOMS	Changed	Feature A00009078 (UA-IP, UA-AAL1, DMS) modifies this table by adding a prompt for a second IP address in the IPADDR field to support another TCP/IP link within an existing linkset. If only one IP address is needed the second prompt for IP address should be cancelled by typing in a $.
ACDGRP ACDSGRP ACDLOGIN ACDENLOG ACDMISPL		Feature A00009085 (PT-AAL1, PT-IP, DMS) expands the maximum size of the following tables: • ACDGRP increases from 1,024 to 5,000 tuples • ACDSGRP is modified to allow provisioning of a maximum of 2,500 sub-groups per ACD group compared to 256 currently. • ACDLOGIN increases to 99,999 tuples. • ACDENLOG increases to 99,999 tuples per partition. Also, ACDMISPL modifies the existing field PROTOCOL to add a new value BCS57.
VEONAME	New	Feature A00009091 (PT-AAL1, PT-IP, DMS) creates this table to hold the list of VEO names. Each name represents a virtual end office that is partitioned on the DMS100/CS2000.
XLAPLAN CXGRP	Changed	Feature A00009091 (PT-AAL1, PT-IP, DMS) modifies tables XLAPLAN and CXGRP to add new option VEONAME which provides an association between the originating line/trunk agent, or PX trunk agent, and the Virtual End Office (VEO). This provides the flexibility to partition the DMS100/CS2000 into multiple virtual end offices.

Summary of new/changed Data Schema/MIBs information for (I)SN09

Table or MIB name	New or changed	Description
LPICPXLA	New	Feature A00009091 (PT-AAL1, PT-IP, DMS) creates this table to provision a list of NPANXX codes to be excluded from LPIC routing on per VEO basis. This table will be implemented using digilators for storing the NPNXX Codes and will be using 1 digilator pool of 32k 1-digits blocks.
TRKGRP	Changed	Feature A00009153 (CHS) modifies table TRKGRP to allow use of the existing MRLT option to provision RLT capability for H.323 trunk groups.
C7UPTMR TRKSGRP	New	Feature A00009190 (UA-IP) modifies C7UPTMR to support provisioning of timers for the UCP protocol. It also modifies TRKSGRP to change the TMRNAME field to the datafilled C7UPTMR index.
(refer to description)	New	Feature A00009375 & 9376 (CHS) creates two areas in the Windows Registry for the storage of information relating to status of installed patches and maintenance releases on this node: • hklm\system\currentcontrolset\services\cxipboot\data\patches is a storage area for patch information. • hklm\system\currentcontrolset\services\cxipboot\data\upgrade is a storage area for maintenance release information.
Product = CS 2000 Management Tools		
GWCEM.GWDOMAIN GWCEM.GLOBALIDS	New	Feature A00009189 (IAW, IAC) creates the following new MIBs: • GWCEM.GWDOMAIN stores the provisioned gateway domain name • GWCEM.GLOBALIDS stores the global id of different devices.

Summary of new/changed Data Schema/MIBs information for (I)SN09

Table or MIB name	New or changed	Description
GWC-GW-MIB GWC-ENDPOINT-MIB GWC-EPID-GRP-MIB GWC-RMGC-MIB GWCEM.GATEWAY GWCEM.GATEWAYPROFILE GWCEM.GWROOTITRANSMIDDLEBOXES	New	Feature A00009189 (IAW, IAC) modifies the following MIBs: • GWC-GW-MIB--From SN09,GWC will replace this MIB with the new table gateWayTableV2 to do corresponding SNMP operations. The new table expands gateWayName size to 64 characters, adds 32 bits gateWayID, and removes useless columns gateWayHeartBeat and gateWayConnset. • GWC-ENDPOINT-MIB--From SN09,GWC will replace this MIB with the new table endPointTableV2 to do corresponding SNMP operations. In the new table, epidGWID replaces endPointGW in V2 table. • GWC-EPID-GRP-MIB--From SN09,GWC will replace this MIB with the new table epidGrpTableV2 to do corresponding SNMP operations. In the new table, epidGrpGWID replaces gatewayName in V2 table. • GWC-RMGC-MIB--From SN09,GWC will replace this MIB with the new table gwToGwcTableV2 to do SNMP operations. In the new table, gwFQDNV2 is expanded to 64 characters. • GWCEM.GATEWAY--The GATEWAYNAME field is expanded to 64 characters, and a new GATEWAYINDEX field is added. • GWCEM.GATEWAYPROFILE--New field FQDN_SUPPORTED is added. • GWCEM.GWROOTITRANSMIDDLEBOXES--The GATEWAYNAME field is expanded to 64 characters
LGRP_TYPE field added to GW profiles	Changed	Feature A00011746 (UA-IP) introduces a new optional field that is included in the profiles certificate. The LGRPType field is introduced and is used to drive “core” datafill for table LGRPINV. As suggested from the core table datafilled, LGRPINV, this field is only applicable for line gateways and is therefore optional in the XML document certificate. Even though this is an optional certificate field, this field is mandatory for all profiles that generate LGPRs.
Product = CS 2000 TOPS		

Summary of new/changed Data Schema/MIBs information for (I)SN09

Table or MIB name	New or changed	Description
XPMIPMAP	Changed	Feature A00009011 (PT-AAL1, PT-IP,DMS) adds a new field, SNMP, which indicates whether SNMP is enabled on the IP-XPM. If SNMP is enabled, the craftsperson must also datafill an SNMP community name in new subfield COMMNAME.
OAFUNDEF	Changed	Feature A00009012 (PT-AAL1, PT-IP,DMS) modifies this table as follows: • Field FUNCAREA adds new subfield USESERV to ensure the service datafilled in field ORIGSERV of OAFUNDEF is used when transferring or triggering to the function. • Field FUNCAREA adds new subfield DARECALL. If Y, the call going to the function is a DA recall and the switch will increment the DA recall counter and set operator indicators for recall if going to an operator. • Subfield AUTOSYS adds new entry MCCS.
TOPSFTR	Changed	Feature A00009012 (PT-AAL1, PT-IP, DMS) modifies table TOPSFTR by adding OSSAIN_ENHANCEMENTS_22 to the range which activates transfer to SN function service and DA Recall function.
ANNMEMS	Changed	Per feature A00009013 (PT-IP, DMS), packet members cannot be datafilled for a custom announcements of type TOPSVR or MDS. Also, note that for custom announcement members with hardware type UAS, the PHLSTIDX field is ignored. This field is present for all members datafilled with HDWTYPE UAS, but it is consulted only if the announcement CLLI is datafilled as STND in table ANNS.
ANNPHLST	Changed	Feature A00009013 (PT-IP, DMS) updates the explanations and example datafill for custom announcement types MCCS and ACTS to correct errors and to document that these applications can use either DRAM or packet announcement resources. Also, the information about custom announcement type AOSSVR was removed in SN09. This application was specific to TOPS MP positions, which are no longer supported.

Commands and User Interface changes overview

The following Commands and/or User Interface are new or changed for (I)SN09. More complete descriptions appear in the Feature Deltas section of this document.

Affected Area	Command/User Interface Description
Product = CS 2000	
CS2K Configuration Management Tools GUI (new GUIs added)	Feature A00007217 (CHS) creates the following new GUIs: • Add Media Proxy Group dialog--used to create a new group containing a subset of the Media Proxies on the system. The group can then be allocated to an ITRANs middlebox and in turn associated with a gateway. When this happens, the GWC for the gateway is provisioned with details of the media proxies in the group. • Change Media Proxy Group Dialog--used to change the number of media proxies in the group (subject to the maximum limit). Also used to replace one or more of the media proxies in the group with another. • Media Proxies Description Dialog--used to provide more information on a specific media proxy group without having to navigate to the gateway controller GUI or the media proxy group GUI. • Media Proxy Groups Tab--used for display purposes and to provide a central point of access for all Media Proxy Group operations; shows a list of Media Proxy Groups along with a comma separated list of the Media Proxies belonging to that group. • Media Proxy Groups Description--used to provide more information on a specific media proxy group without having to navigate to the gateway controller GUI or the media proxy GUI. • NAT Details--replaces existing dialogs to display the GWC ID and GW information for Zones. Adds a new details button to the network zone panels and removes the Display ID and Retrieve GW buttons. Clicking the details button displays the details dialog to display the GWC NAT ID and the gateway report. These options are available if the user selected a specific Network Zone. • NAT VPN Details----shows a table containing all VPNs and the NATs which make them up. An add and delete button is included to allow the user to manage the VPNs. • Add VPN Dialog----a new dialog box used when a new VPN is being created. The dialog contains a text box in which the user adds a new VPN name. On clicking the OK button the VPN is created but is not assigned to any NAT. The new VPN will automatically be added to the VPN combo box on the addnat dialog. The dialog allows the user to optionally specify a shared global ID for that VPN, used where the VPN may span several CS2Ms.

Affected Area	Command/User Interface Description
CS2K Configuration Management Tools GUI (changed)	Feature A00007217 (CHS) modifies the following GUIs: • Media Proxies Tab--modified to contain two sub-tabbed panels. The first sub tab contains the content of the original media proxy tabbed panel. The second sub panel contains the new Media Proxy Groups tabbed panel. • Add Nat Dialog--modified to add the media proxy group combo box, along with the Use VPN checkbox, VPN combo box, and create vpn button. • NAT Middlebox Panel--adds two new fields. The first displays any selected Media Proxy Group name and the second any chosen VPN name. Two new buttons have also been added to the panel. The first, called “VPN” is the link the VPN details dialog. This displays details of the VPNs. The “details” button is the replacement for the buttons to display the zone ID and the gateway report. • Change Nat Dialog--modified to add the media proxy group combo box, along with the Use VPN checkbox, VPN combo box, and create vpn button. • NAT GWCID Details---displays the NAT ID in the GWC. This is existing functionality which has been included in the details dialog. • NAT GW Report Details---now part of the NAT details dialog, it contains the gateway report table that was previously in its own dialog. • GWC Media Proxies Tab---contains the list of media proxies that are provisioned on a GWC. New group information has been added.

Affected Area	Command/User Interface Description
XML Commands for Media Proxy Groups (new)	Feature A00007217 (CHS) creates the following new interfaces to manage Media Proxy Groups: • Add Media Proxy Group - Add a new Media Proxy Group and the Media Proxies associated with that group. • Query Media Proxy Group. - There are three types of query: — List all the Media Proxies within a Media Proxy Group. — List all Media Proxy Groups assigned against a Gateway Controller. — List all the Media Proxy Groups that a Media Proxy belongs to. • Change Media Proxy Group - Modify the list of Media Proxies assigned to a group. • Delete Media Proxy Group - Delete a Media Proxy group. • Add VPN - Add a new VPN with the specified name. • Delete VPN - Delete a VPN from the list of VPNs. • Query VPN - Returns a list of VPNs and the NATs that are in each VPN.
XML Commands for Media Proxy Groups (changed)	Feature A00007217 (CHS) modifies the following interfaces to make use of Media Proxy Groups: • Add Network Zone - When a Network zone is created, allow it to be optionally associated with a Media Proxy group and/or a VPN. This requires changes to Add Nat and add LBL. • Add NAT - When a Nat middlebox is created, allow it to be optionally associated with a Media Proxy group and/or A VPN. • Add LBL - When a LBL middlebox is created, allow it to be optionally associated with a Media Proxy group. • Query Network Zone - Extend the query to return the Media Proxy group and VPN. • Query Nat - Extend the query to return the Media Proxy group and VPN. • Query LBL - Extend the query to return the Media Proxy group. • Change Network Zone - Change the Media Proxy group and/or VPN assigned to a middlebox. • Change NAT - Change the Media Proxy group and/or VPN assigned to a middlebox. • Change LBL - Change the Media Proxy group assigned to a middlebox.

Affected Area	Command/User Interface Description
Remote SIP Server (changed)	Feature A00007269 (PT-IP) enhances the backup functionality provided by the NGSS Session Server for SN09 including a mechanism for the customer to change the backup time.
Remote SIP Server (changed)	Feature A00007544 (PT-IP, CHS, Int'l PT-IP) modifies this GUI to add a "Select the Server Type" option. If the Server Type = Message Server, a SUBSCRIBE message will be sent out to the Remote Server.
Config Data (changed)	Feature A00007544 (PT-IP, CHS, Int'l PT-IP) modifies this GUI to add a "subsRetryTmr" option, with a range of 0 to 50000 milliseconds. If subsRetryTmr = 0, SUBSCRIBE will not be retried.
Add NCAS Link List NCAS Link NCAS Link Add VM Profile List VM Profile (new)	Feature A00007544 (PT-IP, CHS, Int'l PT-IP) creates the following GUIs: • Add NCAS Link--allows the user to add NCAS link datafill for each application, such as Message Waiting. • List NCAS Link--displays currently datafilled NCAS links on the NGSS. • NCAS Link--indicates the status of the link and allowed operations. • Add VM Profile--allows the user to add voice mail profiles related to remote SIP servers. • List VM Profile--displays current voice mail profiles.
QSIP command (new)	A00008556 (CHS) creates the QSIP command at the CI level to query the CS2KSS to get the SIP information. QSIP query takes place through the NCAS link. Hence, the command response depends upon the availability of the NCAS link.
IWCOMM CI (changed)	Feature A00008629 (PT-IP,PT-AAL1) modifies commands BSY_IW and RTS_IW to remove the "Bridging type" parameter. The system will now rely on the setting in MNNODE's BEARCLLI field to determine if the IW-SPM is ATM AAL1, ATM AAL2, or IP.
N905 GWC Profiles SOS CI (new)	Feature A00008916 (PT-IP, UA-IP, IAC) increases capacity for small and large line gateway profiles and combines line and trunk profiles into one profile. These new profiles are only compatible with N905 GWC hardware.
SOS CI (new)	Feature A00009129 (PT-IP, Int'l PT-IP) creates a new SOS CI called CMREXFUL to allow setting the day the full REX will occur.
SOS CAPCI (changed)	Feature A00009129 (PT-IP, Int'l PT-IP) modifies the SOS CAPCI output to reflect either a warm or hot sync state.

Affected Area	Command/User Interface Description
MWTSwap command (new)	Feature A00009200 (PT-IP) creates new command, MWTSwap, from the MAPCI TTP interface, available only on the Succession CS2K & Compact CS2K platforms. The hardware required to perform the test will reside in the AudioCodes Media Server 2000 Series products. The MWTSwap command appears on the TTP level screen only when the office parameter EXTERNAL_GATEWAY_TEST_LINES is set to 'Y' in table OFCVAR. This office parameter determines which test head will be used for hardware based TTP/ATT level trunk testing. The default is 'N' which indicates that tests will use the existing hardware located in the ISM/MTM peripheral. When set to 'Y', all testing currently supported will be performed via the AudioCodes Media Server (AMS) 2000 series products.
CAPCI CI command (changed)	Feature A00009204 (PT-IP) modifies this command to support the SOS Call Agent blade.
CAPACITY MAPCI level (changed)	Feature A00009204 (PT-IP) modifies the output at this level to match the CAPCI CI command.
CS2000 Session Server Tomcat Web Server (changed)	Feature A00009235 (PT-IP) changes this GUI as follows (refer to the CN section of this feature for details on new fields and other changes): • Additions to the Security configuration parameters web page with new parameters • Modification of an existing parameter to the security configuration parameters web page.
MG9K EM Line Circuit Enhancements (changed)	Feature A00009280 (PT-IP) modifies the following GUIs: • Line Card View (WLC, XDSL, GLC, SAA) -- the line card view displays alarm color indications for the ports. A faulty port is indicated with magenta color on the line card view. Display of only voice circuit ilogs changes on a XDSL view for faulty ports. • Line Circuit View -- allows the user to mark a port as faulty with a prerequisite that the port is locked. The faulty combo box is available in the "Circuit Status" section of the Line Circuit View. The Line Circuit View also displays the directory number (DN) associated with a termination point (line circuit), displayed inthe "Circuit Provisioning" section of the Line Circuit View. • Faulty Circuit Listing View -- this GUI is added to a new menu item on the Service menu option, on the NE desktop view. It lists all the ports manually marked as faulty by the User on an NE along with their location information and has a Refresh button available.

Affected Area	Command/User Interface Description
Backup configuration (new)	Feature A00009311 (UA-IP) provides users with an option that can be invoked through the “Backup Configuration” in SSPFS CLI called “***Copy last Oracle backup to DVD or tape”.*** This option will copy the last good Oracle backup from the “Synchronized Backup Manager” and burn it to DVD or tape. The “Synchronized Backup Manager” has its own scheduler for backing up the critical data at scheduled intervals and writes to disk.
SSPFS upgrade with ESD (changed)	Feature A00009313 (UA-IP) modifies the ESD upgrade process by removing the prompt to insert disks. The user will be prompted to upgrade the CBM application.
CS2M GUI (changed)	Feature A00009332 (PT-AAL1, PT-IP, UA-IP, Int’l UA-IP) makes the following changes to the CS2M GUI: • Add Network Profile Dialog lists 8 new codecs available, of which the customer may choose up to 3. • Change Network Profile Dialog allows the customer to select from eleven codecs. • Add P-time Dialog now allows the customer to select from 4 p-times instead of 2. The new P-times are p30ms and p40ms.
NGSS provisioning (changed)	Feature A00009443 (PT-IP, CHS) makes the following changes: • A new boolean provisioning flag **T.38 Annex D Supported** is added to the NGSS option list on the remote server provisioning web page to indicate that the remote server supports T.38 Annex D. • A new boolean provisioning flag **Re-Invite for Voice Band Data** is added to the NGSS option list on the remote server provisioning web page to prevent automatic upspeed from G729 to G711 by 248 PVG on fax detection as is the default PVG behavior. This flag has to be set to ‘Y’ to enable this functionality. It has no effect on non-PVG gateways.
CBM support of Centralized AAA (changed)	Feature A00009463 (PT-AAL1, PT-IP,DMS) provides the CBM capability to support Centralized Authentication, Authorization, Administration (AAA) with the Integrated Element Management System (IEMS). This feature activates PAM, RADIUS, PAM-MKHOMEDIR, NSS-SAML and SAML modules to enable integration of CBM with the IEMS and SAML, in order to allow the use of Centralized AAA.
SecuConf menu of sdmmtc (changed)	Feature A00009470 (UA-IP) enhances the SecuConf menu under sdmmtc to enable SAML client configuration.
deleteIEMSLocalEntry (new)	Feature A00009470 (UA-IP) creates new command deleteIEMSLocalEntry so the administrator can clean up the /etc/passwd file after an SN08 SDM with IEMS as the central server is upgraded to SN09 SDM software. This command is not needed when an SDM with IEMS configuration is upgraded from SN09 or newer releases.

Affected Area	Command/User Interface Description
enableIEMSUser, disableIEMSUser (deleted)	Feature A00009470 (UA-IP) deletes these two commands for SN09.
Session Server Manager link (changed)	Feature A00009514 (PT-IP, IAC, CHS) modifes the following GUIs. • NOA/NPI/PC section menu provides access to Add Mapping, Delete Mapping and List Mappings menu options • Add/Delete NOA, List NOA and NOA/NPI/PC Mapping menu options • SIP Gateway to display the Remote SIP Servr section menu options, including Add Server, List Servers, Modify Server
Post command under MAPCI TTP level (changed)	Feature A00009520 (PT-AAL1, UA-IP) creates new post type "I" and enhances the existing post command under MAPCI TTP level to provide the following functions: • Busy a specific trunk group on an individual MG4K-ATM gateway • Busy a specific trunk group on an individual GWC
CS2M Provisioning GUI (changed)	Feature A00009530 (CHS) modifies the CS2M GUI to allow the provisioning of adjacent Network Zones against the Audiocodes GW. This is done by enabling existing functionality currently supported for small line and H.323 type GWs.
CBM SIM functionality integrated into NPM (changed)	Feature A00009550 (PT-IP, UA-AAL1, DMS) integrates the CBM SIM functionality into NPM and supports a single patch manager for the whole network to administer software updates for TDM/Wireless and Succession configurations. The NPM user interface is utilized as a central location for administering all software updates. For SSPFS based patches, the NPM is used in TDM/Wireless and Succession configurations for patch maintenance and administration. Also, for Core Element (CEM) based applications delivered with CBM, NPM is used for patch maintenance and administration.
Client Session Monitor GUI (new)	Feature A00009822 (PT-AAL1, PT-IP, UA-AAL1, UA-IP, PT-AAL2) creates the Client Session Monitor GUI which provides a report that will give the security user the ability to view the historical client sessions for the users. The report will by default populate with the currently active sessions. However, the user has the ability to configure the display criteria. The report will refresh the displayed contents once every 60 seconds.
ESUP GUI (changed)	Feature A00009839 (PT-AAL1) intoduces a new screen at the begining just **before** the existing screen where ESUP asks for media type. The new screen prompts the user for "Upgrade type" with options of "Upgrade to a higher release" or "Patch only upgrade."

Affected Area	Command/User Interface Description
SSPFS CLI tool (changed)	Feature A00009840 (PT-AAL1) provides an easy-to-use IPSec configuration interface on the CBM for configuring IPSec/IKE parameters, bundled as part of CLI tool of SSPFS for all SSPFS profiles. This interface can be accessed only by the root user and accepts user input values for various parameters related to the IPSec and IKE configurations.
SVCNTRL (new)	Feature A00010303 (DMS) creates this directory and command. On entering command SVCNTRL, the user should enter one of the two options; i.e. either query a service or update a service. For Query, the further options are the DN, the feature/service and the attribute to be queried. For Update, the further options are the DN, the feature/service and the attribute, and the attribute parameter to be updated.
MCS GUIs (changed)	Feature A00012001 (UA-IP) provides for the rebranding and proxying of the MCS GUI's through the IEMS. The Media Proxy NE type has been changed to Media Portal. The functionality of handling faults and provisioning data remains unchanged. When adding the SSLines device, an SSLines Mgr is added instead of an MCS Mgr or RTP Media Portal.
Remote backup configuration tool (new)	Feature A00012210 (UA-IP) provides a remote backup configuration tool to set the necessary parameters and schedule for automatic backup. These backups can be scheduled to automatically occur from once a day to four times per day. Users will be able to enter up to four times of their choice for the automatic backup to occur. This tool also provides a facility for manually initiating a backup and monitoring its progress. Each remote backup session will provide detailed logs of that session.
MDN and PIC (changed)	Per CR Q01151441, Line options PIC, LPIC and/or INTPIC, if present on the PRIMARY member of the MADN group, will be added to non-primary members within the NEW command only. If the MDN option as well as the PIC, LPIC and/or INTPIC option(s) are present within the same NEW command for non-primary members, the PIC options within the command take precendence over the primary member values (if they exist on the primary). MDN EXB is not supported.
Product = CS 2000 Management Tools	
CS2K Mgmnt Tools GUI (new)	Feature A00008522 (UA-IP, MCS) adds the following new GUIs: • When you select View Current Audits from the Maintenance menu of the CS2MT GUI, a new function and panel of "Abort Audit" becomes available. • Line Data Integrity Audit--In the CS2MT GUI -> Maintenance -> Audit System -> Line Data Integrity Audit, the new "Run Audit" GUI provides support for running line audits per GWCs, GWs or LGRPs.

Affected Area	Command/User Interface Description
CS2K Mgmnt Tools GUI (changed)	Feature A00008522 (UA-IP, MCS) modifies the following GUIs: • Associate Gateway--If you select the MSM profile from the Gateway profile name list, a Multi-Site Selection panel appears. New fields on that panel are Site Names (from table SITE in the CM) and Selected Site Names. • Change Gateway--modified to show a different GUI if an MSM gateway is selected. The panel presents Available Site Names on the left, and Provisioned LGRPs on the right. The user can add or remove site names. • Run Audit--shows the process of the running audit.
GWCEM GUI (changed)	• Feature A00009189 (IAW, IAC) adds new optional field "Gateway default domain name" in the Add GWC node GUI. The name (or Not Configured) appears on the right bottom corner of the GWC Provisioning panel.
QGW command (new)	Feature A00009189 (IAW, IAC) creates the Query Gateway Tool (QGW) to output all the LENs and Endpoints for the specified Gateway in table LNENDPT. To use the command, enter the QGW command at the CM CI prompt, followed by a string denoting the Gateway name.
QGW command (changed)	Feature A00009189 (IAW, IAC) modifies the follow XML commands to allow users to input either the gateway host name only or the full FQDN name: • The Add GWC command adds new parameter "gwDefaultDomainName." • disAssocMG accepts either input when the user wants to delete the gateway from the system. • Change MG accepts either input. • The QueryGWC response now includes the gateway domain name.
SSPFS CLUI access restrictions (new)	Feature A00009310 (UA-IP) creates a restricted access shell for non-administrative CLUI functions on the SSPFS platform. It is expected that customers will use this environment when giving users access to CLUIs residing on SSPFS servers. The users will have a restricted command set and shell environment.
CS2K Mgmnt Tools GUI (changed)	Feature A00009339 (IAC) modifies this GUI as follows: • When adding a new network profile, the user can choose from one of three T.38 options currently provided. “Disabled” is changed to “Off,” and “Enabled” is changed to “On (Strict).” The “Loose” option is used for packet cable. • The “DS field” is changed to “DSCP (6-bit binary)” to avoid any confusion between the 6-bit DSCP and an 8-bit DS Field value. On the “Change DQoS Configuration” dialog GUI, the “DSCP (6-bit binary)” field will be added.

Affected Area	Command/User Interface Description
CS2K Audit GUIs (new one added)	Feature A00009890 (CHS) adds the following panel to the CS2K Audit GUIs to allow the user to audit the Session Server (MCSEM) provisioning data: • CS2K Data Integrity Audit Configuration--This GUI allows the user to selectively run the existing CS2K data integrity audit, the new CS2K SIP Media Proxy Data Integrity Audit or both audit components. The GUI is accessed from the Audit System GUI upon selecting the “CS2K Data Integrity Audit” and pressing the “Run Audit” button.
CS2K Audit GUIs (changed)	Feature A00009890 (CHS) modifies the CS2K Audit GUIs to allow the user to audit the Session Server (MCSEM) provisioning data, as follows: • Audit System--when selecting the “CS2K Data Integrity Audit” from the pull down selector, the Audit Description text is enhanced to describe the introduction of new audit functionality related to the audit of IP-VPN(NAT) Zones data fill against the Session Server (MCSEM). • CS2K Data Integrity Audit Report--additional problem types are added that will be detected by the “SIP Media Proxy Data Integrity Audit”. These new problem types will be displayed using the existing mechanism and appropriate Actions will be available via the Actions selector to correct the issues.
SESM GUI (new options added)	Feature A00010617 (IAW, IAC) modifies the SESM GUI as follows: • When associating a media gateway using SESM GUI, in the “Gateway Profile Name” pull down list, two new profile names appear: NUERA_BTX4K and MGCP_IAD_40. • After the introduction of the NUERA_BTX4K certificate/profile, when adding a carrier using the SESM GUI, in the “Add Carrier” dialog box, the following carrier name format can be specified in the “Carrier name” field: ds/ds3-<u1>/ds1-<u2>
Product = CS 2000 TOPS	
TST command (changed)	Feature A00009012 (PT-AAL1, PT-IP,DMS) modifies the functionality of the command and provides one new response message: • When TST is entered for a node, a ping is no longer sent. For OSN however, the Node Connectivity Test message is now sent to the OSN node in place of the ping to verify connectivity. • When TST PING is entered for a node on a platform that does not support ping from SOS, the following new response message is provided: “Use TST without PING.”
Product = Integrated EMS	

Affected Area	Command/User Interface Description
IEMS lockout timer (changed)	Feature A00009289 (UA-IP) modifies the existing locking of the IEMS client as follows: • adds ability to change timeout value without requiring a restart of the server. • adds successive failed attempt lockout functionality to prevent multiple, rapid attempts to guess a password and unlock the client. • removes ability for the user to disable the client lockout.
Configuring Custom View Scope (changed)	Feature A00009292 (UA-IP, UA-AAL1) modifies the Security Administration tool of Integrated EMS such that using the Custom View Scope, rules can be set to customize the view per the customer's requirement. Rules can be set at various levels which allow filtering at different levels: • Topology • Events • Alerts • Inventory • Stats Admin
Launch Remote Ping Launch Remote Trace Route (new)	Feature A00009320 (UA-IP) provides a centralized, graphical user interface on IEMS to allow users to launch ping and traceroute operations remotely on the Gateway Controller (GWC) and SSPFS platforms; including IEMS, CMT, MG9K Manager and CBM. This feature is accessed from the drop-down menu available when the a GWC or SSPFS unit managed object is right-clicked. Two new menu items have been added to the list: Launch Remote Ping, and Launch Remote Trace Route.
Server Security Manager Launch (new)	Feature A00009532 (UA-IP) enables host-to-host IPSec between SSPFS servers. Within IEMS, a new security item under Tools is now available to launch the Server Security Manager. The web site brings up two tables representing currently provisioned security parameters. One for IPSec parameters and one for IKE parameters. Options to add and delete entries are available. Adding entries will be performed using HTML forms. Primary usage of this interface in SN09 is to secure the communications channel between SSPFS server application such as IEMS and an OSS.
UNEM browser launch (new)	Feature A00009611 (UA-IP) adds the following capabilities: • launching the UNEM browser • launching applications for UMUX NEs • adding a UMUX network element manager (UNEM) • adding UMUX NEs
Proxied command line in IEMS (changed)	Feature A00009612 (UA-IP) restores the proxied "Command Line" context menu item used in IEMS.

Affected Area	Command/User Interface Description
MG 3200 added in IEMS GUI (new)	Feature A00009777 (UA-IP) enables provisioning the MG 3200 Network Element in IEMS from the existing Tools-->Add-->EMS / NE menu. In the initial screen, the “IP Address” field represents the IP of the MG 3200 device to be added, “Type” represents whether it is a EMS or NE (in our case it is “NE”), “Device Type” represents the name of the device to be added (in our case it is “MG 3200"), “Device Version” represents the version of device (in our case it is “9.0”) to be added and the “Web Username and Web Password” are the username and password that are needed for the configuration tool. The subsequent screens get all the necessary SNMP interface details that are needed for fault and performance. IEMS supports only SNMP “v1” and “v2c” versions of MG 3200 not “v3” version. This feature also adds IPSec and IKE configuration capabilities to the MG 3200 node configuration tool. “IPSec and IKE Config Tool” will be available on the right click of the MG 3200 Map Symbol. Clicking opens a panel over which the IPSec Configuration frame is embedded.
MG 3200 configure INI Backup (new)	Feature A00009777 (UA-IP) creates a new menu item on the MG 200 right-click menu to configure INI Backup. This screen will have the provision to configure the INI Backup to occur daily or a weekly basis and at a particular time.
Product = MCS	
CS2K MSM Management Console (changed)	Feature A00009028 (MCS) modifies the CS2K MSM Management Console to support SIP lines: • Configuration and maintenance of the NCAS link for querying SIP. • Configuration and maintenance of the Gateway Controller link for Gateway Control Protocol. • Endpoint maintenance • Disabling accounting for SIP lines
Provisioning Client and the OPI (changed)	Feature A00009043 (MCS) provides the capability to provision data required by CS2K SS for the SIP Lines product. The following items will be introduced into CS2K SS: • SIP Lines as a service called CS2000 SIP Line. • SIP Lines attributes to the subscriber. The Provisioning of the SIP Line data will be available via both the Provisioning Client and via OPI (Open Provisioning Interface).
QSIP CI command (new)	Feature A00009241 (MCS) describes the QSIP CI command which obtains the static and dynamic snapshot from the CS2K SS platform related to the SIP line.

Affected Area	Command/User Interface Description
Meet Me Web Collaboration (changed)	Feature A00009651 (MCS) modifies the web collaboration interface to support multiple languages through locale selection, adds a participant roster, and internationalizes the collaboration tool bars to use hover help in the user's language and cleaner graphics for the buttons.
BladeCenter-T RTP Media Portal Configuration (changed)	Feature A00009655 (MCS) modifies the configuration of the BladeCenter-T RTP Media Portal. It can now be configured to operate as either a collection of independent service instances ("Stand-Alone"), or as an N+1 fault tolerant service cluster ("Clustered"). This feature also adds the ability to manage the BladeCenter-T RTP Media Portal as a set of distinct network elements. The configuration adaptations appear as minor changes to the configuration data as presented in the Management Console, and so a consistent interface can be presented for all varieties. Both Stand-Alone and Clustered configurations of the BladeCenter-T RTP Media Portal are configured exactly the same – the differentiation being that the Stand-Alone is configured as a "1+0" (1 active instance, and no standby instances) Service Cluster. The BladeCenter-T RTP Media Portal is configured using the MCS System Management Console, and is accomplished through the use of the new "Clusters" entity in the Network Data, and a new field in the RTP Portals Network Elements (the new field references an entry in the "Clusters" Network Data to specify cluster membership).
Product = MG 9000	
SSPFS Command Line Interface (changed)	Feature A00008858 (UA-AAL1, UA-IP) provides a standard and consistent design across MG9KEM and CallServer 2000 Management Tools (CMT) for client user inactivity time-out. There are three timers that will be configurable from the SSPFS CLI after the initial SSPFS installation. The three timers are: • User Inactivity Timeout • User Termination Timeout • Reauthentication Disable Timeout

Affected Area	Command/User Interface Description
MG9K Audit GUI (changed)	Feature A00008969 (UA-AAL1, UA-IP) modifies the MG9K Audit GUI to allows users to run an immediate audit without having to delete an existing scheduled audit as follows: • Audit view--The “Add” and “Remove” buttons no longer exist. When the audit view is selected, a list of NEs in the subnet is shown which includes only those NEs that are discovered (and are thus auditable). The user chooses an NE of interest and schedules the audit directly in the properties panel. Two tabs exist, one for scheduled audits, and another for immediate ones. • Create Audit View--This GUI is deleted. • Select VMG frame--for immediate audits, users have the option to specify which sub-system (or VMG) to run the audit on.
Subnet View GUI (changed)	Feature A00011167 (UA-IP, UA-AAL1) modifies the Subnet View GUI by adding new entry “User ID and Password” to the pull-down Configuration menu.
Product = Network Patch Manager	
Alarmshow command (new)	Feature A00009227 (PT-IP, UA-IP, IAC, IAW, UA-AAL1) creates command Alarmshow to toggle the display of alarms as they are raised or cleared.

Affected Area	Command/User Interface Description
Command name changes in NPM CLUI (changed)	Feature A00009227 (PT-IP, UA-IP, IAC, IAW, UA-AAL1) describes the command name changes made to ensure command naming consistency for commands that provide similar types of functions: • viewassign (was getassign) is used to list all reportable tables and field names. • viewtabs or vtabs (was ltabs) is used to list all reportable tables and field names. • viewtask or vt (was qtask) is used to display the specified task or all defined tasks. • viewreport all or vr all (was qreps) is used to display the specified report or all defined reports in the database. • viewset all or vs all (was qsets) is used to view the specified set or all defined sets in the database. • viewplan or vplan (was getplan) is used to view the specified plan or all defined plans in the database. • viewalarm or va (was alarminfo) is used to view the specified alarm or all defined alarms in the database. • viewpatch or vp (was display) is used to view the administrative information associated with a patch. • newalarm or na (was addalarm) is used to define a new alarmable condition. • newreport (was newset REPORT) is used to create a report. • newset (was newset SET) is used to create a set definition. • enablealarm (was alarm) is used to enable the specified alarm. • disablealarm (was alarm) is used to disable the specified alarm. • delalarm (was alarm) is used to delete the specified alarm. • alarmmatches (was alarm) is used to list either the patches or devices that caused the specified alarm to be raised. • modifyplan (was sched) is used to modify the scheduled activities of a plan. • updsched (was updplan) is used to update the plan schedule in the database. • runreport or rr (was query) is used to execute the specified report and display the results. • runset or rs (was query) is used to execute the specified set and display the results. • viewversion (was getversion) is used to view the version of the NPM software and database components.

Affected Area	Command/User Interface Description
(continued) Command name changes in NPM CLUI (changed)	(continued) Feature A00009227 (PT-IP, UA-IP, IAC, IAW, UA-AAL1) describes the command name changes made to ensure command naming consistency for commands that provide similar types of functions: • viewprop (was getprop) is used to list the property value for a specified key or all keys.

Servord changes overview

The following Service Order items are new or changed for (I)SN09. More complete descriptions appear in the Feature Deltas section of this document.

Area	New or changed	ServOrd Description
Product = CS 2000		
LCC and options	New option	Feature A00008522 (UA-IP, MCS) introduces a new SERVORD+ option of SIP_DATA.
DPL line option	New	A00008556 (CHS) modifies SERVORD+ to accept three new options related to DPL lines provisioning: DPL, SIP_PASSWORD and SIP_DATA. When provisioning a SIP line all three of the options described above must be present in the SERVORD+ NEW command. They can not be added later via ADO. The new system prompts for the DPL option are SIP, MAX_NUM_CALLS, and ALLOW_BSY_TERM.

Area	New or changed	ServOrd Description
POSID prompt	Changed	Feature A00009085 (PT-AAL1, PT-IP, DMS) increases the range of POSID to be 00001 to 99999. The previous maximum was 30000. The change affects SERVORD commands ADO, NEW, NEWACD, and CHF when used to manipulate ACD option data.
Station Specific Authorization Code	Changed	Per CR Q01151411, The maximum number Station Specific Authorization Codes per line is 16. The previous restriction of 7 SSAC via Servord is removed. If office parameter SO_ALLOW_REDUNDANT _FEATURE is turned on in table OFCVAR, then the ADO command can be used to add additional SSACs to a line that already has SSACs assigned as long as the total does not exceed 16 and there are no duplicate SSACs. The CHF command will now display existing SSAC codes as default values at the AUTHCODE prompt in the prompt mode The default value can be accepted by either hitting ENTER or "$" . The defaulf value can be overwritten by a new code. Also, any or all existing SSACs on a line can be deleted via the CHF comand by overwriting the default values with a "0" at the AUTHCODE prompt (any 1 digit authcode will work). New AUTHCODEs can be added as well. AUTHCODEs can be deleted, changed and added within the same CHF command as long the total does not exceed 16 SSACs per line. This is supported in the noprompt mode as well.

Office Parameter changes overview

The following office parameters are new or changed for (I)SN09. More complete descriptions will appear in the Feature Deltas section of this document.

Summary of new/changed Office Parameters for (I)SN09

Status	Name	Description
Product = CS 2000		
New	AAL2_ATM_ENABLE	Feature A00008629 (PT-IP, PT-AAL1) creates this new parameter in OFCENG to enable the AAL2 ATM IW-SPM feature, which utilizes the new NTLZ20DA GEM-II card.
Changed	MAX_NUMBER_ACD _AGENTS_PER_SWI TCH	Feature A00009085 (PT-AAL1, PT-IP, DMS) increases the maximum range of this parameter from 30,000 to 99,999.

Summary of new/changed Office Parameters for (I)SN09

Status	Name	Description
New	DPT_BICC_TEST_NODE	Feature A00009207 (PT-AAL1) creates this parameter in table OFCVAR to identify the particular node to which all incoming DPT calls will be routed. Provisioning of this parameter provides the node information to allow a test call to be terminated to a specified peripheral. This permits the customer to have a known path when conducting a test.
Changed	MAX_RES_LINES	Feature A00009208 (UA-IP, IAW, IAC) increases the maximum range of this parameter from 1500 to 1800.
Product = CS 2000 TOPS		
New	IPGW_SNMP_COMMUNITY_NAME IPGW_SNMP_MANAGER IPGW_SNMP_ENABLED IPGW_TELNET_ENABLED	Feature A00009011 (PT-IP, PT-AAL1, DMS) creates 4 new office parameters in OFCENG: • IPGW_SNMP_COMMUNITY_NAME allows the craftsperson to configure one SNMP community name for SNMP read, write, and trap operations on the 7X07AA. • IPGW_SNMP_MANAGER allows the craftsperson to configure the IP address of one SNMP manager (also known as a trap manager). The 7X07AA cards will send traps to this IP address. • IPGW_SNMP_ENABLED is a Y/N parameter that allows the craftsperson to enable or disable SNMP on the 7X07AA. • IPGW_TELNET_ENABLED is a Y/N parameter that allows the craftsperson to enable or disable Telnet on the 7X07AA.

OM/PM changes overview

The following OMs/PMs are new or changed for (I)SN09. They also appear in the OMs/PMs-by-product tables later in this document with lists of registers and descriptions.

Summary of new or changed OMs/PMs for (I)SN09

OM Group or PM name	New or Changed	Description
Product = Call Server 2000		
NMSNCAS	New	Feature A00007544 (PT-IP, CHS) creates OM group NMSNCAS with 4 registers to keep a record of the NMS messages sent and received by the CS2K Core over NCAS link. Associated with logs NMSS115, NMSS116, NMSS117, and NMSS118.
NCAS_LINK	New	Feature A00007544 (PT-IP, CHS) creates OM group NCAS_LINK with 6 registers to keep a record of the state changes of the NCAS Link and the number of messages sent and received over the NCAS link between CS2K Core and Session Server. It will also have a count of the number of times the NCAS Link has gone down and come up.
DPLOM	New	Feature A00007547 (CHS) creates OM group DPLOM with 13 registers for pegs and usage measurements of the VID resource pool. Refer to the Performance section of this feature for details.
OM Data Delivery (OMDD) Application	Changed	Feature A00008724 (PT-AAL1) provides the following enhancements: • implements an FTP retry mechanism so any reports not sent are re-sent at the next scheduled interval. • improves the audit mechanism to ensure that the omdata filesystem will not reach 100% at any instance for the currently supported OM capacity. • enhances the file rotation mechanism to ensure that all OM reports will be sent to downstream according to the configured schedule.
CICM QoS Statistics	New	Feature A00009364 (CHS) creates a set of 37 CICM per-call QoS statistics. Refer to Table 1 in the FN for a complete list, explanations of each parameter, and identification of which apply to Basic QoS and which apply to Extended QoS.
SIPGW_OVERLOAD	New	Feature A00009893 (PT-IP) adds OM group SIPGW_OVERLOAD to the Session Server to provide statistics related to the resources that are monitored to determine whether the SIP Gateway application is in overload. The group includes six registers.

Summary of new or changed OMs/PMs for (I)SN09

OM Group or PM name	New or Changed	Description
C7SCCP	Changed	CR Q01102601 adds two extension registers to this OM group: C7UDTSR2 and C7UDTST2.
C7SCCPCO	Changed	CR Q01102601 adds two extension registers to this OM group: C7CREFR2 and C7CREFT2.
DCADTALG DCAIA DCAMCEIA	Deleted	CR Q01073417 removes these three OM groups in SN09 as they are obsolete.
TRNK2	Changed	CR Q01127143 adds two extension registers to this OM group: NPQUERY2 and NPRESP2.
Product = IEMS		
MG 3200 performance metrics	New	Feature A00009777 (PT-IP) creates three groups of performance measurements for the MG 3200 element manager in the acPerfMediaGateway MIB. Refer to the FN for the complete list. • Call Processing Performance Management (10 measurements) • RTP Performance Measurements (12 measurements) • System Performance Measurements (2 measurements)
Product = MCS		
Refer to description	New	Feature A00009045 (MCS) creates the following new OMs: • CheckpointedCalls--used on the standby instance to monitor the number of calls that would be preserved in a case of a failover. • Presence Event Report--this new OM group tracks the behavior of the various presence events that are processed by the server. For the 8 presence event types, OM registers count events Created, Processed, Optimized, Queued, and Parked. • The following OMs are added to the existing "Pesence" OM group: — throttleNotifySelfOnly, pegged every time the system does not send out a notifications to non-self subscriptions because of a presence state change during minor overload. This is pegged once for the entire state change, and does not reflect the actual number of notify messages that were not sent out.

Summary of new or changed OMs/PMs for (I)SN09

OM Group or PM name	New or Changed	Description
(continued) Refer to description	(continued) New	(continued) Feature A00009045 (MCS) creates the following new OMs: — throttleNotifyAll, pegged every time the system does not send out any notifications, including self-subscriptions because of a presence state change during major or severe overload. This is pegged once for the entire state change, and does not reflect the actual number of notify messages that were not sent out.
PCMM Aggregate OMs	New	Feature A00011740 (IAC) creates the following new aggregate OMs that are not specific to any particular policy server: • incomingMsgQHighWater - This OM indicates thehighest percentage used for the incoming PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported. • transactionQHighWater - This OM indicates the highest percentage used for the outgoing PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported. • voiceGateAttempts - Total number of PCMM voice half calls processed across all policy servers connected to this session server. • unsVoiceGateAttempts - Total number of unsuccessful PCMM voice half calls processed. • unsupCodecVoiceGateAttempts - Total number of PCMM voice half calls with an SDP containing at least one codec for which bandwidth could not be calculated. • videoGateAttempts - Total number of PCMM video half calls processed across all policy servers connected to this session server. • unsVideoGateAttempts - otal number of unsuccessful PCMM video half calls processed. • unsupCodecVideoGateAttempts - Total number of PCMM video half calls with an SDP containing at least one codec for which bandwidth could not be calculated.

Summary of new or changed OMs/PMs for (I)SN09

OM Group or PM name	New or Changed	Description
(continued) PCMM Aggregate OMs	(continued) New	(continued) Feature A00011740 (IAC) creates the following new aggregate OMs that are not specific to any particular policy server: • outstandingDiscStale - The number of transactions that were discarded because no response was received from the policy server or because the outstanding transaction queue was full and the oldest transaction waiting for a response was removed to make room for a new transaction. • unkMediaGateAttempts - The number of PCMM gate attempts that could not be processed because the media type was unknown (i.e. not voice, video, or image).
PCMM Per-Policy Server OMs	New	Feature A00011740 (IAC) creates the following new per-policy server OMs that are specific to a chosen policy server: • numInitializations - Number of times the policy server COPS connection successfully completed the PCMM initialization sequence. • cnxPSDrop - Number of times the policy server gracefully closed the COPS TCP connection (i.e. in a way that caused a TCP FIN message to be sent from the policy server to the session server). • cnxDropProtTimeout - Number of times the connection was dropped by the session server due to lack of PCMM response from the policy server. • tcpSendFail - Number of times that PCMM messages had to be discarded due to the outgoing TCP buffer being full. • transDiscLinkDown - Number of PCMM transactions that were discarded due to the PCMM signaling link being down. • transDiscStale - Number of PCMM transactions that were discarded because no response was received from the policy server for more than seven seconds. Or, if the outstanding transaction queue is full, the number of oldest transactions that were discarded to make room for new outstanding transactions. • voiceGateAttempts - Total number of PCMM voice half calls processed for this policy server.

Summary of new or changed OMs/PMs for (I)SN09

OM Group or PM name	New or Changed	Description
(continued) PCMM Per-Policy Server OMs	(continued) New	(continued) Feature A00011740 (IAC) creates the following new per-policy server OMs that are specific to a chosen policy server: • unsVoiceGateAttempts- Total number of unsuccessful PCMM voice half calls processed. • videoGateAttempts - Total number of PCMM voice half calls processed for this policy server. • unsVideoGateAttempts - Total number of unsuccessful PCMM video half calls processed. • gsaReceived - Total number of Gate-Set-Ack messages received from the policy server. • gdSent - Total number of Gate-Delete messages sent to the policy server. • upVoiceGSEReceived - Total number of Gate-Set-Err messages received from the policy server for upstream voice gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason. • upVoiceGSENoResources - Number of Gate-Set-Err messages for upstream voice gates with error code 1 - Insufficient Resources. • upVoiceGSEUnkGateId - Number of Gate-Set-Err messages for upstream voice gates with error code 2 - Unknown GateID. • upVoiceGSEOther - Number of Gate-Set-Err messages for upstream voice gates with error code 127 - Other, Unspecified Error. • dnVoiceGSEReceived - Total number of Gate-Set-Err messages received from the policy server for downstream voice gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason. • dnVoiceGSENoResources - Number of Gate-Set-Err messages for downstream voice gates with error code 1 - Insufficient Resources. • dnVoiceGSEUnkGateId - Number of Gate-Set-Err messages for downstream voice gates with error code 2 - Unknown GateID. • dnVoiceGSEOther - Number of Gate-Set-Err messages for downstream voice gates with error code 127 - Other, Unspecified Error.

Summary of new or changed OMs/PMs for (I)SN09

OM Group or PM name	New or Changed	Description
(continued) PCMM Per-Policy Server OMs	(continued) New	(continued) Feature A00011740 (IAC) creates the following new per-policy server OMs that are specific to a chosen policy server: • gseInvSubscr - Number of Gate-Set-Err messages for voice and video, upstream and downstream gates with error code 13 - Invalid Subscriber ID. • gseInvAMID - Number of Gate-Set-Err messages for voice and video, upstream and downstream gates with error code 14 - Unauthorized AMID. • upVideoGSEReceived - Total number of Gate-Set-Err messages received from the policy server for upstream video gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason. • upVideoGSENoResources - Number of Gate-Set-Err messages for upstream video gates with error code 1 - Insufficient Resources. • upVideoGSEUnkGateId - Number of Gate-Set-Err messages for upstream video gates with error code 2 - Unknown GateID. • upVideoGSEOther - Number of Gate-Set-Err messages for upstream video gates with error code 127 - Other, Unspecified Error. • dnVideoGSEReceived - Total number of Gate-Set-Err messages received from the policy server for downstream video gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason. • dnVideoGSENoResources - Number of Gate-Set-Err messages for downstream video gates with error code 1 - Insufficient Resources. • dnVideoGSEUnkGateId - Number of Gate-Set-Err messages for downstream video gates with error code 2 - Unknown GateID. • dnVideoGSEOther - Number of Gate-Set-Err messages for downstream video gates with error code 127 - Other, Unspecified Error. • grsClose - otal number of Gate-Report-State messages received indicating that a gate was closed by the CMTS for all reasons. • grsCloseResReassign - Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 1 - reservation reassignment.

Summary of new or changed OMs/PMs for (I)SN09

OM Group or PM name	New or Changed	Description
(continued) PCMM Per-Policy Server OMs	(continued) New	(continued) Feature A00011740 (IAC) creates the following new per-policy server OMs that are specific to a chosen policy server: • grsCloseMacLayer - Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 2 - lack of DOCSIS MAC-Layer responses. • grsCloseT1 - PCMM timer T1 specifies the number of seconds a PCMM gate can be authorized but not reserved. This OM indicates the number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 3 - timer T1 expiration. • grsCloseT2 - PCMM timer T2 specifies the number of seconds a PCMM gate must hold bandwidth reserved in excess of what was committed. Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 4 - timer T2 expiration. • grsCloseResMaint - Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 6 - lack of reservation maintenance. • grsCloseT4 - Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 8 - timer T4 expiration. • grsNotif - Total number of Gate-Report-State messages received indicating a change of gate state (for any reason) that did not result in the gate being closed. • grsNotifT3 - Number of Gate-Report-State messages received indicating that a gate was transitioned to the Committed-Recovery state by the CMTS due to the T3 timer expiring.

AMA/Billing changes overview

The following AMA/Billing information is new or changed for (I)SN09. More complete descriptions appear in the Feature Deltas section of this document.

Summary of new or changed AMA/billing

AMA/billing item	New or Changed	Description
Product = CS 2000		
Closure of billing files	Changed	Feature A00008090 (PT-AAL1) facilitates the closure of billing files at the scheduled Interval as specified in the Stream Configuration and provides an additional functionality of Resetting the DIRP Billing File sequence number at Midnight. With this feature, all the open billing files are rotated exactly at scheduled interval without any drift or delay.
AMAOPTS	Changed	Feature A00009252 (UA-IP) allows the customer to record a corrected timestamp for billing records that originate on agents with the MTZ line option. The connect timestamp will be modified to the agent's time zone and this timestamp will be appended to the existing billing record in AMA using a module code and SMDR using an extension record. Table AMAOPTS contains a new switch wide option (RECORD_MTZ) that will allow customers to use the MTZ option and decide whether or not they want to record the modified timestamp.
AMA billing Module 260	New	Feature A00009508 (UA-IP) creates new AMA billing Module 260 with two new fields COMPONENT ROLE and IP SERVICE PROTOCOL to the BAF database on SDM/CBM to be supported by AMADUMP tool on SDM/CBM. This captures originating and terminating agent component and protocol information for packet network agents.
AMAOPTS	Changed	Feature A00009508 (UA-IP) creates a new tuple in table AMAOPTS to activate and deactivate Module 260 inclusion. The new OPTION is called RECORD_MC260, and the SCHEDULE will be either ON or OFF. The default setting is OFF. The new option activates recording of packet client involvement for both originating and terminating agents. This option does not force billing; it collects the additional information for existing billable scenarios.

Software Optionality Control (SOC) changes overview

The following SOC information is new or changed for (I)SN09. More complete descriptions appear in the Feature Deltas section of this document.

Summary of new or changed SOC information for (I)SN09

SOC code	New or Changed	Description
Product = CS 2000		
MDC00078	New	Feature A00007544 (PT-IP, CHS, Int'l PT-IP) creates state SOC "NMS Over IP (SCTP)" to activate or deactivate network message waiting service over IP.
CS2C0005	New	A00008556 (CHS) creates this usage SOC, "Number of SIP Clients." The SOC limit defines the maximum number of DPL lines that can be provisioned in the switch. The SOC code is functional whenever a line is provisioned with the DPL option whether through table control / servord.
ICM00081	New	Feature A00009078 (UA-IP, UA-AAL1, DMS) creates state SOC "ICM Dual Link" to activate or deactivate the functionality of the second TCP/IP link within a linkset.
ACD00101	Changed	Per feature A00009085 (PT-AAL1, PT-IP, DMS), this SOC correlates with office parameter MAX_NUMBER_ACD_AGENTS_PER_SWITCH. The maximum limit of this SOC is increased to 99,999. When the SOC usage limit is increased or decreased, the value stored in the office parameter is automatically updated to reflect the new limit.
ACD00104	New	Per feature A00009085 (PT-AAL1, PT-IP, DMS), this SOC controls the maximum number of ACD Groups per switch, which is now increased to 5,000. This SOC also controls the maximum number of ACD Subgroups and Supervisors per Group.
ACD00105	New	Per feature A00009085 (PT-AAL1, PT-IP, DMS), this SOC controls the maximum number of ACD Agents per Group.
ACD00106	New	Per feature A00009085 (PT-AAL1, PT-IP, DMS), this SOC controls the maximum number of incoming and incoming overflowed calls per ACD Group.
ICM00082	New	Per feature A00009085 (PT-AAL1, PT-IP, DMS), this SOC controls the maximum number of DNs that can be associated per ICM Session

Summary of new or changed SOC information for (I)SN09

SOC code	New or Changed	Description
EQA00032	New	Feature A00009091 (PT-AAL1, PT-IP, DMS) creates this state SOC to allow call processing and Traver access to new table LPICPXLA if the originating agent has VEONAME assigned.
SMGT0001	New	Feature A00010303 (DMS) creates state SOC “Map Based Service Control” to control the CI interface to Service Management. This SOC is independent of the AIN TCAP Service Management SOC.

Chapter 2: IEMS Functionality

IEMS Northbound Interfaces

General Information

The IEMS provides a consolidated location to manage the Fault, Configuration, Performance Collection and Security account domains for devices (Network Elements, Element Managers, Management Applications and Platforms) in a CS 2000 central office. A brief description of its capabilities include the following:

- Topology: The IEMS provides a graphical representation of the managed devices in a central office. The IEMS client comes with default views (Network Elements, Element Mangers, Applications and Platforms) of the managed network and provides flexible interfaces that allow a craftperson to create customized views of the network. The alarm state of each of the managed devices in the IEMS topology is dynamically depicted by the associated background color (Red= Critical, Red=Major, Amber=Minor, Yellow=Warning, Green=Clear) of the managed device.
- Fault: The IEMS aggregates the event streams received from the various EMSs, NEs, applications, and platforms that it manages. It normalizes the events received from these streams and forwards the events over its northbound interfaces (such as SCC2, NTSTD, SNMP, and SYSLOG). The IEMS alarm and event browsers provide a consolidated real-time and historical view of the events that have occurred in a CS 2000 central office. It provides tools to view and page through the events and alarms in a common graphical interface. The Alarm and event browsers provide a wide range of features to manage, sort, filter and view events in a single centralized location. For detailed information on the IEMS fault management features please refer to the IEMS Fault Management document (NN10334-911).
- Performance: The IEMS provides a centralized location for collecting, storing and forwarding performance data in a CS 2000 central office. Its performance collection sub-system provides some basic tools for viewing and graphing the collected performance attributes. In addition, it does provide interfaces to configure the generation of threshold alarms for the

collected Operation Measurement data. For detailed information on the IEMS performance management features please refer to the IEMS Performance Management document (NN10327-711).

- Configuration: The IEMS provides a centralized location to launch the various Succession Configuration management interfaces. For detailed information on the IEMS configuration management features please refer to the IEMS Configuration Management document (NN10330-511).
- Security: The IEMS provides a centralized graphical interface to configure and manage the user accounts in a Succession Central Office. The IEMS Security subsystem provides centralized authentication and authorization server for many of its managed devices. It also provides centralized security logging for successful and failed authentications. In addition it provides Single Sign-on support enabling a user to log in to the IEMS client once and access multiple Succession Management interfacse without requiring the user to re-enter a userid and password. For detailed information on the IEMS Security management features please refer to the IEMS Security and Administration document (NN10336-611).

IEMS Northbound Fault Interface

User Setup, Administration, and Customization of Views

For information on initial setup and customization of the Northbound fault feed from IEMS see:

- IEMS Fault Management Guide - NN10334-911

Device Fault Mapping References for Northbound Interface

The following table shows the log identification criteria for each device, manager, and application supported by IEMS. Log references for table entries defined in *italics* can be found in:

NN10275-909 - Succession Fault Management Logs Reference (volumes 1-3)

See the table below for additional fault documentation

Fault Correlation for SN09 Devices

	NB format -> **Device/EM**	**Documentation Log Key**	**Document Reference**
1	***"Audio Provisioning Server (APS)"***	Log name and number	NN10328-911 MS 2000 Series Fault Management

| | NB format ->

Device/EM | Documentation Log Key | Document Reference |
|---|---|---|---|
| 2 | **“Call Agent Core”** | Log name and number | see “ Fault documentation for Call Agent Core :” |
| 3 | ***“Call Agent Platform”*** | Log name and number | NN10087-911 Call Agent Fault Management |
| 4 | ***CBM***

See “CS2000 Core Manager” | Log name and number | **See “CS2000 Core Manager”** |
5	***CEM***	Log value from the CEM logs	NN10334-911 IEMS Fault Management
6	**“Centrex IP Call Manager (CICM)”**	Log name and number	NN10334-911 IEMS Fault Management
7	***“CS2000 Core Manager”***	Log name and number	NN10082-911 CS 2000 Core Manager Fault Management
8	***“Gateway Controller (GWC)”***	Log name and number	NN10202-911 GWC Fault Management
9	***“GWC Manager”***	Log name and number	PLN-i09-OSS (I)SN09 OSS Guide
10	***Keymile UNEM and UMUX***	Log name and number	Keymile UMUX User’s Guide and Keymile UNEM User’s Guide
11	**“Media Application Server (MAS)”**	Log name and number from the specific problem	NN10375-113 MAS Unified Communications Service Guide
12	**“Multimedia Communication Server (MCS)”**	Log name and number	NN10030-111 System Manager Basics
13	**Media Gateway 3200 (MG 3200)**	Log name and number	LTRT-72704: MG3200 H.248 User Manual
14	**“Multi-Service Data Manager (MDM)”**	faultCode (specificProblem)	241-6001-500, *MDM Alarms Reference,* and 241-6001-011, *MDM Fault Management Tools*.

	NB format -> Device/EM	Documentation Log Key	Document Reference
15	**MDM for BSC** **see "Multi-Service Data Manager (MDM)"**	faultCode (specificProblem)	see **"Multi-Service Data Manager (MDM)"**
16	**MDM - carrier** **see "Multi-Service Data Manager (MDM)"**	faultCode (specificProblem)	see **"Multi-Service Data Manager (MDM)"**
17	**MDM Client-Server** **see "Multi-Service Data Manager (MDM)"**	faultCode (specificProblem)	see **"Multi-Service Data Manager (MDM)"**
18	**"MultiService Switch 7400, 15000, 20000"**	Log name and number	NN10600-500 Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference NN10600-520 Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management MSS 15000, MG 15000 & MDM Fault Overview
19	***"Media Gateway 9000 (MG9000)"***	Log name and number	NN10074-911 MG9000 Fault Management
20	***"MG9000 Manager"***	Log name and number	NN10074-911 MG9000 Fault Management
21	**"MS2000 Series Node"**	Log name and number	NN10328-911 MS2000 Series Fault Management
22	***"Network Patch Manager (NPM)"***	Log name and number	N10408-900 ATM/IP Solution-level Fault Management
23	**"Ethernet Routing Switch 8600 (formerly Passport 8600)"**	Log name and number	241-6003-110 Passport 8600 Device Integration Cartridge User Guide
24	**"QoS Collector Application (QCA)"**	Log name and number	NN10083-911 Communication Server 2000 Fault Management

	NB format -> Device/EM	Documentation Log Key	Document Reference
25	***"SAM21 Element Manager"***	Log name and number	NN10089-911 SAM21 Shelf Controller Fault Management
26	***"SAM21 Shelf Controller"***	Log name and number	NN10089-911 SAM21 Shelf Controller Fault Management
27	***"Core Manager Platform"*** ***See "CS2000 Core Manager"***	Log name and number	NN10082-911 CS 2000 Core Manager Fault Management
28	**"Session Server Manager"**	Log name and number	NN10332-911 Session Server Fault Management
29	***"Succession Server Platform Foundation Software (SSPFS)"***	Log name and number	NN10408-900 ATM/IP Solution-level Fault Management
30	***"Storage Manager (STORM)"***	Log name and number	NN10088-911 Storm Fault Management
31	***"Universal Audio Server (UAS)"***	Log name and number	NN10275-909 v3 Succession Fault Management Logs Reference NN10073-911 UAS Fault Management
32	**"Universal Signaling Point (USP)"**	Specific Problem: Log Group=<text> & Log Number=<number> Note: Log GroupID is not used	NN10071-911 USP Fault Management
33	**"XACore"**	Log name and number	297-8991-510 XA-Core Maintenance Manual

IEMS Northbound Fault Specifications

Fault events are available from any of four Northbound interfaces. Log formats supported in this release are: NTSTD, SCC2, Syslog, and SNMP. A description of each of these interfaces is given in the sections that follow.

OSS clients can receive faults in **SCC2** and **NTSTD** formats from IEMS by initiating a TCP socket connection to designated ports on the IEMS server.

When a connection attempt is made by a remote host, the IEMS validates the connecting OSS as an authorized client. It then forwards all logs that satisfy the configured filter criteria to the OSS. The port numbers and remote clients eligible to connect to these log streams are configured by the administrator.

> ***Note:*** **In legacy environments, the ECORE option was used to include the originating node name in the log header for SCC2 and NTSTD formats. This option is NOT supported with Nortel Networks Carrier VoIP solution. All references to ECORE in the following sections will assume this option is disabled.**

Faults can be delivered to hosts via **SNMP** by configuring the IP address and port of the remote management application.

The standard **Syslog** interface can also be configured as a fault stream for remote management systems.

The following table summarizes the characteristics of the four Northbound fault feeds from IEMS.

IEMS Northbound Fault Stream Characteristics

Fault format	Port	OSS Connection	Stream type	IEMS Config required
NTSTD	8555	Incoming. IEMS waits for connection by remote host	ACSII stream over TCP, push	OSS IP address or hostname
SCC2	8556	Incoming. IEMS waits for connection by remote host	ACSII stream over TCP, push	OSS IP address or hostname
SNMP	user-defined on remote listener	IEMS forwards SNMP faults as SNMP traps to OSS. OSS can also query IEMS for active alarm data. By default, the following attribute values are used for configuring SNMP northbound fault feed. The administrator can change the attribute values.	SNMP trap events (UDP), push	IP address and port of listener on OSS

Fault format	Port	OSS Connection	Stream type	IEMS Config required
Syslog	designated port for Syslog service (514)	IEMS forwards log events to remote host	ACSII data over UDP, push	syslog.conf requires forwarding entry for log facility **Fault:** local7.notice **Audit:** local0.notice **Security:** local3.notice

Each fault interface is discussed in the sections that follow.

Northbound SCC2 Specification

SCC2 is an ACSII stream delivered to a Northbound receiving application. The stream is delivered over a TCP socket and is configured by the administrator.

This section provides a detailed description of the SCC2 log format delivered by IEMS.

SCC2 Format Summary:

<Alarm Severity><Minute Indicator><Log Name><Log Number><Threshold>< Sequence Number><Event Type><Event Label><Equipment Identifier><Body Text>

SCC2 Header Formats

SCC2 Header format:

```
-------------------------------------------------------------------
-------
123456789012345678901234567890123456789012345678901234567890123
3456789
---------|---------|---------|---------|---------|---------|--
-------
aabb\ccccdddeffff\gggg\h.../i.../j...
---------|---------|---------|---------|---------|---------|--
-------
```

1. The backslash sign (\) signifies a space.
2. The forward slash sign (/) signifies a space that only appears if the preceding optional field exists.
3. The periods (...) signify variable length data.

4 The 'greater than' sign followed by periods (>...) signifies variable length indentation determined by the application.

5 The vertical lines do not appear on the actual report, they are used for presentation purposes in the above figure.

6 This notation only represents the header and does not include the application data area (i.e. the rest of the log report).

An example of a SCC2 log header is given below. It is also used in explaining the individual fields in the log header.

SCC2 Log Header Example:

```
* 03 PM  128+0417 TBL  ISTB LIU7 348
            ISTb     From InSv
```

SCC2 Field Descriptions

Fld	Name	Description	Example
a	**Alarm Severity**	The severity level of the log report. This is a 2 character field left justified and padded with blanks. Possible values are: '*C' = critical alarm, '**' = major alarm, '* ' = minor alarm, ' ' = no alarm.	'*'
b	**Minute Indicator**	This value represents the minutes after the hour. It consists of 2 numeric characters, right justified and padded with zeroes. It ranges from 00 to 59.	'03'
c	**Log Name**	This value can be 2 to 4 non blank characters. Within this fixed 4 characters, it is left justified and padded with blanks.	'PM '
d	**Log Number**	This value is always 3 digits ranging from 000 to 999. It is right justified and padded with zeroes. For PROTOLOGs (i.e. TRAP, SWERR, INIT, INFO, and LOCK logs) it is a string of 3 spaces.	'128'

Fld	Name	Description	Example
e	**Threshold**	Indicates whether a threshold was set for the given log report. A threshold can be temporarily set by using LOGUTIL.Thresholding will survive any restart by turning on the office parameter threshold_is_sampling in table OFCVAR and datafilling threshold value for individual log report in table LOGCLASS and RLOGCLAS on the CallServer. If THRESHOLD_IS_SAMPLING is on (Y), a log report is generated for every n-th instance of the log report generated. If threshold_is_sampling is off (N), every log report after the n-th report is generated. Possible values are: '+' = a threshold was set, ' ' = no threshold was set.	'+'
f	**Sequence Number**	This field defines the unique sequence for each log report. It is right justified and padded with zeroes. It represents 4 numeric characters ranging from 0000 to 9999.	'0417'
g	**Event Type**	Log report event type which is a string of 4 uppercase characters, left justified and padded with blanks. This field is defined by the applications that generate the log report. Possible values include: ' ', 'CBSY', 'EXC ', 'FAIL', 'FLT ', 'INFO', 'INIT', 'LO ', 'MANB', 'OFFL', 'PASS', 'PBSY', 'RTS ', 'SUMM', 'SYSB', 'TBL ', 'TRAN', 'TRAP', 'UNEQ'.	'TBL '
h	**Event Label**	A variable length character string that represents application event description. It is an optional field.	'ISTB'
		The following fields are defined by the applications that generate the log report. These fields are optional and independent of each other.	
i	**Equipment Identifier**	A conditional equipment identifier determined by the application. It is a variable length character string.	'LIU7 348'
j	**Body Text**	Application specific log body text starts here. This may contain several lines. Each new line is indented by eight spaces. Most log bodies start with a carriage return character so that none of it appears on the header line.	'ISTb From InSv'

Examples of Logs with SCC2 Header

The sample logs below are shown for example only. They are syntactically correct but field contents may vary.

1 Gateway Controller example

```
**14 GWC 307 7250 TBL  GWC Fault
      Location: GWC-2-UNIT-0
      NotificationID: 4
      State: Raise
      Category: Communications
      Cause: Communications subsystem failure
      Time: Jan 23 15:15:59 2004
      Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Unit=
      unit_0;Software=NODE MTC
      Specific Problem: EM not responding, provisioned data
      loaded from local Flash
      Description: Element Manager communication failure.
```

2 Call Server example:

```
56 LINE138 3778 INFO TRMT
       SLOA 21 1 02 01    DN 2145202111
     TREATMENT SET = BUSY   CALLED NO =           5202111
       CALLID= 01BE 036D
```

Northbound NTSTD

NTSTD is an ACSII stream delivered to a Northbound receiving application. The stream is delivered over a TCP socket and is configured by the administrator.

This section provides a detailed description of the NTSTD log format delivered by IEMS.

NTSTD Format Summary:
<Office Identifier><Alarm Severity><Threshold><Log Name><Log Number><Time MMMMDD hh:mm:ss>< Sequence Number><Event Type><Event Label><Equipment Identifier><Body Text>

Standard Header Formats

```
ECORE Format OFF:
-------------------------------------------------------------
-------
12345678901234567890123456789012345678901234567890123456789012
```

```
3456789
---------|---------|---------|---------|---------|---------|--
-------
a...#cccdeeeefff\ggghh\ii:jj:kk\llll\nnnn\o.../p.../q...
---------|---------|---------|---------|---------|---------|--
-------
```

Notes:

1. The placeholder represented by the pound sign (#) is non-existent if both office parameter log_office_id and ecore_format in table OFCVAR are turned off. The pound sign (#) represents a space in other cases (i.e. log_office_id is datafilled and ecore_format is turned off; and whenever ecore_format is turned on regardless of log_office_id).
2. The backslash sign (\) signifies a space.
3. The forward slash sign (/) signifies a space that only appears if the preceding optional field exists.
4. The periods (...) signify variable length data.
5. The vertical lines do not appear on the actual report, they are used for presentation purposes in the above figure.
6. This notation only represents the header and does not include the application data area (i.e. the rest of the log report).

An example of a standard log header is given below. It is also used in explaining the individual fields in the log header.

Standard log header example:

```
SCP2B *+  PM128 OCT20 10:03:42 0417 TBL  ISTB LIU7 348
            ISTb     From InSv
```

NTSTD format field descriptions

Fld	Name	Description	Example
a	**Office Identifier**	Identifies the switch generating the Identifier log. This is an optional field. It is output if the office parameter log_office_id in table OFCVAR on the CallServer is datafilled. It has variable length from 0 up to 12 characters.	'SCP 2B'

Fld	Name	Description	Example
b	**Ecore Node Name**	Originating node name where this log Node Name report is generated. It is an eight character field, its contents are left justified and padded with blanks. It is contained in the header if the office parameter ecore_format in table OFCVAR is turned on. ***As of SN07, this option is not supported***	'CM '
c	**Alarm Severity**	The severity level of the log report. This is a 3 character field right justified and padded with blanks. Possible values are: '***' = critical alarm, ' **' = major alarm, ' *' = minor alarm, ' ' = no alarm.	' *'
d	**Threshold**	Indicates whether a threshold was set for the given log report. A threshold can be temporarily set by using LOGUTIL. Thresholding will survive any restart by turning on the office parameter threshold_is_sampling in table OFCVAR and datafilling threshold value for individual log report in table LOGCLASS and RLOGCLAS on the CallServer. If threshold_is_sampling is on (Y), a log report is generated for every n-th instance of the log report generated. If threshold_is_sampling is off (N), every log report after the n-th report is generated. Possible values are: '+' = a threshold was set, ' ' = no threshold was set.	'+'
e	**Log Name**	This value can be 2 to 4 non blank characters. Within this fixed 4 characters, it is right justified and padded with blanks.	' PM'
f	**Log Number**	This value is always 3 digits ranging from 000 to 999. It is right justified and padded with zeroes. For PROTOLOGs, (ie. TRAP, SWERR, INIT, INFO and LOCK logs) it is a string of 3 spaces.	'128'
g	**Month Indicator**	Consists of 3 uppercase characters ranging from 'JAN' to 'DEC' that represent the month.	'OCT '
h	**Day Indicator**	Consists of 2 numeric characters ranging from 01 to 31 that represent the day of the month	'20'
i	**Hour Indicator**	Consists of 2 numeric characters ranging from 00 to 23 that represent the hour of the day.	'10'

Fld	Name	Description	Example
j	**Minute Indicator**	Consists of 2 numeric characters ranging from 00 to 59 that represent the minute of the hour.	'03'
k	**Second Indicator**	Consists of 2 numeric characters ranging from 00 to 59 that represent the second of the minute.	'42'
l	**Sequence Number**	This field defines the unique sequence for each log report. It is right justified and padded left with zeroes. Represents 4 numeric characters ranging from 0000 to 9999.	'0417'
n	**Event Type**	Log report event type which is a string of 4 uppercase characters, left justified and padded with blanks. This field is defined by the applications that generate the log report. Possible values include: ' ', 'CBSY', 'EXC ', 'FAIL', 'FLT ', 'INFO', 'INIT', 'LO ', 'MANB', 'OFFL', 'PASS', 'PBSY', 'RTS ', 'SUMM', 'SYSB', 'TBL ', 'TRAN', 'TRAP', 'UNEQ'.	'TBL '
o	**Event Label**	A variable length character string that represents application event description. This field is optional.	'ISTB'
		The following fields are defined by the applications that generate the log report. These fields are optional and independent of each other.	
p	**Equipmnt Identifier**	A conditional equipment identifier determined by the application. It is a variable length character string.	'LIU 7 348'
q	**Body Text**	Application specific log body text starts here. This may contain several lines. Each new line is indented by eight spaces. Most log bodies start with a carriage return character so that none of it appears on the header line.	'ISTb From InSv'

Examples of Logs with Standard Header

The sample logs below are shown for example only. They are syntactically correct but field contents may vary.

1 Gateway Controller example:

```
RTPU07BU  **  GWC307 Jan23 20:14:38 7250 TBL  GWC Fault
        Location: GWC-2-UNIT-0
        NotificationID: 4
```

```
State: Raise
Category: Communications
Cause: Communications subsystem failure
Time: Jan 23 15:15:59 2004
Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Uni
t=unit_0;Software=NODEMTC
Specific Problem: EM not responding, provisioned
data loaded from local
Flash
Description: Element Manager communication failure.
```

2 Call Server example:

```
RTPU07BR     LINE138 Jan23 16:56:30 3778 INFO TRMT
        SLOA 21 1 02 01    DN 2145202111
        TREATMENT SET = BUSY   CALLED NO =              5202111
        CALLID= 01BE 036D
```

Northbound Syslog

Syslog is a standardized UDP protocol defined by the IETF working group: **Syslog Protocol (RFC 3164): http://www.ietf.org/rfc/rfc3164.txt**

This ACSII fault stream is delivered to a Northbound receiving Syslog host over the local 7 facility. On the IEMS server, Syslog routing is configured through the SSPFS command line interface. This interface manages any required changes to syslog.conf.

This section covers the vendor-specific information on the format and content of Syslog messages not covered under RFC3164.

The following shows a breakdown of the components of the MSG portion of a Syslog message provided by the IEMS Northbound interface:

<Time> <Host> IEMS:
_V2_~**I=**<NodeId>~**H=**<Host>~**A=**<ApplicationName>~**S=**<Seq.Number>
~~ <LogName><LogNumber> <AlarmSeverity> <EventType> <Label> ^M
<LogBody>

The following Syslog message will be used to discuss the structure of Syslog messages from IEMS :

```
Feb 23 12:38:54 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=4317~~
MGEM302 NONE TBL  MG9K InvalidEMIPAddress^M        Location: MG9k EM
Comm Network^M        Notification Id: 17180020453^M        State:
```

```
Cleared^M       Category: communications^M       Cause: Communications
Subsystem Failure^M          Invalid EM IP Address - An invalid EM IP
address has been set on the GW^M         Component Id: MG9k EM Comm
Network^M        specificProblem: Invalid EM IP Address - An invalid
EM IP address has be^M         en set on the GW^M         Description:
An invalid EM IP address has been set on the GW
```

Note: See " MG9000 Manager" for comparison of this log in all IEMS Northbound formats.

RFC3164 MSG Fields

Each Syslog message is prefixed by a timestamp and hostname. These fields are shown in *italics* in the example above. Section 4.1.2 of RFC3164 defines these fields as follows:

The **TIMESTAMP** field is the local time and is in the format of "Mmm dd

hh:mm:ss" (without the quote marks) where:

Mmm is the English language abbreviation for the month of the year with the first character in uppercase and the other two characters in lowercase. The following are the only acceptable values:

Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

dd is the day of the month. If the day of the month is less than 10, then it MUST be represented as a space and then the number. For example, the 7th day of August would be represented as "Aug 7", with two spaces between the "g" and the "7".

hh:mm:ss is the local time. The hour (hh) is represented in a 24-hour format. Valid entries are between 00 and 23, inclusive. The minute (mm) and second (ss) entries are between 00 and 59 inclusive.

A single space character MUST follow the TIMESTAMP field.

The **HOSTNAME** field will contain only the hostname, the IPv4 address,

or the IPv6 address of the originator of the message. The preferred value is the hostname. If the hostname is used, the HOSTNAME field

MUST contain the hostname of the device as specified in STD 13 [4].

It should be noted that this MUST NOT contain any embedded spaces.

The Domain Name MUST NOT be included in the HOSTNAME field. If the IPv4 address is used, it MUST be shown as the dotted decimal notation as used in STD 13 [5]. If an IPv6 address is used, any valid representation used in RFC 2373 [6] MAY be used.

A single space character MUST also follow the HOSTNAME field.

IEMS Header

After the timestamp and hostnames fields, the following constants can be found in the next two fields - separated by a space:

IEMS: Indicates the start of fault-specific information

_V2_ - Syslog format version

Immediately following this tag are several attributes specified as name-value pairs (NVPs). NVP tags are prefixed by a tilde '~'<tag>=<value> for easy identifcation by downstream parsers.

NVPs for IEMS Syslog message

Tag name	Description	example
~I	Node Identifier	~I=
~H	Host name of	~H=znc0s0jh
~A	Reporting Application name	~A=IEMS
~S	Log Sequence number	~S=4317
~~	Indicates start of formatted log header from originator. **Note: This indicator is NOT actually an NVP. It is followed by a single space character	~~ MGEM302 NONE TBL MG9K InvalidEMI PAddress

Parsing Conventions for Formatted Log Data:

The format of the log header and body follow a number of conventions to facilitate parsing by downstream applications:

1 Line feeds in message text are identified by the ^M character sequence (this denotes a sequence of the two printable characters: caret and upper case M).

2 The log header start can be identified by the ~~ sequence followed by a space. The header is delimited by the line feed indicator (discussed in the previous bullet).

3 The log body is separated into lines using ^M sequences defined in bullet 1. Each line is prefixed with eight (8) space characters.

4 Line length (including leading spaces) will not exceed 80 characters . See example log above.

5 All text in the log header and body will consist of printable ACSII characters.

6 Blank lines are not allowed in the formatted log message. This includes both header and body components.

Log Header

The log header consists of the following fields. These fields map to the corresponding fields defined in both SCC2 and NTSTD.

A typical log header will appear in the following format ('\' indicates a space character):

~~\<logname><lognumber>\<AlarmSeverity>\<EventType>\<Label>^M<LogBody>

Log Header fields in Syslog message

Name	Description	Example
Log Name	This value can be 2 to 4 non blank characters. Within this fixed 4 characters, it is right justified and padded with blanks.	' MGEM'
Log Number	This value is always 3 digits ranging from 000 to 999. It is right justified and padded with zeroes. For PROTOLOGs, (ie. TRAP, SWERR, INIT, INFO and LOCK logs) it is a string of 3 spaces.	'302'
Alarm Severity	This field defines the alarm severity and consists of one of the following text strings: NONE, MINOR, MAJOR, CRIT	'NONE'

Name	Description	Example
Event Type	Log report event type which is a string of 4 uppercase characters, left justified and padded with blanks. This field is defined by the applications that generate the log report. Possible values include: ' ', 'CBSY', 'EXC ', 'FAIL', 'FLT ', 'INFO', 'INIT', 'LO ', 'MANB', 'OFFL', 'PASS', 'PBSY', 'RTS ', 'SUMM', 'SYSB', 'TBL ', 'TRAN', 'TRAP', 'UNEQ'.	'TBL '
Label	A variable length character string that represents application event description. This field is optional.	'MG9K InvalidEMIPAddress'
Log Body	Application specific log body text starts here. This may contain several lines. Each new line is indented by eight spaces and delimited by the ^M (caret-M) character sequence.	' Location: MG9k EMCommNetwork**^M** Notification Id: 17180020453**^M** State: Cleared**^M** Category: communications**^M** Cause: Communications SubsystemFailure**^M** Invalid EM IP Address - An invalid EM IP address has been set on the GW**^M** Component Id: MG9k EMCommNetwork**^M** specificProblem: Invalid EM IP Address - An invalid EM IP address has be**^M** en set on the GW**^M** Description: An invalid EM IP address has been set on the GW'

Notes on Log Body Text

The remainder of the message consists of the log body. The message text in this portion of the message is defined by the originating source. The presentation of this text is constrained only by the rules outlined in "Parsing Conventions for Formatted Log Data:" on page 94.

Note: See **Syslog Protocol (RFC 3164): http://www.ietf.org/rfc/rfc3164.txt** for full details on this specification.

Security and Audit logs

IEMS Security and Audit logs are managed through Syslog and can be forwarded to a remote Syslog host in the same way as fault events. Note that some Solaris applications forward security logs to authlog (/varlog/authlog). Sample content of each follow:

Audit log sample (/var/log/auditlog):

```
Jan 16 10:37:55 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requeued

Jan 16 10:38:06 sspfs_svr ID[SUNWcluster.pmf.1018]: "CorbaNotification" Failed to stay
up.

Jan 16 10:38:06 sspfs_svr ID[SUNWcluster.pmf.1019]: "CorbaNotification" restarting too
often ... sleeping 30 seconds.

Jan 16 10:38:36 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requeued

Jan 16 10:38:46 sspfs_svr ID[SUNWcluster.pmf.1018]: "CorbaNotification" Failed to stay
up.

Jan 16 10:38:46 sspfs_svr ID[SUNWcluster.pmf.1019]: "CorbaNotification" restarting too
often ... sleeping 30 seconds.

Jan 16 10:39:16 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requeued

Jan 16 10:41:42 sspfs_svr ID[SUNWcluster.pmf.1018]: "snmpp" Failed to stay up.

Jan 16 10:42:16 sspfs_svr ID[SUNWcluster.pmf.1018]: "ompush" Failed to stay up.

Jan 16 10:42:41 sspfs_svr ID[SUNWcluster.pmf.1018]: "CorbaNotification" Failed to stay
up.

Jan 16 10:42:41 sspfs_svr ID[SUNWcluster.pmf.1020]: "CorbaNotification" requeued

Jan 16 10:42:49 sspfs_svr ID[SUNWcluster.pmf.1018]: "PropServer" Failed to stay up.
```

Security log sample (/var/log/securitylog):

```
Feb  6 22:03:16 wnc0s0qh IEMS: IEMS class_security.ver01 STAT=SUCCESS  SRC.USR=root
EVNT.TYPE =Authentication

Feb  6 22:03:16 wnc0s0qh last message repeated 1 time

Feb  9 14:34:33 wnc0s0qh IEMS: IEMS class_security.ver01 STAT=SUCCESS  SRC.USR=root
EVNT.TYPE =Authentication

Feb  9 14:34:33 wnc0s0qh last message repeated 1 time

Feb  9 15:36:20 wnc0s0qh IEMS: IEMS class_security.ver01 STAT=SUCCESS  SRC.USR=root
EVNT.TYPE =Authentication

Feb  9 15:36:20 wnc0s0qh last message repeated 1 time

Feb 11 10:15:53 wnc0s0qh IEMS: IEMS class_security.ver01 STAT=SUCCESS  SRC.USR=root
EVNT.TYPE =Authentication

Feb 11 10:15:53 wnc0s0qh last message repeated 1 time
```

Security log sample (/var/log/securitylog):

Dec 15 06:48:37 comp5iems su: 'su oracle' succeeded for root on /dev/???
Dec 15 06:48:56 comp5iems sshd[12755]: Accepted publickey for root from 192.168.47.2 port 64329 ssh2
Dec 15 08:42:36 comp5iems su[1200]: 'su root' failed for maint on /dev/pts/4
Dec 15 08:42:53 comp5iems su[2685]: 'su root' succeeded for maint on /dev/pts/4

The following table shows a summary of all Syslog facilities used by IEMS.

> ***Note:*** Only *Fault, Audit, and Security* streams are supported for use by downstream systems. Shaded entries are intended for support purposes only.

IEMS Northbound Syslog Facilities

Log Stream	Log file location on IEMS Server	Syslog facility
Fault	/var/log/iemsCustomerlog	local7
Audit	/var/log/auditlog	local0
Security	/var/log/securitylog /var/log/authlog/, auth (facility)	local3
Customer log	/var/log/customerlog	local1
Debug	/var/log/debuglog	local2
SSPFS	/var/log/sspfslog	local4
NPM	/var/log/npm_designlog	local5

Northbound SNMP - IETF MIB specification

IEMS provides an SNMP interface that forwards faults in trap messages and responds to SNMP requests.

The SNMP Northbound interface is based on an the IETF RFC 3877 standard which includes features such as alarm synchronization not available with NTSTD or SCC2.

This section provides a high-level description of how to support the IETF Alarm MIB draft defined in the DISMAN working group of the IETF. See the MIBs on the server in the locations specified in the table below. In this document, IEMS is the agent implementing the MIBs for the manager at the OSS level.

MIB Loading Sequence

The MIB loading sequence for a manager application is as follows:

These MIBs are available on the IEMS server in the locations noted in the following table.

MIB Loading Sequence

Load Order	MIB Name	IEMS Server File location
1	SNMPv2-CONF	(Not required by the IEMS server)
2	SNMPv2-SMI	/opt/nortel/iems/current/mibs
3	SNMPv2-TC	/opt/nortel/iems/current/mibs
4	SNMPv2-MIB	/opt/nortel/iems/current/mibs SNMPv2-MIB.txt
5	SNMP-FRAMEWORK-MIB	/opt/net-snmp/share/snmp/mibs/ SNMP-FRAMEWORK-MIB.txt
6	INET-ADDRESS-MIB	/opt/net-snmp/share/snmp/mibs/ INET-ADDRESS-MIB.txt
7	RFC1212	(Not required by the IEMS server)
8	RFC1155-SMI	/opt/nortel/iems/current/mibs
9	RFC1213-MIB	/opt/nortel/iems/current/mibs RFC1213-MIB.txt
10	RMON-MIB	/opt/nortel/iems/current/mibs/cicm RMON-MIB.txt
11	TOKEN-RING-RMON-MIB	/opt/nortel/iems/current/mibs/cicm TOKEN-RING-RMON-MIB.txt
12	RMON2-MIB	/opt/nortel/iems/current/mibs/cicm RMON2-MIB.txt
13	ALARM-MIB	/opt/nortel/iems/current/mibs/usp/ ALARM-MIB-disman-18.txt
14	IANA-ITU-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ IANA-ITU-ALARM-TC-disman-18.txt

Load Order	MIB Name	IEMS Server File location
15	ITU-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ ITU-ALARM-TC-disman-18.txt
16	ITU-ALARM-MIB	/opt/nortel/iems/current/mibs/usp/ ITU-ALARM-MIB-disman-18.txt
17	ITU-IANA-ALARM-TC	/opt/nortel/iems/current/mibs/usp/ ITU-IANA-ALARM-TC-disman-04.txt
18	NOTIFICATION-LOG-MIB	/opt/nortel/iems/current/mibs/usp/ NOTIFICATION-LOG-MIB-rfc3014.txt
19	NORTEL-MIB	/opt/nortel/iems/current/mibs/usp/nortel.mib
20	NORTEL-GENERIC-MIB	/opt/nortel/iems/current/mibs/usp/ nortelGenericMIBs-smi2.mib
21	ENTITY-MIB	/opt/nortel/iems/current/mibs/usp/ ENTITY-MIB-entmib-03.txt
22	ENTITY-STATE-MIB	/opt/nortel/iems/current/mibs/usp/ ENTITY-STATE-MIB-entmib-01.txt
23	NORTEL-ALARM-EXT-MIB	/opt/nortel/iems/current/mibs/usp/ nortel_alarm_ext_smi.txt
24	NORTEL-NMI-MIB	/opt/nortel/iems/current/mibs/usp/ nortelNMI-smi2.smi
25	NORTEL-NMI-ALARM-CLEAR-MIB	/opt/nortel/iems/current/mibs/usp/ nortelNMIalarmClear_smi.txt

Support for the IETF Alarm MIB is new to IEMS. The MIBs defined by the DISMAN working group of IETF are designed to allow surveillance of network elements. We have used this set of MIBs to present the state of our softswitch. The ALARM MIB presents a set of tables that contain the current alarm information for the device. The alarm MIB does not prescribe the notifications used to set and clear alarms on the device.

Nortel has provided an extension MIB to allow a manager to monitor the system alarm changes through SNMP notifications. These notifications are the primary interface for monitoring faults in the Succession node.

Nortel Alarm Extension MIB

This MIB defines notifications used for alarm asserts and clears in addition to data type definitions and tables related to notifications that can be sent.

A complete listing and description of our fault management MIB may be found in "IEMS Appendix 2: Nortel Alarm Extension MIB".

TABLE SUPPORT IN NORTEL ALARM EXTENSION MIB

The table nnExtAlarmActiveTable along with the AlarmActiveTable contains all the information required to resynchronize the northbound SNMP agent and to give the OSS a complete view of the active alarms within the scope of the IEMS.

The *nnExtAlarmStateTable* is not supported at this time.

NOTIFICATION SUPPORT IN NORTEL ALARM EXTENSION MIB

All notifications defined in this MIB are supported. All OIDs defined within the notifications are also populated. The alarm notifications include sequence numbers so the SNMP manager can determine if a message is missed. Specific formats are supported as described in the following table.

Alarm Notifications Varbinds

Variable name	Format	OID
alarmActiveResourceId	OID	.1.3.6.1.2.1.118.1.2.2.1.10
alarmActiveDateAndTime	DateandTime	.1.3.6.1.2.1.118.1.2.2.1.2
alarmActiveDescription	Human readable string	1.3.6.1.2.1.118.1.2.2.1.11
nnExtAlarmActiveEventType	Enum	.1.3.6.1.4.1.562.29.6.1.1.1.1
nnExtAlarmActiveProbableCause	Enum	.1.3.6.1.4.1.562.29.6.1.1.1.2
nnExtAlarmActiveAdditionalText	String	.1.3.6.1.4.1.562.29.6.1.1.1.3
nnExtAlarmActiveDocumentation Pointer	String: up to 4 chars + 3 digits	.1.3.6.1.4.1.562.29.6.1.1.1.4

Variable name	Format	OID

nnExtAlarmActiveResourceDescription	compType=compname;
	subcompType=subcompName;
	….. for as many levels of hierarchy is required to identify the alarmed entity
		.1.3.6.1.4.1.562.29.6.1.1.1.5

nnExtAlarmActiveManualClear	enum	.1.3.6.1.4.1.562.29.6.1.1.1.6
nnExtAlarmActiveSequenceNumber	Numeric	.1.3.6.1.4.1.562.29.6.1.1.1.7

These varbinds are included in all 5 of the alarm notifications supported by the IEMS. As defined all notifications in SNMP, *sysUpTime* and the OID of the notification are included in the varbinds for all notification types (see the following table). Each of the notifications signifies a different severity of the specified alarm. Notifications are defined for critical, major, minor, warning and cleared alarms. The notifications are defined in the table below.

Trap OIDs and Alarm Severity

Trap OID	Severity
.1.3.6.1.4.1.562.29.6.1.0.306	nnExtAlarmMessage
.1.3.6.1.4.1.562.29.6.1.0.305	nnExtAlarmCritical
.1.3.6.1.4.1.562.29.6.1.0.304	nnExtAlarmMajor
.1.3.6.1.4.1.562.29.6.1.0.303	nnExtAlarmMinor
.1.3.6.1.4.1.562.29.6.1.0.302	nnExtAlarmWarning
.1.3.6.1.4.1.562.29.6.1.0.301	nnExtAlarmClear

The nnExtAlarmMessage notifications can be used to send informational messages from IEMS. Because these notifications are information, reliability is not addressed. As illustrated in the table below, we populate with information in the message header and bodytext of our NTSTD and CUSTLOG feeds.

Message Notification Varbinds

Variable name	Format	OID
nnExtAlarmMessageResource	OID	.1.3.6.1.4.1.562.29.6.1.3.1.1

Variable name	Format	OID
nnExtAlarmMessageResourceDescription	String	.1.3.6.1.4.1.562.29.6.1.3.1.2
nnExtAlarmMessageDateAndTime	DateAndTime	.1.3.6.1.4.1.562.29.6.1.3.1.3
nnExtAlarmMessageDocumentationPointer	String	.1.3.6.1.4.1.562.29.6.1.3.1.4
nnExtAlarmMessageInfo	String	.1.3.6.1.4.1.562.29.6.1.3.1.5
nnExtAlarmMessageResource	OID	.1.3.6.1.4.1.562.29.6.1.3.1.1

OTHER DEFINITIONS IN THIS MIB

This MIB also defines OSI state variables that are not defined in the IETF Entity State MIB. These variables and tables are not supported at this time.

IETF RFC 3877 MIB Tables

There are several tables introduced by the IETF Alarm MIB Model. This document will discuss each table and intended use.

ALARM MODEL TABLE

This table defines the notifications used by IEMS to express alarm events. Notifications to communicate alarm asserts and clears have been defined by NortelNetworks in a separate MIB. These new notifications are defined in “Nortel Alarm Extension MIB” on page 101.

This table is not currently supported. This table is a static table and we will look to support this in some future release. This table provides model documentation to OSSes.

ALARM ACTIVE TABLE

This table contains a list of active alarms on IEMS and is supported. It, along with 2 other tables - the alarm active variable table and the Nortel Alarm Extension Table - provide a complete view of the active alarms within the scope of the IEMS.

The instance array of the Table is created used a readable string format of the AlarmActiveDateAndTime index value, not the OCTET STRING representation of it.

Limitations

If the OSS requires the AlarmActiveTable to be traversed, the OSS should issue sequential SNMP GETNEXT requests starting from the first column till the response reaches the end of the Table. The OSS will not be able to retrieve the values by giving incomplete instance values to query this table. If one uses a incomplete instance value to query a column, the response value will have the first row of the next immediate column in the AlarmActiveTable which will not be expected by the OSS. For example, the OSS will not be able to query the Table such that it can retrieve the Active Alarm List after a particular date by giving the instance value accordingly.

Walking the AlarmActiveTable
To walk the alarmActiveTable, for example, an OSS can send a snmp getnext pdu with the individual column varbinds of interest (i.e.,):

```
Getnext:

.iso.org.dod.internet.mgmt.mib-
2.alarmMIB.alarmObjects.alarmActive.alarmActiveTabl
e.alarmActiveEntry.alarmActiveEngineID

iso.org.dod.internet.mgmt.mib-
2.alarmMIB.alarmObjects.alarmActive.alarmActiveTabl
e.alarmActiveEntry.alarmActiveEngineAddressType

iso.org.dod.internet.mgmt.mib-
2.alarmMIB.alarmObjects.alarmActive.alarmActiveTabl
e.alarmActiveEntry.alarmActiveEntry.alarmActiveEngi
neAddress

..

..

iso.org.dod.internet.mgmt.mib-
2.alarmMIB.alarmObjects.alarmActive.alarmActiveTabl
e.alarmActiveEntry.alarmActiveSpecificPointer
```

This would result in the IEMS agent returning the first instance of these columns in the alarmActiveTable. The returned instance values varbinds in turn can be used in the subsequent getnext messages from the manager to traverse the associated columns in this table. This can be used until the IEMS agent returns that last instance (i.e., last row) in the associated table.

This can be identified by parsing the OID in the response varbind, reaching the next column or the next group if that is the last column in the table.

Table walk Limitations:
Due to limitations with using a DateAndTime value octet string as a table index, the IEMS agent does not support the ability to use partial indexes to walk the alarmActiveTable. The alarmActiveTable, for example, has a 3-part

index (alarmListName, alarmActiveDateAndTime, and alarmActiveDateAndTime). Beyond the initial getnext to get the first instance (i.e., first row) in this table, all getnext requests must include all 3 index instances to lexicographically step through the columns in this table. For example, a user can **not** do the following to attempt to get the next alarmActiveEngineID instance that is lexicographically greater then the provided date.

Example (Wrong request)

```
Getnext:
alarmActiveEngineID.alarmListName.alarmActiveDateAndTime
```

Instead of returning the next alarmActiveEngineID, the IEMS northbound SNMP agent will return the first instance in the next column (In this example it would be the alarmActiveEngineAddressType).

Indexes into this table are: *alarmListName, alarmActiveDateAndTime, alarmActiveIndex*. AlarmListName matches the index nlmLogName for nlmLogTable from RFC3014 (Notification Log MIB). For our Succession IEMS table we use the string "Nortel_fault".

The following table describes expected values for entries in this table.

IETF Alarm Active Entry

Sequence Field	Default Value
alarmListName	Nortel_fault
alarmActiveDateAndTime	none
alarmActiveIndex	Numerical index defined by agent, unique in table
alarmActiveEngineID	IEMS agent engine ID in SNMPv3; empty string in SNMPv2
alarmActiveEngineAddressType	Inet address type (IPv4)
alarmActiveEngineAddress	IPv4 address of active IEMS agent
alarmActiveContextName	“”
alarmActiveVariables	12 = number of fields in our alarm set notifications + 2 mandatory entries per alarm
alarmActiveNotificationID	OID of notification sent for this alarm set
alarmActiveResourceId	OID that describes this entry in the Active Alarm Table
alarmActiveDescription	none

Sequence Field	Default Value
alarmActiveLogPointer	not implemented - default = 0.0
alarmActiveModelPointer	not implemented - default = 0.0
alarmActiveSpecificPointer	not implemented - default = 0.0

ALARM ACTIVE VARIABLE TABLE

Alarm Active variable table contains the varbinds for all the active alarm notifications. The indexes to the table are: *alarmListName, alarmActiveIndex, alarmVariableIndex*. For each alarm in the alarm active table there will be 12 entries in the alarm active variable table. The index *alarmVariableIndex* will be from 1 to 12 (also from 1 to alarmActiveVariables in the alarmActiveTableEntry). The notifications contain some varbinds that are not in the standard table so the OSS can index into this table to get the additional data. (Similarly, the OSS can index into the Nortel Extension Active Alarm Table for the additional information as well.)

The instance array of the Table is created used a readable string format of the AlarmActiveDateAndTime index value, not the OCTET STRING representation of it.

Fields in this table for each alarm are as follows:

Alarm Active Variable Table

Alarm Active Variable Entry	Notification Varbind	Default Value
alarmActiveVariableIndex 1	sysUpTime	sysUpTime
alarmActiveVariableIndex 2	snmpTrapOID	snmpTrapOID
alarmActiveVariableIndex 3	alarmActiveResourceId	OID that describes this entry in the Active Alarm Table
alarmActiveVariableIndex 4	alarmActiveDescription	none
alarmActiveVariableIndex 5	alarmActiveDateAndTime	none
alarmActiveVariableIndex 6	nnExtAlarmActiveEventType	none
alarmActiveVariableIndex 7	nnExtAlarmActiveProbableCause	none
alarmActiveVariableIndex 8	nnExtAlarmActiveAdditionalText	none
alarmActiveVariableIndex 9	nnExtAlarmActiveDocumentationPointer	This is often logname & number

Alarm Active Variable Entry	Notification Varbind	Default Value
alarmActiveVariableIndex 10	nnExtAlarmActiveResource Description	none
alarmActiveVariableIndex 11	nnExtAlarmActiveManualCl ear	none
alarmActiveVariableIndex 12	nnExtAlarmActiveSequence Number	none

ALARM CLEAR TABLE

Not supported.

Manual clears are performed with SNMP SET operations using the alarmActiveIndex of the alarm to be cleared. See section " Manual Clear" on page 117 for details.

ACTIVE ALARM STATS TABLE

Not supported.

ITU ALARM ACTIVE TABLE

Not supported.

ITU ALARM ACTIVE VARIABLE TABLE

Not supported.

ITU ALARM ACTIVE STATS TABLE

Supported.

NLM LOG TABLE (RFC 3014)

NLM Log Table is defined in IETF RFC 3014. Implementation of the MIB is provided to support incremental resynchronization of the OSS. The OSS SNMP managers can reach into the nlmLogTable to get missed events. See Notification Log MIB (RFC 3014): http://www.ietf.org/rfc/rfc3014.txt?number=3014.

The Notification Log MIB has 3 different MIB groups:

- configuration parameters dealing with log storage and reporting
- statistics of log reporting
- the actual history of notifications

Configuration

Configuration defines the size and the aging criteria of the *nlmLogTable*. Table *nlmConfigLogTable* also defines the named log entries supported in the

nlmLogTable. We use a specific named log entry for allowing fault resync. This table also defines filtering of these logs.

Each entry in the config log table contains: *nlmLogName, nlmConfigLogFilterName, nlmConfigLogEntryLimit, nlmConfigLogAdminStatus*. This table enables Alarm notification resynchronization. The first and only entry in this table has an *nlmLogName* that matches the *alarmListName* index for the active alarm tables above. This index is "Nortel_fault."

nlmConfigLogFilterName is defined as "default". We do not support the correlation of this value to any specific data in the *snmpNotifyFilterTable* in the SNMP Notification MIB.

nlmConfigLogEntryLimit defines the size of the log table. This defines the number of alarm events that are available to the SNMP manager through the SNMP agent. Since there is only one entry in this table for Nortel_fault, this value is over-ridden by *nlmConfigGlobalEntryLimit*.

> ***Note:*** It is recommended that *nlmConfigGlobalEntryLimit* be set to a minimum value as it maintains this history in memory. Do **not** set this value to zero. Setting this value to zero will lead to unlimited entries being saved and lead to potential resource issues in the system.

nlmConfigLogAdminStatus is set to enabled (1).

nlmConfigLogOperStatus is set to noFilter (3).

nlmConfigLogStorageType is a storageType OID. Data associated with this entry is considered volatile and will be lost when the agent is restarted.

SNMP sets for the configuration items in this table are not supported.

Statistics

The statistics group contains two scalars and a table. The table is required for the resync algorithm. The table *nlmStatsLogTable* augments the *nlmConfigLogTable* and has only two values in each entry: *nlmStatsLogNotificationsLogged* and *nlmStatsLogNotificationsBumped*. Because this table augments the *nlmConfigLogTable*, the index for these notifications uses the same key - "Nortel_fault"

nlmStatsLogNotifications for the named logs in Nortel_fault is the sequence number (*nnExtAlarmActiveSequenceNumber*) sent in IEMS notifications of the faults. This also provides the secondary index into the *nlmLogTable* for notifications that have been missed - as detected through sequence numbers in those notifications.

It is the responsibility of the SNMP agent sending fault notifications to increment the *nlmStatsLogNotificationsLogged* and include the value in the varbinds of that notification as documented.

nlmStatsGlobalNotificationsBumped defines the number of logs that have been removed or “bumped” from the log table due to the limits imposed by the *nlmConfigGlobalEntryLimit* setting.

Log Table

The *nlmLogTable* contains the history of notifications sent to the manager. The indices are: *nlmLogName* and *nlmLogIndex*. *nlmLogName* is "Nortel_fault" and the *nlmLogIndex* is the sequence number in the proprietary notifications.

This section defines two tables: *nlmLogTable* and *nlmLogVariableTable*. The first provides the indices for retrieving missed notifications, and the second contains the varbinds for the notifications. We have 2 different size alarm notifications (in terms of number of varbinds)- alarm assert notifications are all the same size, and alarm clear notifications are slightly smaller (1 varbind). Only alarm notifications are stored in the log table, message notifications are not logged in this table.

The structure and implementation of the *nlmLogVariableTable* is the same as that of the *alarmActiveVariableTable* and is not described further.

Connecting to the NB feed:

The default SNMP Port in which the agent is listening is 8001. This port is configurable through the IEMS client. User can also disable the SNMP agent if he wishes. OSS has to register its SNMP manager host and port to which the traps are to be sent.

Connection Reliability

There are several scenarios which must be considered by an SNMP manager to ensure that the alarms presented at the OSS layer will be in sync with the actual alarms maintained on the device. Resynchronization will be required when either the OSS or the IEMS system goes through a restart, or when a lost trap is detected. See section “ Message Sequences and Manager Operations” on page 115 for details on resynchonization of active alarms.

Lost Traps

If the OSS detects a lost trap via an out-of-order sequence number, the OSS must either try to recover the lost sequence numbers from the notification log table or re-synchronize from the the active alarm table. The notification log MIB will contain the last 25 traps sent. If the sequence number delta is within this range, the notification log table can be used to obtain missed traps. Otherwise, a read of the active alarm table must be used to determine the active alarms in the system.

Additionally, OSS can poll the sequence number of the last alarm or clear sent from the agent. The sequence number of last notification sent will be in the *nlmStatsLogNotifications* table in the *nlmStatsLogNotificationsLogged* variable in the "Nortel_fault" entry as described above.

Note: Since there is only one entry in this table, the scalar *nlmStatsGlobalNotificationsLogged* can also be used to obtain this value.

SNMP Alarm Events & Correlation

The *alarmActiveResourceID* uniquely identifies an alarm occurrence in the system. To correlate a clear notification to the appropriate assert, the *alarmActiveResourceID* must be used.

Event Types and ProbableCauses

Each alarm notification and record in the alarm table includes event type and probable cause. Values for these fields are define in the IANA-ITU-ALARM-TC MIB table. These values come from both the X.7xx and M.3100 series of standards.

Alarm Event Type Format:

IANAItuEventType - Valid values for this entry are provided here for convenience.

other (1),

communicationsAlarm (2),

qualityOfServiceAlarm (3),

processingErrorAlarm (4),

equipmentAlarm (5),

environmentalAlarm (6),

integrityViolation (7),

operationalViolation (8),

physicalViolation (9),

securityServiceOrMechanismViolation (10),

timeDomainViolation (11)

Probable Cause Format:

IANAItuProbableCause - Valid values for this entry are provided here for convenience.

aIS (1), callSetUpFailure (2), degradedSignal (3), farEndReceiverFailure (4), framingError (5), lossOfFrame (6), lossOfPointer (7), lossOfSignal (8), payloadTypeMismatch (9), transmissionError (10), remoteAlarmInterface (11), excessiveBER

(12), pathTraceMismatch (13), unavailable (14), signalLabelMismatch (15), lossOfMultiFrame (16), receiveFailure (17), transmitFailure (18), modulationFailure (19), demodulationFailure (20), broadcastChannelFailure (21), connectionEstablishmentError (22), invalidMessageReceived (23), localNodeTransmissionError (24), remoteNodeTransmissionError (25), routingFailure (26), backplaneFailure (51), dataSetProblem (52), equipmentIdentifierDuplication (53), externalIFDeviceProblem (54), lineCardProblem (55), multiplexerProblem (56), nEIdentifierDuplication (57), powerProblem (58), processorProblem (59), protectionPathFailure (60), receiverFailure (61), replaceableUnitMissing (62), replaceableUnitTypeMismatch (63), synchronizationSourceMismatch (64), terminalProblem (65), timingProblem (66), transmitterFailure (67), trunkCardProblem (68), replaceableUnitProblem (69), realTimeClockFailure (70), antennaFailure (71), batteryChargingFailure (72), diskFailure (73), frequencyHoppingFailure (74), iODeviceError (75), lossOfSynchronisation (76), lossOfRedundancy (77), powerSupplyFailure (78), signalQualityEvaluationFailure (79), tranceiverFailure (80), protectionMechanismFailure (81), protectingResourceFailure (82), airCompressorFailure (101), airConditioningFailure (102), airDryerFailure (103), batteryDischarging (104), batteryFailure (105), commercialPowerFailure (106), coolingFanFailure (107), engineFailure (108), fireDetectorFailure (109), fuseFailure (110), generatorFailure (111), lowBatteryThreshold (112), pumpFailure (113), rectifierFailure (114), rectifierHighVoltage (115), rectifierLowFVoltage (116), ventilationsSystemFailure (117), enclosureDoorOpen (118), explosiveGas (119), fire (120), flood (121), highHumidity (122), highTemperature (123), highWind (124), iceBuildUp (125), intrusionDetection (126), lowFuel (127), lowHumidity (128), lowCablePressure (129), lowTemperatue (130), lowWater (131), smoke (132), toxicGas (133), coolingSystemFailure (134), externalEquipmentFailure (135), externalPointFailure (136), storageCapacityProblem (151), memoryMismatch (152), corruptData (153), outOfCPUCycles (154), sfwrEnvironmentProblem (155), sfwrDownloadFailure (156), lossOfRealTimel (157), applicationSubsystemFailure (158), configurationOrCustomisationError (159), databaseInconsistency (160), fileError (161), outOfMemory (162), softwareError (163), timeoutExpired (164), underlayingResourceUnavailable (165), versionMismatch (166), adapterError (500), applicationSubsystemFailture (501), bandwidthReducedX733 (502), callEstablishmentError (503), communicationsProtocolError (504), communicationsSubsystemFailure (505), configurationOrCustomizationError (506), congestionX733 (507), coruptData (508), cpuCyclesLimitExceeded (509),

dataSetOrModemError (510), degradedSignalX733 (511), dteDceInterfaceError (512), enclosureDoorOpenX733 (513), equipmentMalfunction (514), excessiveVibration (515), fileErrorX733 (516), fireDetected (517), framingErrorX733 (518), heatingVentCoolingSystemProblem (519), humidityUnacceptable (520), inputOutputDeviceError (521), inputDeviceError (522), lanError (523), leakDetected (524), localNodeTransmissionErrorX733 (525), lossOfFrameX733 (526), lossOfSignalX733 (527), materialSupplyExhausted (528), multiplexerProblemX733 (529), outOfMemoryX733 (530), ouputDeviceError (531), performanceDegraded (532), powerProblems (533), pressureUnacceptable (534), processorProblems (535), pumpFailureX733 (536), queueSizeExceeded (537), receiveFailureX733 (538), receiverFailureX733 (539), remoteNodeTransmissionErrorX733 (540), resourceAtOrNearingCapacity (541), responseTimeExecessive (542), retransmissionRateExcessive (543), softwareErrorX733 (544), softwareProgramAbnormallyTerminated (545), softwareProgramError (546), storageCapacityProblemX733 (547), temperatureUnacceptable (548), thresholdCrossed (549), timingProblemX733 (550), toxicLeakDetected (551), transmitFailureX733 (552), transmiterFailure (553), underlyingResourceUnavailable (554), versionMismatchX733 (555), -- The following are defined in X.736 authenticationFailure (600), breachOfConfidentiality (601), cableTamper (602), delayedInformation (603), denialOfService (604), duplicateInformation (605), informationMissing (606), informationModificationDetected (607), informationOutOfSequence (608), keyExpired (609), nonRepudiationFailure (610), outOfHoursActivity (611), outOfService (612), proceduralError (613), unauthorizedAccessAttempt (614), unexpectedInformation (615), other (1024).

Northbound Fault Mapping

The following table shows the correlation between the fields of the supported Northbound fault feeds.

Northbound Fault Format Summary

Row#	IEMS Schema	SYSLOG	NTSTD	SCC2	SNMP
1.	Severity 1= critical 2 = major 3 = minor 4= warning 5 =clear 6 = info	Alarm Severity CRIT =1, MAJOR =2, MINOR =3, NONE =4,5,6 None	1 = '***' 2 = '** ' 3 = '* ' 4,5,6 = ' ' 6 = ' '	1 = '*C' 2 = '**' 3 = '* ' 4,5,6 = ' ' 6 = ' '	Based on the severity the concerned alarm, appropriate notification will be sent. nnExtNotificationPrefix : .1.3.6.1.4.1.562.29.6.1.0 **Alarm Events:** nnExtAlarmCritical = 1 .1.3.6.1.4.1.562.29.6.1.0.305 nnExtAlarmMajor = 2 .1.3.6.1.4.1.562.29.6.1.0.304 nnExtAlarmMinor = 3 .1.3.6.1.4.1.562.29.6.1.0.303 nnExtAlarmWarning = 4 .1.3.6.1.4.1.562.29.6.1.0.302 nnExtAlarmClear = 5 .1.3.6.1.4.1.562.29.6.1.0.301 **Non-alarm Events:** nnExtAlarmMessage = 6 .1.3.6.1.4.1.562.29.6.1.0.306
2.	Time(long)	MMM DD hh:mm:ss -> UTC time	MMM DD hh:mm:ss UTC time	UTC -> Minute Indicator	**Alarm event:** alarmActiveDateAndTime .1.3.6.1.2.1.118.1.2.2.1.2 **Non-alarm event:** nnExtAlarmMessageDateAndTime .1.3.6.1.4.1.562.29.6.1.3.1.3

Northbound Fault Format Summary

Row#	IEMS Schema	SYSLOG	NTSTD	SCC2	SNMP
3.	LogName	Report Name	LogName	LogName	Log name&number shown in varbind **Alarm event:** nnExtAlarmActiveDocumentationPointer .1.3.6.1.4.1.562.29.6.1.1.1.4 **Non-alarm event:** nnExtAlarmMessageDocumentationPointer .1.3.6.1.4.1.562.29.6.1.3.1.4
4.	LogNumber	ReportNumber	LogNumber	LogNumber	Log name&number shown in varbind **Alarm event:** nnExtAlarmActiveDocumentationPointer .1.3.6.1.4.1.562.29.6.1.1.1.4 **Non-alarm event:** nnExtAlarmMessageDocumentationPointer .1.3.6.1.4.1.562.29.6.1.3.1.4
5.	Threshold	-	Threshold '+' set ' ' not set	Threshold '+' set ' ' not set	not supported
6.	ID(Integer)	NotificationID	NotificationID	NotificationID	last integer in the OID specified by: alarmActiveResourceID .12.78.111.114.116.101.108.95.102.97.117.108.116.25.50.48.48.52.45.49.45.56.44.51.58.50.49.58.53.55.46.49.44.43.48.53.58.51.48**.10**
7.	Sequence Number	Generated Sequence Number	Global Sequence Number (generated)	Global Sequence Number (generated)	**Alarm event:** nnExtAlarmActiveSequenceNumber .1.3.6.1.4.1.562.29.6.1.1.1.7
8.	EventType	EventType	EventType	EventType	**Alarm event:** not supported
9.	EventLabel	EventLabel	EventLabel	EventLabel	not supported
10.	Equipment Identifier	Location:	Location:	Location:	Not supported

Northbound Fault Format Summary

Row#	IEMS Schema	SYSLOG	NTSTD	SCC2	SNMP
11.	Probable Cause	Cause	Cause	Cause	**Alarm event:** nnExtAlarmActiveProbableCause .1.3.6.1.4.1.562.29.6.1.1.1.2
12.	Category	Category:	Category:	Category:	**Alarm event:** nnExtAlarmActiveEventType .1.3.6.1.4.1.562.29.6.1.1.1.1
13.	Specific Problem Note: Specific Problem is now a part of the nnExtAlarmActiveAdditionalText VarBind.				**Alarm event:** alarmActiveDescription: .1.3.6.1.2.1.118.1.2.2.1.11
14.	NotificationID	not sent	not sent	non sent	not sent
15.	ComponentID	ComponentID	ComponentID	ComponentID	**Alarm event:** nnExtAlarmActiveResourceDescription .1.3.6.1.4.1.562.29.6.1.1.1.5 **Non-alarm event:** nnExtAlarmMessageResourceDescription .1.3.6.1.4.1.562.29.6.1.3.1.2
16.	BodyText	BodyText	BodyText	BodyText	The mmessage or the description of the event

Message Sequences and Manager Operations

Raise Alarm

This sequence applies t the following alarm event types:

- nnAlarmWarning
- nnAlarmMinor
- nnAlarmMajor
- nnAlarmCritical

1 IEMS forwards alarm from device. The trap contains references to the 12 varbinds depicted in Table , “Alarm Active Variable Table,” on page 106.

2 The OSS receives the alarm and notes the resource ID of the alarm event to allow correlation with a subsequent alarmClear event. IEMS adds the alarm entry to the *alarmActiveTable*, *alarmActiveVariableTable*, and *nnExtAlarmActiveTable*. The *nlmLogTable* and *nlmLogVariableTable* also

maintain a rolling log of the last n alarm events received - where n is defined by the variable *nlmConfigGlobalEntryLimit*.

Clear Alarm

1. IEMS forwards clearAlarm event from device. The trap contains references to all varbinds listed in Please refer to " Alarm Active Variable Table" on page 106. except for *nnExtAlarmActiveManualClear* - which is not included in this message.
2. The OSS receives the clear event and matches its resource ID in **alarmActiveResourceId** against the ID of its corresponding alarm event in the alarmActiveTable.

   The corresponding alarm entry is removed from all active alarm tables:

   alarmActiveTable

   alarmActiveVariableTable

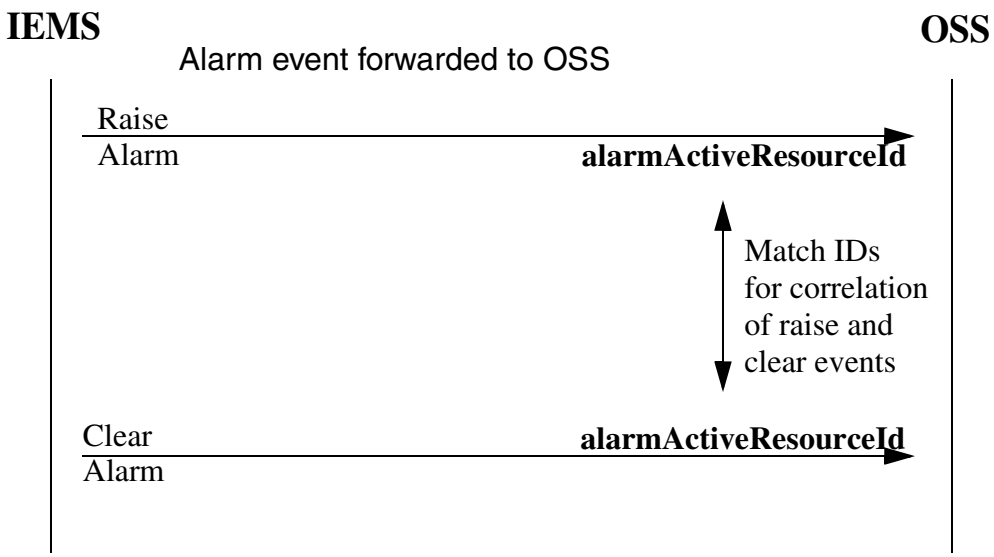
   nnExtAlarmActiveTable

   An entry is made in the log notification tables for the CLEAR event.

   nlmLogTable

   nlmLogVariableTable

Alarm Raise & Clear Correlation



Manual Clear

Each alarm event contains information that indicates whether it can be manually cleared. The value in the varbind *nnExtAlarmActiveManualClear* makes this determination and can have the following values:

other (1),

forbidden (2),

required (3),

optional (4)

Note: Alarms with a value of *forbidden* in this field cannot be manually cleared.

Eligible alarms can be manually cleared by sending a SET request to the alarm clear interface variable *nortelNMIalarmClear (*.1.3.6.1.4.1.562.29.1.8.1*)* in the NORTEL_NMI-ALARM-CLEAR-MIB. The alarm to be cleared can be specified by using the *alarmActiveIndex* of the target alarm. The value of the *alarmActiveIndex* is stored as the last element in the *alarmActiveResourceId*.

Example: An alarm is generated and stored in the *alarmActiveTable* with the following values:

alarmsListName:**Nortel_fault**

alarmActiveDateAndTime:2004-1-8,3:21:57.1,+05:30

alarmActiveIndex:**10**

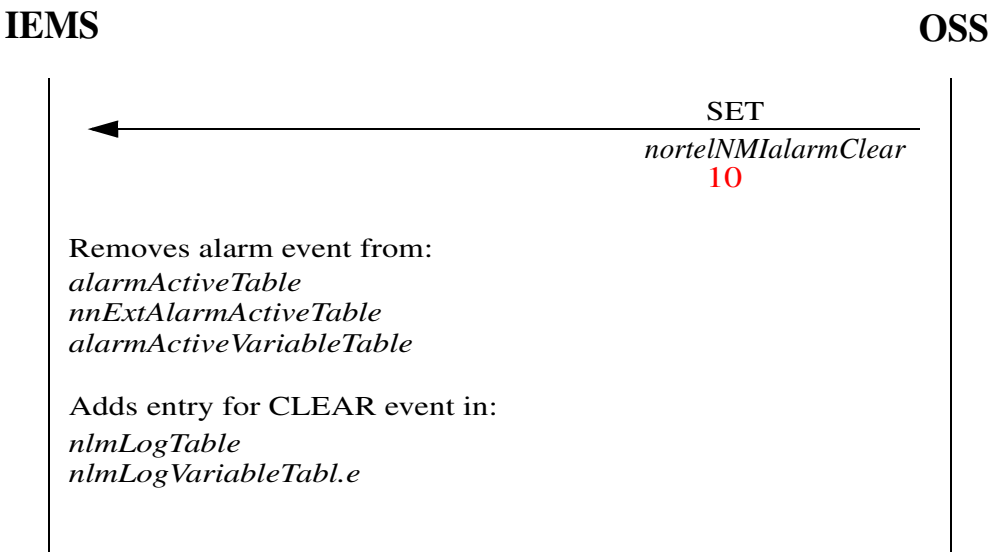
The resulting alarmAcitveResourceId will be:

alarmAcitveResourceId.**12.78.111.114.116.101.108.95.102.97.117.108.116.**25.50.48.48.52.45.49.45.56.44.51.58.50.49.58.53.55.46.49.44.43.48.53.58.51.48.**10**

Note: *alarmActiveResourceId* is shown fully encoded.

The SET request will be sent with a value of 10. The corresponding alarm entry is removed from the alarmActiveTable,alarmActiveVariableTable, and nnExtAlarmActiveTable. A corresponding entry for the manual clear is then made in *nlmLogTable* and *nlmLogVariableTable.* See the following figure.

Manual Clear of Alarm Event



Detecting System Restarts

Before an alarm event is forwarded to a downstream manager, the IEMS assigns the current system up-time of the server to the alarm contents. As discussed previously, it can be found in the *sysUpTime* varbind of the alarm. On restart of the IEMS server, this value is initialized to 0 to signal downstream systems of the event. The OSS can use *sysUptime* to monitor system restarts as follows:

Correlation with sequence numbers

Since *sysUpTime* will always increase with each sequential alarm event, restart conditions can be detected if the following condition is met:

(*sysUpTime* of current event) < (*sysUpTime* of previous event)

Restart Recovery

When the OSS determines that IEMS has been restarted, it must perform a full reload of the active alarms in the system to synchronize its data with the agent. See "Full Resync of Active Alarms" on page 119 for details.

Detection of Missing Logs

Each alarm event generated by IEMS contains a unique sequence number that can be used to detect lost notifications. Once an OSS identifies a missing sequence number, it can be re-queried from the IEMS server if the following condition is met:

(sequence# of latest event) - (sequence# of missing event)

<= *nlmConfigGlobalEntryLimit (*default = 25*)*

If this condition is met, then the missing log can be recovered. See “ Incremental Resync of missing logs”.

Otherwise, a full resynchronization of the alarm tables will be required. See “Full Resync of Active Alarms” on page 119.

Full Resync of Active Alarms

There are two scenarios for which an SNMP manager will be required to perform a complete reload of the active alarms from IEMS:

- on startup of the management application
- when missing alarm notifications are sufficiently old to have been rotated out of the *nlmLogTable*. This table maintains a snapshot of the most recent 25 alarm events. If the missing sequence number cannot be found in this table, then a reload of all active alarms is required.

Active alarm data resides in:

alarmActiveTable

nnExtAlarmActiveTable

A full table read must be performed on the varbinds in Please refer to “ Required Varbinds for Active Alarm resync” on page 119. to perform the resync:

Required Varbinds for Active Alarm resync

Varbind	OID
snmpTrapOID	.1.3.6.1.6.3.1.1.4.1
alarmActiveResourceId	.1.3.6.1.2.1.118.1.2.2.1.10
alarmActiveDateAndTime	.1.3.6.1.2.1.118.1.2.2.1.2
alarmActiveDescription	.1.3.6.1.2.1.118.1.2.2.1.11
nnExtAlarmActiveEventType	.1.3.6.1.4.1.562.29.6.1.1.1.1
nnExtAlarmActiveProbableCause	.1.3.6.1.4.1.562.29.6.1.1.1.2
nnExtAlarmActiveAdditionalText	.1.3.6.1.4.1.562.29.6.1.1.1.3
nnExtAlarmActiveDocumentationPointer	.1.3.6.1.4.1.562.29.6.1.1.1.4
nnExtAlarmActiveResourceDescription	.1.3.6.1.4.1.562.29.6.1.1.1.5
nnExtAlarmActiveManualClear	.1.3.6.1.4.1.562.29.6.1.1.1.6
nnExtAlarmActiveSequenceNumber	.1.3.6.1.4.1.562.29.6.1.1.1.7

Note: These varbinds are retrieved from the *alarmActiveVariableTable*

The manager can perform a full resync with the *alarmActiveTable* in a similar way to that used when performing an incremental resync from the *nlmLogVariableTable* (see " Incremental Resync of missing logs"). As stated earlier, each alarm entry in the *alarmActive* table has a corresponding entry for all of the alarm components in the *alarmActiveVariable* table. The complete set of alarm data can be retrieved for each alarm by first retrieving the *alarmActiveIndex* of the entry in the *alarmActiveTable*, and then using this index to request its corresponding entries from the *alarmActiveVariableTable*. These steps can be summarized as follows:

1. Poll the IEMS server for the latest sequence number. Issue a GET request on *nlmStatsLogNotificationsLogged*. Perform steps 2 to 3until all alarms have been retrieved from IEMS.
2. Derive the list of indices to the *alarmActive* table by performing a series of GETNEXT requests on any one of its columns. The *alarmActiveIndex* for entries can be parsed from this data.
3. For each *alarmActiveIndex* derived in step 2, determine the alarm type perform a GET request on the *alarmActiveVariableTable* all index fields for the alarm type. The specific index fields requested will be based on the alarm type specified by the *snmpTrapOID* in index 2. See " Incremental Resync of missing logs" for a description of varbinds used in the different event types. This step essentially performs repeated incremental resync operations until complete.
4. Based on the alarm type determined is step 3, request all varbinds (GET) in the *alarmActiveVariableTable* for the constructed index

   alarmListName = Nortel_fault

   alarmActiveIndex = (derived in step 2)

   alarmActiveVariableIndex (1-n) - depends on alarm type found in step 3

Note: The *alarmActiveVariableTable* and *nlmLogVariableTable* contain the same indexed alarm information and are accessed in similar ways. The main difference between the two is that *alarmActiveVariableTable* uses the *alarmActiveIndex* as one of its key components, whereas the *nlmLogVariableTable* uses the sequence number.

Incremental Resync of missing logs

An OSS can monitor sequence numbers from alarm events to detect missing notifications. If a missing notification is found (as described in " Detection of Missing Logs"), then it can be queried from the *nlmLogVariableTable* using the sequence number.

1. OSS detects missing sequence number

2 Missing alarm events can be recovered from the *nlmLogVariableTable* using the sequence number. Depending on the alarm event type, different numbers of varbinds will be present in the table for the entry.

The following table shows an example of the varbinds that would be used to recover a missing RAISE event with a sequence number of "***1390***". RAISE events include the following alarm types:

nnExtAlarmWarning (.1.3.6.1.4.1.562.29.6.1.0.302)

nnExtAlarmMinor (.1.3.6.1.4.1.562.29.6.1.0.303)

nnExtAlarmMajor (.1.3.6.1.4.1.562.29.6.1.0.304)

nnExtAlarmCritical (.1.3.6.1.4.1.562.29.6.1.0.305)

Table , "nlmLogVariableTable varbinds for recovery of lost CLEAR notification," on page 123 shows an example of the varbinds that would be used to recover a missing CLEAR event with a sequence number of "***1390***". CLEAR events are specified by the following OID:

nnExtAlarmClear (.1.3.6.1.4.1.562.29.6.1.0.301)

The alarm type can be determined by examining the value of the snmpTrapOID of the missed alarm. For both alarm types, this value is assigned index 2 of the nlmLogVariable table and can be queried with the OIDs shown in the following table. The alarm type will determine the mapping for the remining fields in the notification message.

nlmLogVariableTable varbinds for recovery of lost RAISE notification

nlmLogVariableTable Index Variable	OID (nlmLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 12)	Notification Varbind Represented
nlmLogVariableIndex 1	nlmLogVariableTimeTicksVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.1	sysUpTime
nlmLogVariableIndex 2	nlmLogVariableOidVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.2	snmpTrapOID
nlmLogVariableIndex 3	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.1390.3	alarmActiveResourceId

nlmLogVariableTable varbinds for recovery of lost RAISE notification

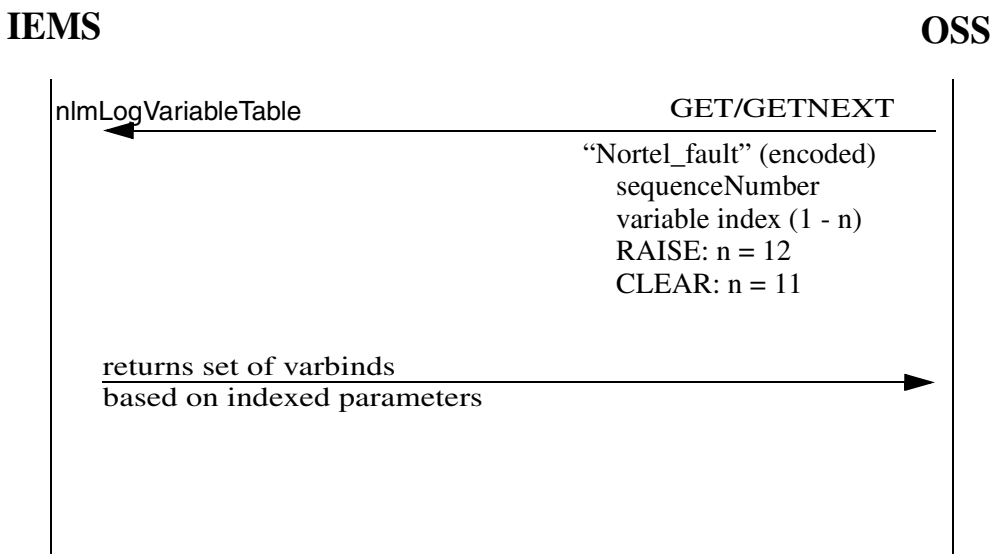
nlmLogVariableTable Index Variable	OID (nlmLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 12)	Notification Varbind Represented
nlmLogVariableIndex 4	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.4	alarmActiveDescription
nlmLogVariableIndex 5	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.5	alarmActiveDateAndTime
nlmLogVariableIndex 6	nlmLogVariableInteger32Val.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.6	ituAlarmEventType
nlmLogVariableIndex 7	nlmLogVariableInteger32Val.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.7	ituAlarmProbableCause
nlmLogVariableIndex 8	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.8	ituAlarmAdditionalText
nlmLogVariableIndex 9	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.9	nnItuAlarmActiveDocumentationPointer
nlmLogVariableIndex 10	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.10	nnItuAlarmActiveResourceDescription
nlmLogVariableIndex 11	nlmLogVariableInteger32Val.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.11	nnItuAlarmActiveManualClear (**not** present in CLEAR events, see next table)
nlmLogVariableIndex 12	nlmLogVariableInteger32Val.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.12	nnItuAlarmActiveSequenceNumber

nlmLogVariableTable varbinds for recovery of lost CLEAR notification

nlmLogVariableTable Index Variable	OID (nlmLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 11)	Notification Varbind Represented
nlmLogVariableIndex 1	nlmLogVariableTimeTicksVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.1	sysUpTime
nlmLogVariableIndex 2	nlmLogVariableOidVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.2	snmpTrapOID
nlmLogVariableIndex 3	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.3	alarmActiveResourceId
nlmLogVariableIndex 4	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.4	alarmActiveDescription
nlmLogVariableIndex 5	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.5	alarmActiveDateAndTime
nlmLogVariableIndex 6	nlmLogVariableInteger32Val.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.6	ituAlarmEventType
nlmLogVariableIndex 7	nlmLogVariableInteger32Val.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.7	ituAlarmProbableCause
nlmLogVariableIndex 8	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.8	ituAlarmAdditionalText
nlmLogVariableIndex 9	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.9	nnItuAlarmActiveDocumentationPointer
nlmLogVariableIndex 10	nlmLogVariableOctetStringVal.12.78.111.114.116.101.108.95.102.97.117.108.116.**1390**.10	nnItuAlarmActiveResourceDescription

nlmLogVariableTable Index Variable	OID (nlmLogName = "Nortel_fault" (encoded) Sequence# = 1390 Index = 1 - 11)	Notification Varbind Represented
nlmLogVariableIndex 11	nlmLogVariableInteger32Val .12.78.111.114.116.101.108 .95.102.97.117.108.116.**139 0**.11	nnItuAlarmActiveSequenceNumber

Recovery of missing alarm by sequence number



Northbound Performance Interface

IEMS Performance Interface Specification

The Northbound performance interface provides the customer a single reporting interface for the managed network. This has been acheived through the defintion of a "Common Performance Record format" (CPR-F). The common format maps operational statistics from across network elements to a common set of metrics to provide a network-level view of performance.

The Common Performance Record format specification is defined using a standardized XML interface. It provides a full definition of the normalized containment hierarchy describing performance statistics for reporting network components. PM collection jobs configured in IEMS can report device metrics in either XML or CSV formats.

The following is a list of devices that support collection of performance data in the SN09 release, PP8600, STORM, MS2000, Session Server-Trunks (platform PMs only), MAS, MCS, MCS Mgr, FPM, MG15000, SAM21, IEMS, UAS, GWC, USP, MG9K, and SSPFS.

XML

If XML is selected as the output format, then the data is collected and saved as an ACSII file in the format defined by the CPR-F XML Schema Document. The format specification below provides a full description of the normalized representation of PM data for supported network elements.

Conversion to CSV

When CSV output is configured in the collection job, data is initially transformed to the XML format described above. An additional step then converts the XML file to its corresponding CSV representation. There is no loss of information during this process. Net content represented by each output is identical.

The next section defines the CPR-F in terms of its XML structure followed by a discussion of its *conversion* to CSV format.

Also, collected CSV and XML performance files can be transfered from IEMS to an OSS system by configuring a transfer job for the performance files. The transfer can be done using FTP or SFTP.

For more information on configuring, retrieving, and transfering performance measurements through IEMS, see NN10327-711 - IEMS Performance Management Guide.

The Common Performance Record XML Format

For examples of each of the supported PM files, refer to the section in this chapter entitled “IEMS Supported Devices” on page 154.

Overview

The Common Performance record is an XML document specified using an XML Schema Document (XSD).

There are two major aspects to encoding performance measurements – identifying the source of the measurements within the network and recording the measurement data itself.

The CPR-F uses an XML containment structure to indicate the source point in the network of the performance measurements. A typical performance measurement may have originated in an NE and then been passed up to an element management system (EMS). The EMS in turn may have passed the measurements along to an Operations Support System (OSS).

For this particular case, the common record would contain an XML element representing the management system (the OSS) which ultimately received the set of performance measurements. Within this OSS element would be an element representing the EMS which forwarded the measurements to the OSS.

And within this EMS element, there would be an XML element representing the NE (network element) from which the PMs were obtained. The NE element may itself contain another XML element representing the sub-component in the NE which generated the measurement.

The measurement data itself would also be encoded in one or more XML elements. These data elements would be contained within the sub-component element above.

XML Elements

The common performance record format uses thirteen major elements to encode performance information:

The *PMFile* element is the top-level element and contains all other elements.

The *System* element, *Entity* element and *SubEntity* element are used to relate the measurements to some origination point in the network and to capture their path through the management systems.

The *SingleValues* & *SingleValue* elements, the *GroupOfValues* & *GroupValue* elements and the *Table, Labels, Label, RowOfValues* & *RowValue* elements may all be used to capture the performance measurement information itself.

Encoding Source Identification for Performance Measurements

A performance measurement (PM) originates in some device in the network which records the measured value. This measurement may be combined with other measurements within the device and forwarded to a management system. The management system may combine the PMs from many devices into a single grouping and may forward this grouping of PMs to some superior management system. Again this superior management system may combine groupings of measurements from many domains in the network and forward the combined package of measurements to yet another management system.

This path that PMs take as they move from the network device level to the management level is encoded in the CPR. Three elements are used to indicate this path:

System element

Entity element

SubEntity element.

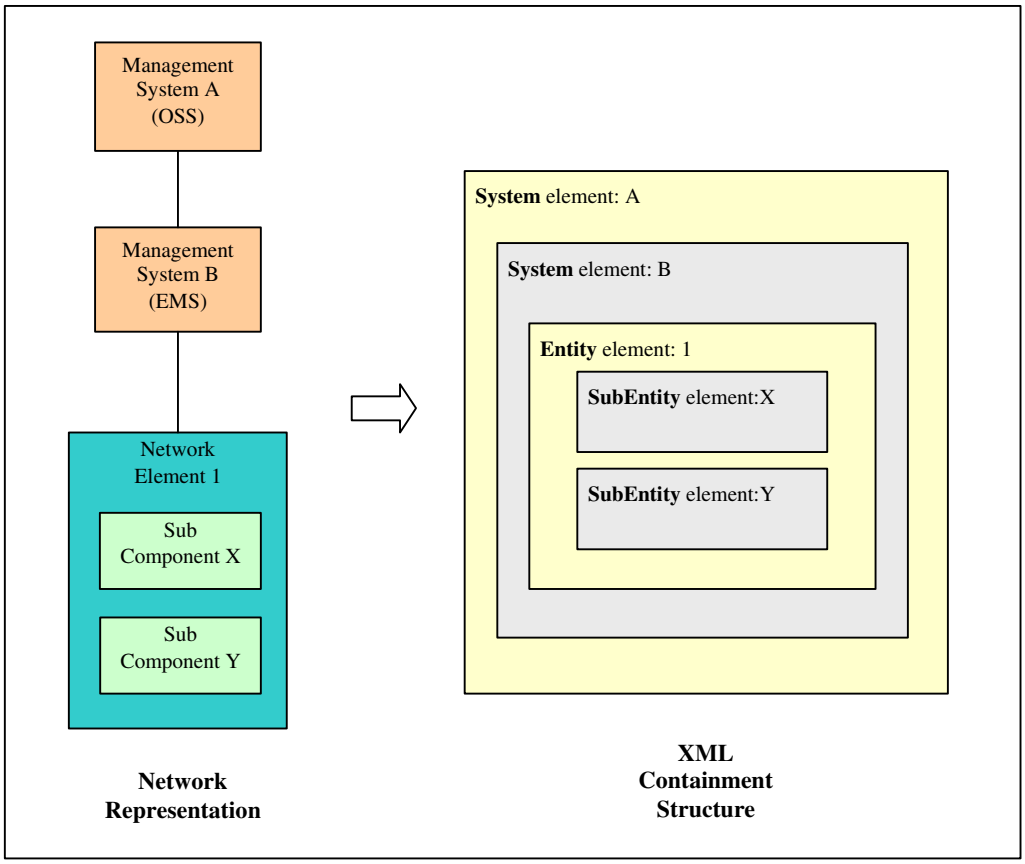
The intent of the Entity element is to represent the NE itself. What constitutes an NE and what device granularity determines an NE is an implementation choice for any particular product or technology. The System, Entity and SubEntity form a hierarchy. In this hierarchy, the Entity element may appear only once.

A Network Element may contain many sub-components and these sub-components may themselves contain sub-components and so on to some arbitrary level of decomposition. The SubEntity element represents a sub-component within the NE. A SubEntity element may contain other SubEntity elements to reflect the component structure within the NE. What constitutes a sub-component within an NE is, again, an implementation choice for any particular product or technology.

A set of performance measurements may traverse one or more management systems as it travels to some final destination system. Each of these intermediate management systems may be represented by a System element. A System element may contain another System element encoding the sequence of management systems which handle the performance measurement data.

The CPR may be emitted by a management system or by a network element. When an NE emits the record, the top-most XML element within the PMFile element will be an Entity element representing the NE which is sending the measurements. When a management system emits the CPR, the top-most XML element within the PMFile element will be a System element representing the management system.

OSS/EMS/NE hierarchy encoded in XML elements



Encoding the Performance Measurement Data

Measurement Descriptors

In general, a performance measurement is some number which is bound to a measurement identifier such as: numberOfPackets = 23145. As well as these two items, a performance measurement may contain contextual information indicating the circumstances under which the measurement was taken or giving some further information as to the meaning of the measurement or its interpretation. The following information items are used in the common performance record format to describe measurement information:

Measurement Identifier: This is the name or label which uniquely identifies the measurement.

Measurement Value: This is (generally) the numerical value of the measurement (such as an integer or decimal number). Or it could be a string or some enumerated value

Measurement Kind: There are two kinds of performance measurement: ‘snapshot’ and ‘period-based’.

A ‘snapShot’ measurement is one in which the measurement quantity (for example, some counter in a network device) is sampled at an instant in time and is being reported to the management system. There is no time significance attached to this sampled value. To derive information from a snapshot value, it may need to be compared to some previous snapshot of the counter or gauge and conclusions drawn about the change, if any, between the two values.

In contrast, a period-based measurement represents the value of some measurement quantity in the network device over a specified period of time. The measurement value relates only to activity which occurred within the measurement period.

Capture Time: This is the time at which the measurement value was captured. For a period-based measurement, this is the time at which measurement accrual stopped. For a snapshot measurement, it represents the time at which the measurement was sampled.

Interval Duration: This is the length of the time interval governing the performance measurement. For a period-based measurement, this interval is the duration between the time the measurement was started and the time the measurement was stopped. For a snapshot measurement, the interval indicates the duration between the time the current value was sampled and the time of the previous sample.

Last Record: If true this indicates that the performance measurement is the last value for the reporting time interval (indicated in IntervalDuration).

Reliability: This is an indicator of the quality or reliability of the measurement. It can take values such ‘valid’, ‘invalid’ and so on.

Unit: This names the unit in which the measurement is expressed (for example, packets, bytes and so on).

Value Type: This indicates the type of data contained in the Measurement Value. It can take on values such as ‘integer’, ‘decimal’, ‘string’ and so on).

Register Type: A register is the generic name given to the hardware or software capability in an NE which actually records the performance measurement. For numeric values the RegisterType property indicates whether the register behaves as a counter or a gauge or some other numeric register. (A counter is a register which accumulates a count of some defined event such as

the arrival of a packet. A gauge is a register which holds a state of usage sample – for example, the number of items in a queue).

Maximum Value: This property indicates the highest value the register can hold.

Reset Time: This is the register reset time. For numeric values this is the date/time when the register was last reset to zero.

Monitored Time: This indicates the actual duration of the period over which the measurements were taken. This property is used for cases where the actual measurement period is less than the period indicated in the Interval Duration value.

Intervals Covered: As an efficiency mechanism, it may be decided not to forward measurements when they have a value of zero at the end of the measurement period (for example, no events of interest occurred in the measurement period). This practice is called zero-suppression. In the case where a zero suppression representation is used, this attribute specifies the number of consecutive intervals over which a zero value was obtained for the measurement.

Table and Group Identifiers

Performance measurements may be stored within the common format as tables of values or as groups of values. The properties below are used to identify these tables and groups.

Table Identifier: This is the name or label for a particular table of measurements. This property is only used in the Table element.

KeyOfRow: This is a property specific to a column label used in representing tabular measurements. When it has a value of ‘true’ it indicates that this particular column of the table contains the key of the row of data values. The key is the identity of the object to which the row measurements pertain. This would generally refer to a sub-component in the network element.

Group Identifier: This is the name or label for a particular group of measurements. This property is only used in the GroupOfValues element.

Supplementary Identifiers

In many cases the identity of a network element, NE sub-component or performance measurement can be expressed in a single identifier. In other cases the identity will be contained in a number of individual identifiers. The approach taken in the common performance record format is to use supplementary identifiers to hold any additional identification information required in an element.

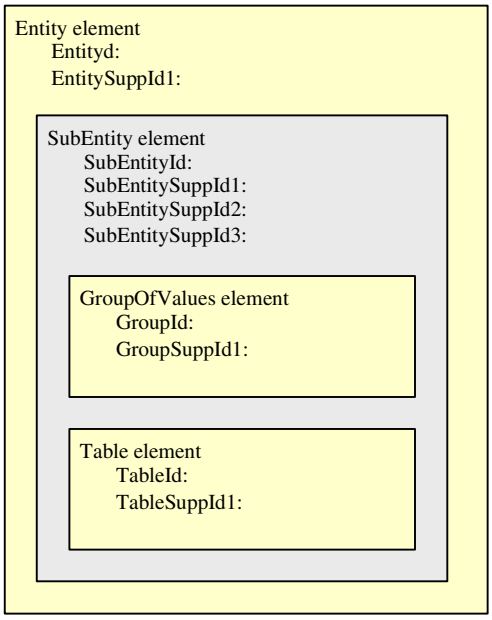
In the case of an *Entity* element (which is used to hold measurements for a particular NE), there are two identifiers: an EntityId (Entity Identifier) and an EntitySuppId (Entity Supplementary Identifier).

Likewise, the *SubEntity* element (which holds measurements for a sub-component of the NE) has a SubEntityId and three supplementary identifiers – SubEntitySuppId1, SubEntitySuppId2 and SubEntitySuppId3. Note that in the case of the *SubEntity* supplementary identifiers, it is not stipulated in which order or in which combination they are to be used. This is left as an implementation decision for any particular product/technology.

The performance measurement itself has a supplementary identifier – MeasureSuppId1. Both the *Table* element and *GroupOfValues* element also have a supplementary identifier – respectively TableSuppId1 and GroupSuppId1.

Some of these identifiers are mandatory and some are optional. See section "Optionality" on page 136 for more information.

Example of Identifiers and Supplementary Identifiers



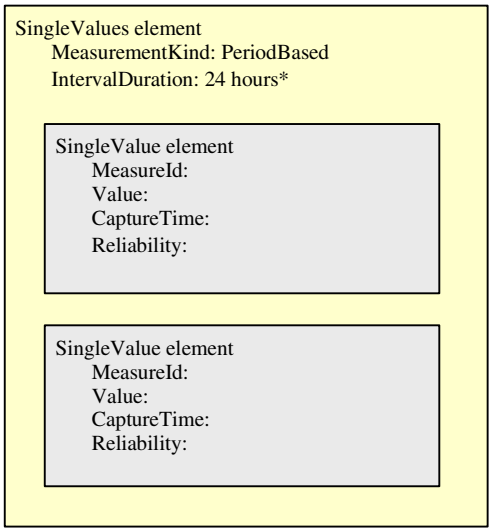
Measurement Elements

There are three ways to encode performance measurements in the common format – using a *SingleValues* approach, a *GroupOfValues* approach or a *Table* approach.

Single Values Approach

With this approach each performance measurement is considered as a standalone value with no explicit relationship to any other measurement value which may accompany it. Each measurement is encoded in a *SingleValue* element. One or more *SingleValue* elements are contained in a *SingleValues* element which specifies the kind of measurements contained within it (period-based or snapshot) and the interval duration for those measurements (for example, whether they are measurements for a 5-minute, 15-minute or 24-hour interval).

A SingleValues element containing two values



Group Values Approach

Like the SingleValues element, the GroupOfValues element contains one or more individual measurements. However, there is an explicit relationship between the measurements in the element. They are part of a group of measurements with a collective identity. The GroupId value contains the identity of the group. As with the SingleValues element, the GroupOfValues element specifies the kind of measurements it contains and their interval duration. In addition, many of the individual measurement properties such as CaptureTime and Reliability are common to the group and these are encoded once in the GroupOfValues element itself rather than being encoded for each measurement in the individual GroupValue element.

A GroupOfValues element containing two measurements

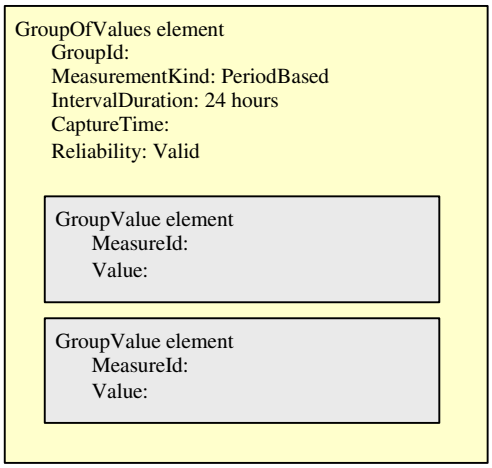
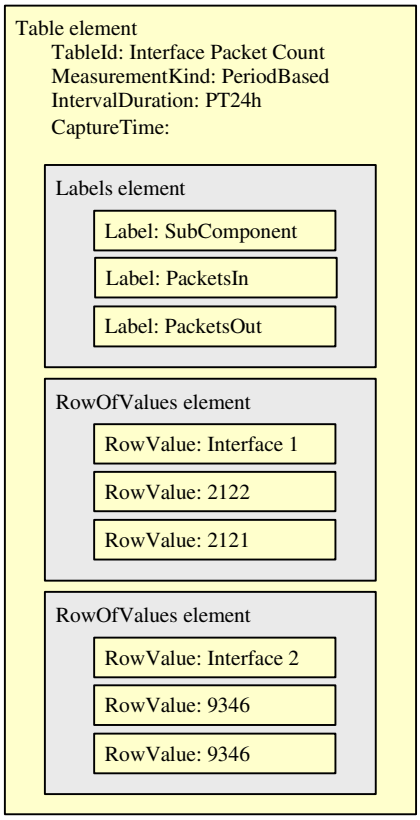


Table Approach

The table approach encodes performance measurements in a tabular format. A Table element will contain a Labels element to hold the column headings for the table. The Table element will also contain one or more RowOfValues elements. Each RowOfValues element contains a row of individual data items with a one-to-one correspondence to the labels in the Labels element. One or more of the data items in a row may contain key information indicating the source of the measurements (that is, the data item will identify the sub-component from which the measurements were taken). This facet is indicated using the KeyOfRow property in the Label element.

A table may be explicitly identified using a TableId property or it may be an anonymous table with no name.

A Table element containing two rows of values



Interface Packet Count Table

SubComponent	PacketsIn	PacketsOut
Interface 1		

Top Level Properties

The performance measurements encoded in the common format constitute an XML string. This set of values will have high level properties in common. These are captured in the PMFile element. The term ‘file’ as used below is intended to designate the XML string containing the performance measurements.

MeasurementCategory: This property describes the type of measurements contained within the PM file (its value is always "PM" indicating the file contains performance measurements).

PMReportType: This describes the type of performance measurement report contained in the file (for example, this property could be used in the case where it is desired to distinguish between different types of PM reports).

FileCreationTime: This specifies the date/time when the PM file was created.

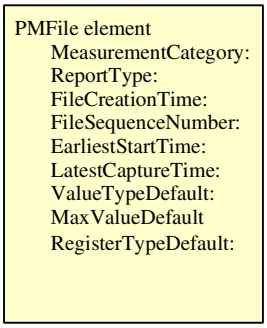
FileSchema: The FileSchema contains information which describes the format of a source non-CPR format PM file or the mapping file used to translate the source file into the common format.

FileSequenceNumber: The position of this file in some sequence of related PM files.

EarliestStartTime: This is set to the start time of the earliest measurement contained in the file.

LatestCaptureTime: This is set to the capture time of the latest measurement in the file.

PM File element contents



Default Values

ValueType, MaxValue and RegisterType are three properties which may be specified for a measurement (See Measurement Descriptors on page 11). It is possible to set defaults for these values in the file using the ValueTypeDefault, MaxValueDefault and RegisterTypeDefault properties in the top-level *PMFile* element. The scope of these default values is the entire PM file.

It is also possible to specify one or more of ValueType, MaxValue and RegisterType for each *SingleValue* element, each GroupValue element or each *Label* element (contained in a *Table* element). This local specification overrides the default value in *PMFile* for the particular element which contains the local specification.

If the property is not locally specified in the *SingleValue*, *GroupValue* or *Label* element, then the default value specified in the *PMFile* element is used.

If a default property is not specified in the PMFile element, then the following implicit default values are assumed. These implicit values function as if they were explicitly specified in PMFile.

RegisterTypeDefault:"counter"

ValueTypeDefault: "integer"

MaxValueDefault: 4,294,967,295 (that is, 232 – 1)

Optionality

It is possible to qualify a performance measurement with very many properties as shown above. Most of these properties are optional and are used in specific technologies or are needed to accommodate specific product performance management practices.

The following is the minimum set of properties required to identify a performance measurement. These are the required properties in a PM file:

PMFile Element: MeasurementCategory

System Element: SystemId

Entity: EntityId

SubEntity: SubEntityId

SingleValues Element: MeasurementKind

SingleValue Element: MeasureId; Value; CaptureTime

GroupOfValues Element: GroupId; CaptureTime; MeasurementKind

GroupValue Element: MeasureId; Value

Table Element: CaptureTime; MeasurementKind

Labels Element: N/A

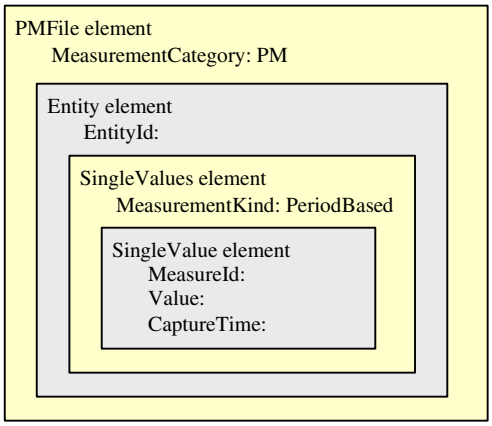
Label Element: N/A

RowOfValues Element: N/A

RowValue Element: Value

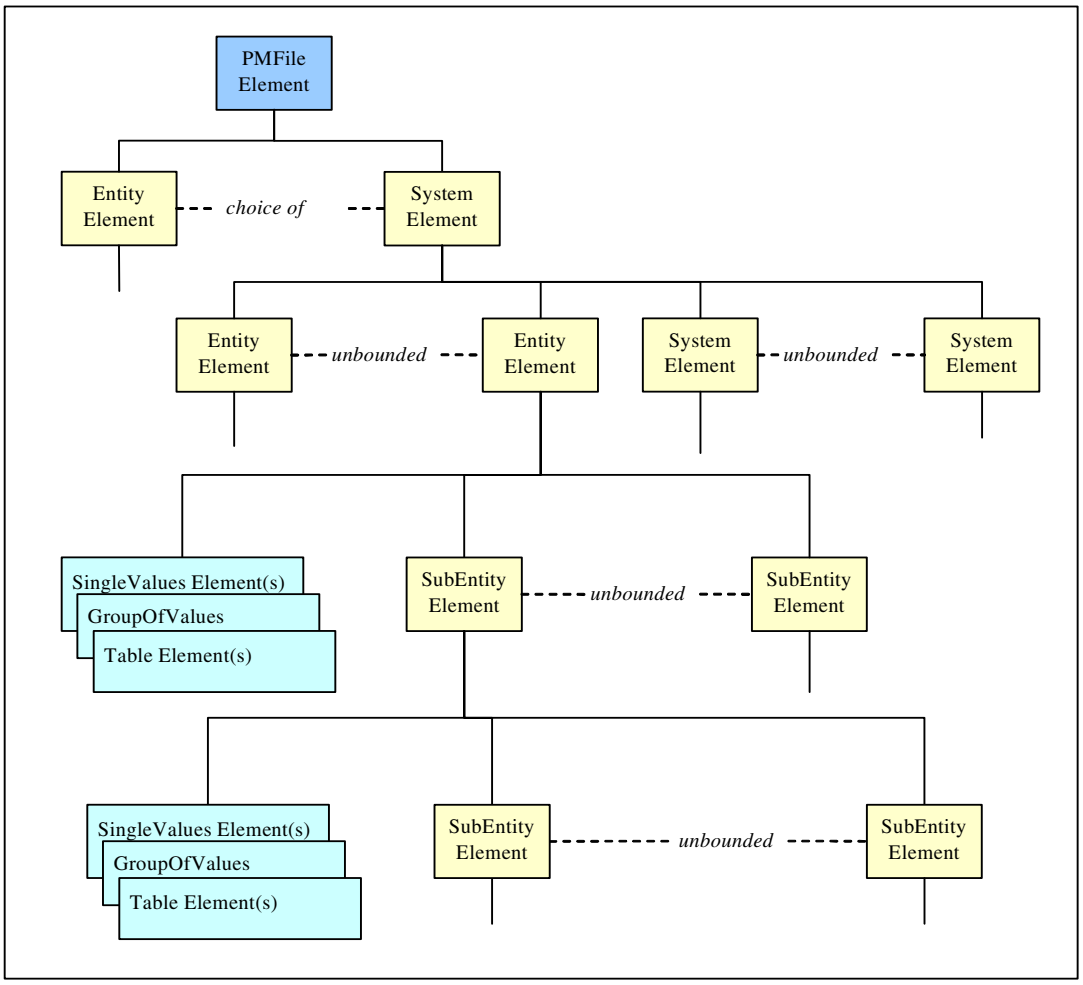
So a minimal CPR file would look like this:

Minimal Common Record Performance Record file



The figure below shows the hierarchical relationship of the major XML elements in the common performance record.

Hierarchy of the major XML elements



Attribute and Element Encoding

In the common performance record format some information is encoded as element data while other information is encoded using attributes. The approach followed is that attributes are used to encode metadata while elements are used for instance values.

Metadata is data which describes or qualifies some piece of information in terms of its class. So, in the common performance record, the *MeasurementKind* property differentiates between period-based measurements and snapshot measurements. This property is coded as an attribute.

Data which identifies or describes a specific instance of information rather than a class of information is encoded using an element. So the CaptureTime

property describes the time instant when a specific measurement was taken and so is not metadata. It is encoded as an element.

It also needs to be mentioned that the common performance record format adopts the approach of encoding the measurement name or label using an XML element. For instance:

Example 1: <MeasureId> numberOfPackets </MeasureId>

This is in contrast to the approach of directly coding the measurement name as an element tag:

Example 2: <numberOfPackets> </numberOfPackets>

The requirement for the common performance record format is to have standard fields for measurement information which could be used across all of Nortel (see the Performance Strategy requirements on page 5). This has been achieved using the current approach as shown in Example 1 above.

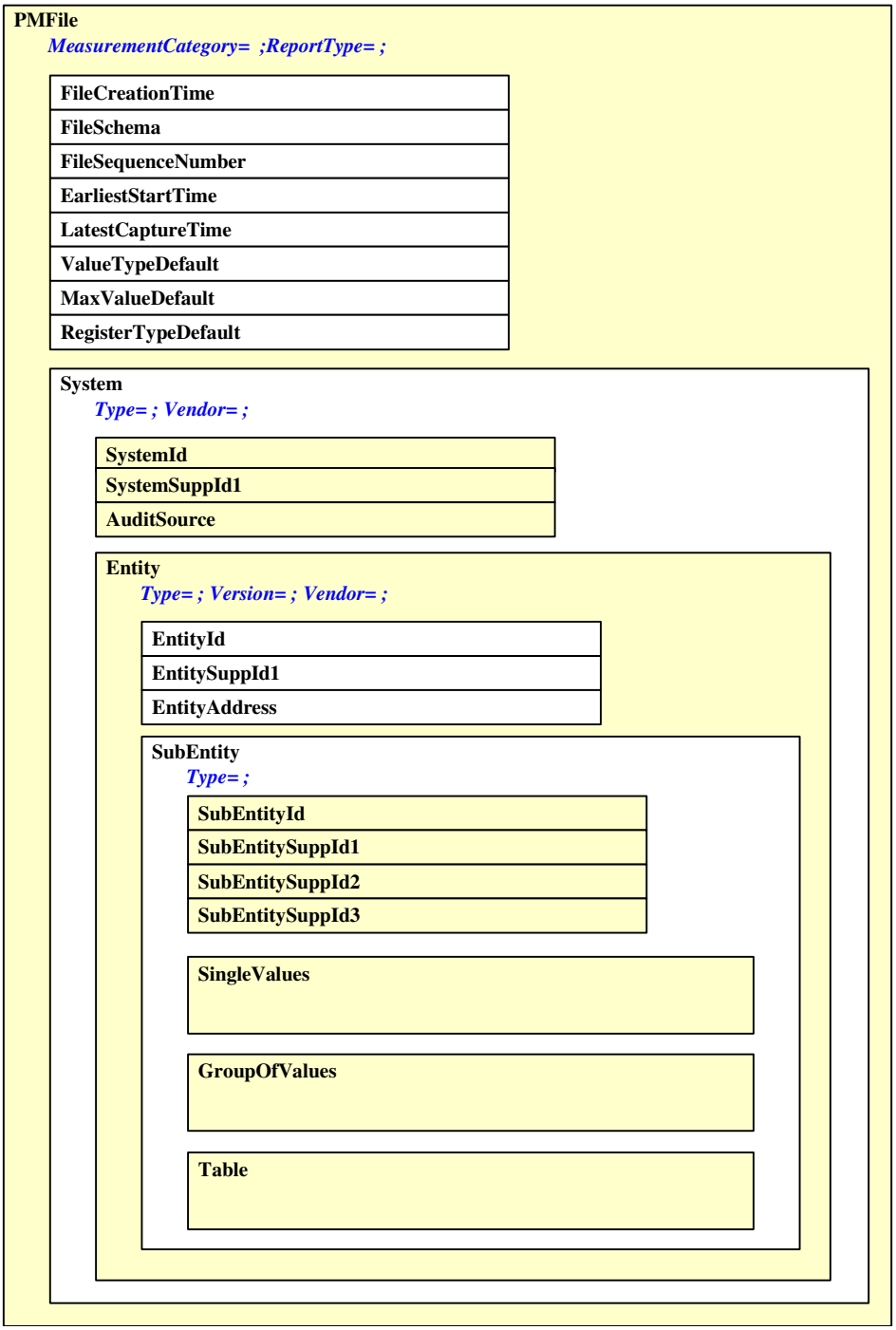
In order to use a direct coding of the measurement name as the element tag (Example 2 above) would require alignment across Nortel on the identification and semantics of all performance measurements which could possibly be encoded in the common performance record format. This alignment task has not been undertaken yet. It is envisaged that upon completion of such a convergence, the common performance record would be able to evolve to use measurement identifiers as tag names.

An additional concern is sometimes raised concerning the use of tables in the common performance record format. From a theoretical viewpoint, these tables are considered to constitute a lower quality of XML encoding than other means of encoding the data. However the common performance record format has opted to allow a tabular representation of data for pragmatic reasons. Tabular format measurement data has been the norm in most products for many years. Many operations systems expect their performance data to arrive in this customary format. In addition, industry standards for performance measurements such as 3GPP (Third Generation Partnership Project) mandate the use of tables for transporting performance data.

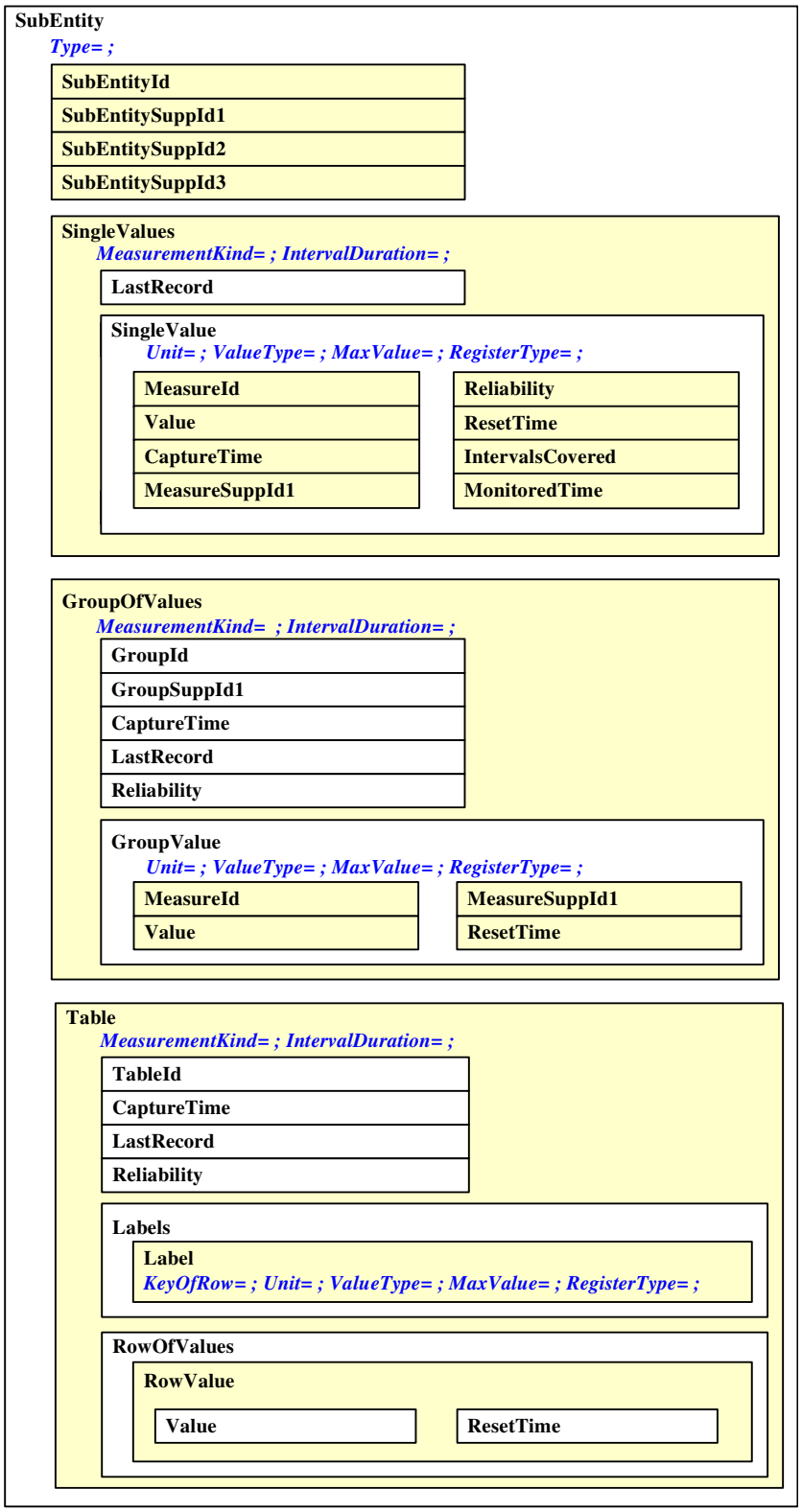
Layout of Elements and Attributes in the Common Format

The two figures below indicate which properties are expressed as elements and which are expressed via attributes. The figures represent one of many combinations of element types which are possible in the common performance record format. (Attributes are shown as *blue italicized* text. Elements are represented as boxes).

Layout of elements & attributes in the Common Performance Record



Layout of elements & attributes in the CPR-F (cont'd)



Common Performance Record Comma Separated Values (CSV) format

For examples of each of the supported PM files, refer to the section in this chapter entitled “IEMS Supported Devices” on page 154.

Note: The SNMP PM Poller is not supported for (I)SN09.

The following is an abbreviated generic description of the CPR CSV format. The CPR format is designed to be parsable into or from CPR XML format without loss of information.

The following elements are treated as ‘blocks’: PMFile, System, Entity, SubEntity, Table, GroupOfValues, SingleValues.

The start and end of these elements are marked or indicated in CSV with unique ‘Begin’ and ‘End’ markers. The format of an element block is as follows:

{element_name}=Begin

… CSV heading row for attributes & child text element nodes children of <element> …

… CSV value row for attributes & child text element nodes of <element> …

… recursive handling of all complex sub-elements (element children that are not text nodes) …

{element_name}=End

For each element, a specific property (attribute or text element) has been selected as the identifier for that element. The identifier will always appear as the *first* of the comma separated values in the CSV representation of that element.

Values that contain commas are enclosed in double quotes in CSV format.

Element blocks and identifiers

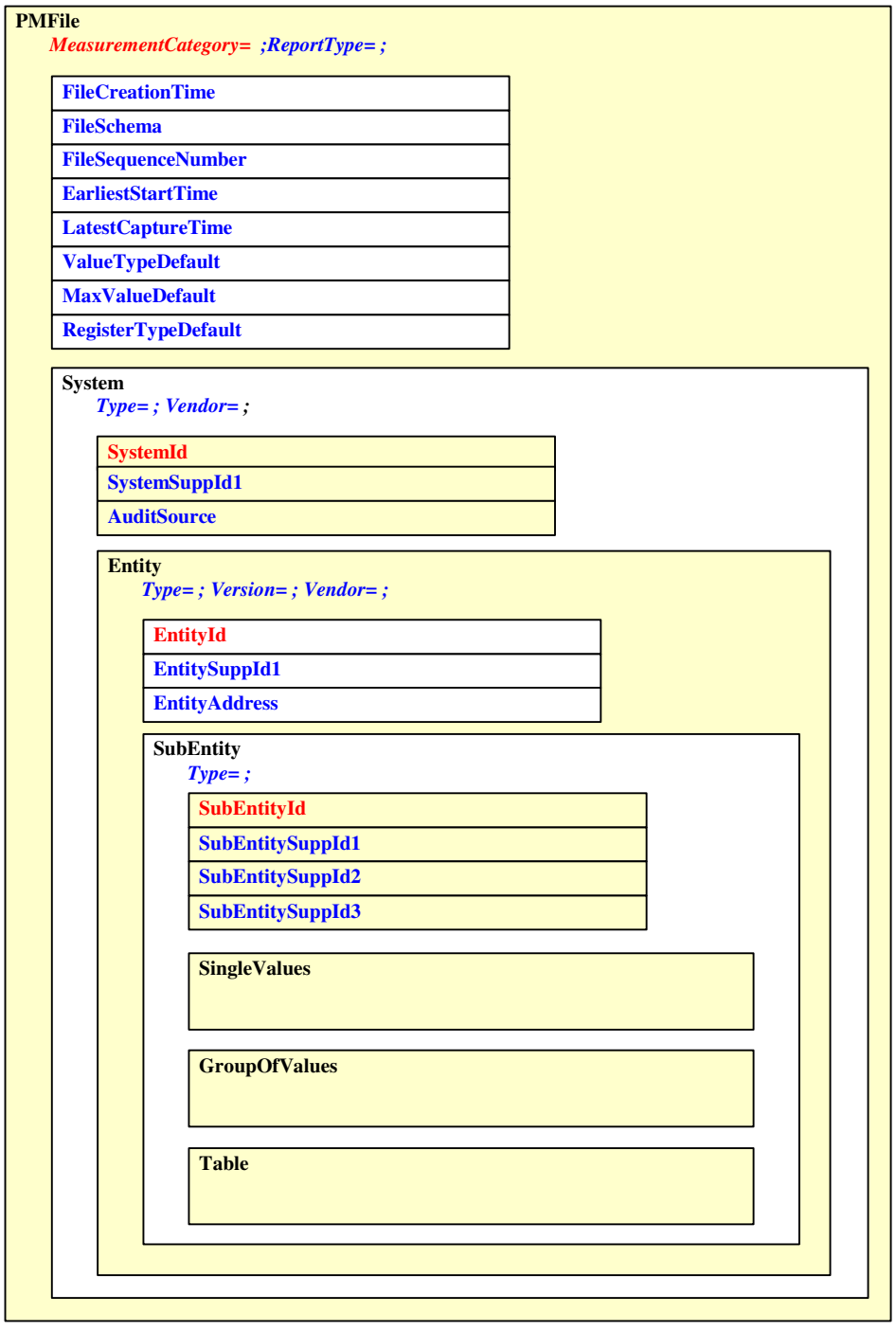
Element	Block?	Identifier
PMFile	Y	MeasurementCategory
System	Y	SystemId
Entity	Y	EntityId
SubEntity	Y	SubEntityId
Table	Y	TableId

Element	Block?	Identifier
Labels	N	Label
RowOfValues	N	RowValue/Value
GroupOfValues	Y	GroupId
GroupValue	N	MeasureId
SingleValues	Y	MeasurementKind
SingleValue	N	MeasureId

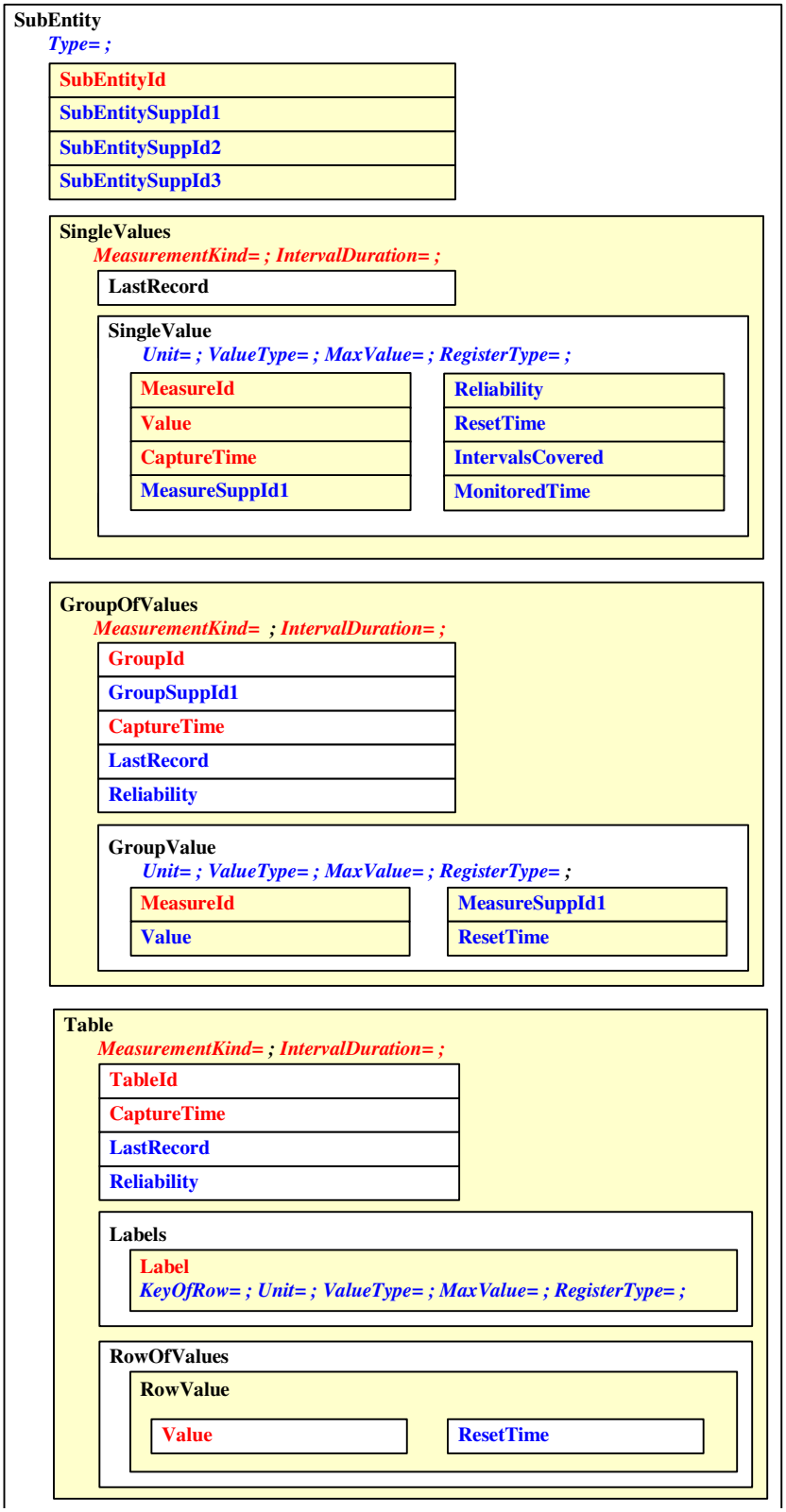
As not all identifiers are in fact mandatory, when the identifier is not found in the XML being translated the value of _Unnamed_ is used in the CSV output where the value of the identifier would normally appear.

For reference, "Layout of elements & attributes in the Common Performance Record" and "Layout of elements & attributes in the CPR-F (cont'd)" (which had been presented earlier) are shown below. The two figures indicate which properties are considered identifiers for each element, and therefore will always appear as the first comma separated value within a row. (Mandatory identifiers are shown in red. Optional identifiers are shown in blue. Attributes are shown as *italicized* text. Elements are represented as boxes.)

Layout of Elements & Attributes in the CPR-F



Layout of elements & attributes in the CPR-F (cont'd)



CSV Table example

```
    PMFile=Begin
PM,commonFormat.xsd,2004-06-23T13:01:14EST

System=Begin
NortelNetworks/IEMS

Entity=Begin
47.165.168.120,CICM

Table=Begin
.iso.org.dod.internet.mgmt.mib-
    2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5
    ,2004-06-23T13:00:00EST
usrHistoryControlInterval,usrHistoryControlIndex,usrHistoryControlStatus,usrHi
    storyControlOwner
900,5,1,CICM-120A
Table=End

Table=Begin
.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfR
    efMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot,5,200
    4-06-23T13:00:02EST
nnPerfMetricValue,nnPerfMetricSources,nnPerfMetricDataType,nnPerfMetricGroup,n
    nPerfMetricName,nnPerfMetricRefIndex
0,2,1,CICM,ActiveConnections,5
0,2,1,CICM,PercentageCpuUsed,4
0,2,1,CICM,PercentageMemoryUsed,3
0,2,1,CICM,NumberOfLogs,2
0,2,1,CICM,ActiveSessions,1
Table=End
Entity=End
System=End
PMFile=End
```

Table attributes & text elements values

Labels attributes & text elements values

RowOfValues attributes & text elements

CSV SingleValues example

```
PMFile=Begin
PM,commonFormat.xsd,2004-06-23T17:30:21EST

System=Begin
NortelNetworks/IEMS

Entity=Begin
47.174.74.179,Session Server

SingleValues=Begin
Snapshot,5
sysDescr,2004-06-23T17:26:20EST,.iso.org.dod.internet.mgmt.mib-2.system,Linux sp2k-1
2.4.22-samxts #1 Thu May 13 01:48:09 EDT 2004 i686,Valid
snmpOutPkts,2004-06-23T17:26:20EST,.iso.org.dod.internet.mgmt.mib-2.snmp,8639,Valid
snmpInBadVersions,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInBadCommunityNames,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,1,Valid
snmpInTotalReqVars,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,9689,Valid
snmpOutTraps,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInBadCommunityUses,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInPkts,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,8652,Valid
snmpInTotalSetVars,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInASNParseErrs,2004-06-23T17:26:21EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
hrSystemDate,2004-06-23T17:26:22EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,0,Valid
hrSystemUptime,2004-06-23T17:26:22EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,1315598,Valid
hrSystemProcesses,2004-06-23T17:26:22EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,170,Valid
snmpSilentDrops,2004-06-23T17:26:22EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
SingleValues=End

Entity=End
System=End
PMFile=End
```

Note on CSV Examples

All CSV examples are with header information suppressed by default. This is the default behavior for all CSV performance reports in the SN09 release.

To have the header information included in the CSV performance reports, the user must change the “suppress-headers” option from “true” to “false”. The “suppress-headers” option is located in the cprxml2csv.properties file in the /opt/nortel/iems/current/resources directory.

CSV with header information example:

PMFile=Begin

MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime

PM,commonFormat.xsd,2004-06-23T12:45:04EST

System=Begin

SystemId

NortelNetworks/IEMS

Entity=Begin

EntityId,Type

47.165.168.120,CICM

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.mgmt.mib-2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5,2004-06-23T12:40:00EST

Label,Label,Label,Label

usrHistoryControlInterval,usrHistoryControlIndex,usrHistoryControlStatus,usrHistoryControlOwner

Value,Value,Value,Value

900,5,1,CICM-120A

Table=End

Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot,5,2004-06-23T12:40:01EST

Label,Label,Label,Label,Label,Label

nnPerfMetricValue,nnPerfMetricSources,nnPerfMetricDataType,nnPerfMetricGroup,nnPerfMetricName,nnPerfMetricRefIndex

Value,Value,Value,Value,Value,Value

0,2,1,CICM,ActiveConnections,5

0,2,1,CICM,PercentageCpuUsed,4

0,2,1,CICM,PercentageMemoryUsed,3

0,2,1,CICM,NumberOfLogs,2

2662732,2,1,CICM,ActiveSessions,1

Table=End

Entity=End

System=End

PMFile=End

Note: **Collected performance files (in CSV and XML format) can be forwarded from the IEMS server to an OSS system by configuring an IEMS transfer job. Transfer jobs can be configured to to forward these files using FTP or the secure SFTP protocols.**

Inventory/Topology Interface

Overview

The IEMS provides the ability to perform an ACSII dump of provisioned network inventory/topology information for use by 3rd party systems. The snapshot is initiated from the IEMS user interface and outputs full configuration details of the component hierarchy to the IEMS server as a text file. By default, the data is placed in the file */opt/nortel/iems/current/logs/inventoryData.txt.* This information can then be retrieved and processed by third parties. For a full description of the format and content of these topology listings see the section titled “Dumping Inventory Details” in:

NN10330-511 - IEMS Configuration Management

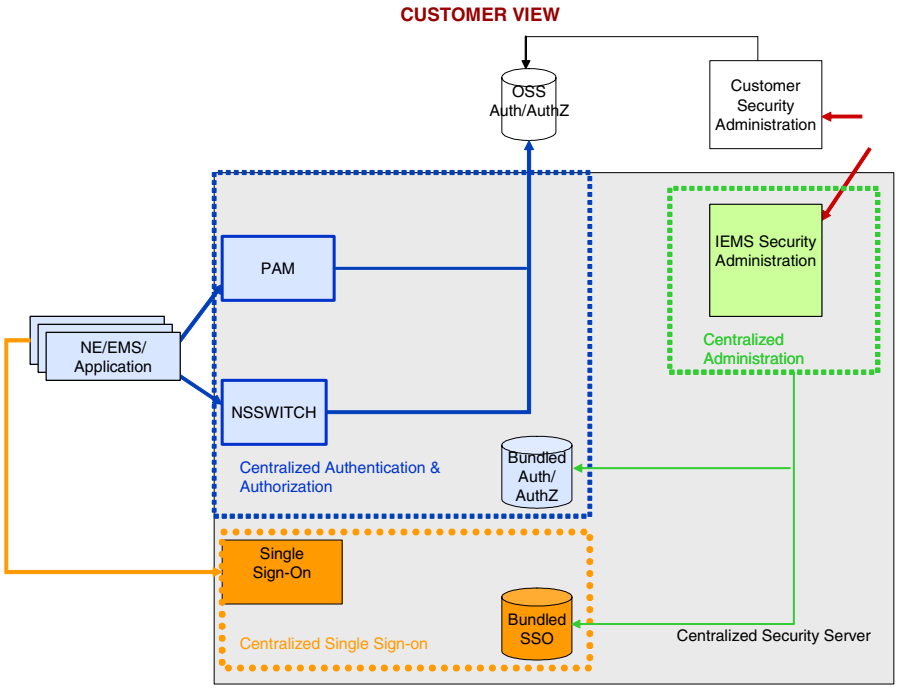
Network Security

Centralized Security Administration (Network Security)

Overview

The IEMS provides a comprehensive security architecture based on PAM (Pluggable Authentication Module) and NSSwitch (Name Services Switch). The following figure shows the Nortel Networks VoIP Security Architecture.

Centralized Security Architecture



Features

This architecture provides the following features:

- Support for central administration of user accounts and user groups
- Support for central authentication: authentication of centrally administered user accounts is performed by the IEMS Security Server.
- Support for central authorization: authorization information needed to support user access control is securely managed and provided by the IEMS Security Server.
- Support for Single Sign-on (SSO)- This capability enables the user to access multiple network elements, applications, and features from a single login session. Session information for a user is shared between IEMS and network elements supporting SSO.
- Customer Plug-ability - provides the ability for third parties to plug-in its own Authentication/Authorization solutions on IEMS. Client authentication and authorization information are provided by the customer's security backend via the IEMS Security Server.

The following table lists the devices and applications supporting these features:

Authentication and Authorization

Central Security Administration -Supported Devices

Network Element/EMS Platforms	Device Authentication Method	Device Reference Documentation
USP	HTTPS	USP Security and Administration, NN10159-611
ERS 8600 (formerly Passport 8600)	Radius	Configuring and Managing Security, 314724-B
SSPFS CS 2000 Management Tools (ossgate, sam2em, gwcem, uasem, apsem, lmm, tmm, Audio Provisioning Server (APS) Network Patch Manager (NPM) MG 9000 Manager	Radius	ATM/IP Solution-level Security and Administration, NN10402-600
IEMS	HTTPS	IEMS Security and Administration, NN10336-611
GWC	PAM Proxy	?
IEMS	HTTPS	IEMS Security and Administration, NN10336-611
CICM Manager	HTTPS	IEMS Security and Administration, NN10336-611
SDM	Radius	?
MDM and MDM Operator Client, PAM and Sun ONEIS	Radius	?
MG15000 (previously PVG)	Radius	?
CEM	PAM Proxy	?
MG9K	Radius	?

The following table lists IEMS single sign-on launch points.

IEMS single sign-on launch points

Network element/EMS platform/application	IEMS launch point
USP	USP Command Line
	USP Manager
ERS 8600 (formerly Passport 8600)	ERS8600 Command Line
SSPFS	CS 2000 Management Tools
CS 2000 Management Tools	
Audio Provisioning Server (APS)	
Network Patch Manager (NPM)	
MG 9000 Manager	
SAM21 Manager	SAM21 Manager
UAS Manager	UAS Manager
LMM	LMM
TMM	TMM
OSSGate	OSSGate
	BPT Servlet
	BPT Command Line
MG9000 Manager	MG9000 Manager
MG9000 Mid-Tier	
APS	APS Manager
	APS Application
NPM	NPM
	NPM Command Line
QOS	QOS Command Line
CEM	CEM
SSPFS	SSPFS

Network Elements and Applications can be configured to use Centralized Security Administration. To enable a device to use Centralized Security Administration, the device must be configured to use the IEMS central security server to authenticate users and access user profile information.

The IEMS Central Security Server uses PAM (Pluggable Authentication Module) to process the authentication requests and NSSwitch (Name Services Switch) to return user privilege and user profile information to Network Elements and Applications.

PAM Services

PAM provides authentication services for clients in the managed network. Customers have the option to use the PAM services that come pre-bundled with the security server or to provide their own. When customers use the PAM services provided by the IEMS Security Server, the user accounts are managed via the IEMS security and administration GUI.

When a request is forwarded to the IEMS PAM SPI (PAM Service Provider), then authentication is performed against data provisioned and administered by the Security Administration application on the IEMS client.

Conversely, when a PAM services are provided by a customer, incoming authentication requests are forwarded to the customer SPI for resolution against their remote database.

NSSwitch Services

NSSwitch provides services to obtain group and profile information for users. Centralized access to network resources depends on the definition of a common set of user groups to map security access for each user. The Nortel Networks solution provides a number of predefined user groups to address the full range of OAM&P functions required across a managed network. For a full discussion of these user groups and their categorization, see *NN10281-600 - ATM/IP Administration and Security.*

Customers can configure NSSwitch to use the service pre-bundled with IEMS or, as with PAM services, provide their own service remotely. When the pre-bundled service is used, group and user profile information is administered via the IEMS security and administration GUI. See NN10336-611 - IEMS Administration and Security.

If NSSwitch services are configured on a third party system, it is important to note that this security solution supports *only* the NSSwitch group and password databases. Although other database types may be defined in NSSwitch, they are not used by the central security feature.

See the References section for additional information on PAM and NSSwitch.

Single Sign-on (SSO)

The Single Sign-on feature allows users transparent access to multiple network elements and applications through a single login.

Once a user has been successfully authenticated for the first time (by user login), an SSO token is created by the IEMS security server that will be used to authenticate the same user on subsequent login attempts.

Network Elements and Applications use a Single Sign-On (SSO) interface on the Central Security Server to request SSO tokens whenever authentication is required.

For full details on the interface specification, see *NN10336-611 - IEMS Administration and Security.*

Configuring Security Administration

Managing Accounts

It is recommended practice that all user accounts be managed centrally with the following exceptions:

- accounts required to provide emergency access to a device.
- super user accounts (for example ‘root’ users)

For more information on adding a centrally managed user, refer to the "Adding New Users" section of *IEMS Administration and Security.*

Note: Detailed procedures for these steps can be found in *NN10336-611 - IEMS Administration and Security.*

Configuring Centralized Security Administration on NEs and EMS Platforms

An OSS must configure NEs and EMS Platforms to use centralized security administration. To enable centralized security administration on a device, the OSS must follow the procedures outlined for the device. For security configuration information for a specific device, look for its listing in the “Supported Devices” section of this document.

Note: Detailed procedures for these steps can be found in *NN10336-611 - IEMS Administration and Security.*

IEMS Supported Devices

The sections that follow contain a directory to provide customers a quick reference to device-specific information on faults, performance, interfaces, and other user documentation. The intended purpose is to allow customers to correlate IEMS Northbound interface events and behaviors with their originating source.

Each device in the listings below provide sample logs from all four Northbound fault streams: SCC2, NTSTD, Syslog, and SNMP. With the exception of the SNMP fault feed, these samples are shown as they appear from the Northbound interfaces.

Understanding SNMP Fault samples

Since SNMP has no inherent display format, each event is presented in a format that displays the short name of the MIB variables populated by the event:

<short MIB variable Name> => <value>

for example:

nnExtAlarmActiveResourceDescription =>
IEMS=nc0rtp2127.us.nortel.com-MS2000;

The following table provides a mapping of the displayed "short" variable name to its full form as well as its associated OID.

OID Short Name Mapping in SNMP Log Samples

Short name	**sysUpTime**
Long name	**system.**sysUpTime.0
OID	.1.3.6.1.2.1.1.3
Short name	**snmpTrapOID**.0
Long name	**.iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.**snmpTrapOID.0
OID	.1.3.6.1.6.3.1.1.4.1
Short name	**alarmActiveResourceId**
Long name	**alarmMIB.alarmObjects.alarmActive.alarmActiveTable.alarmActiveEntry.**alarmActiveResourceId
OID	.1.3.6.1.2.1.118.1.2.2.1.10
Short name	**alarmActiveDateAndTime**

Long name	**alarmMIB.alarmObjects.alarmActive.alarmActiveTable.alarmActiveEntry.**alarmActiveDateAndTime
OID	.1.3.6.1.2.1.118.1.2.2.1.2
Short name	**alarmActiveDescription**
Long name	**alarmMIB.alarmObjects.alarmActive.alarmActiveTable.alarmActiveEntry.**alarmActiveDescription
OID	.1.3.6.1.2.1.118.1.2.2.1.11
Short name	**nnExtAlarmActiveEventType**
Long name	**enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.**nnExtAlarmActiveEventType
OID	.1.3.6.1.4.1.562.29.6.1.1.1.1
Short name	**nnExtAlarmActiveProbableCause**
Long name	**enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.**nnExtAlarmActiveProbableCause
OID	.1.3.6.1.4.1.562.29.6.1.1.1.2
Short name	**nnExtAlarmActiveAdditionalText**
Long name	**enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.**nnExtAlarmActiveAdditionalText
OID	.1.3.6.1.4.1.562.29.6.1.1.1.3
Short name	**nnExtAlarmActiveDocumentationPointer**
Long name	**enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.**nnExtAlarmActiveDocumentationPointer
OID	.1.3.6.1.4.1.562.29.6.1.1.1.4
Short name	**nnExtAlarmActiveResourceDescription**
Long name	**enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.**nnExtAlarmActiveResourceDescription
OID	.1.3.6.1.4.1.562.29.6.1.1.1.5
Short name	**nnExtAlarmActiveManualClear**
Long name	**enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.**nnExtAlarmActiveManualClear
OID	.1.3.6.1.4.1.562.29.6.1.1.1.6

Short name	**nnExtAlarmActiveSequenceNumber**
Long name	**enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmActiveTable.nnExtAlarmActiveEntry.**nnExtAlarmActiveSequenceNumber
OID	.1.3.6.1.4.1.562.29.6.1.1.1.7
Short name	**nnExtAlarmMessageResource**
Long name	**.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.**nnExtAlarmMessageResource
OID	.1.3.6.1.4.1.562.29.6.1.3.1.1
Short name	**nnExtAlarmMessageResourceDescription**
Long name	**iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.**nnExtAlarmMessageResourceDescription
OID	.1.3.6.1.4.1.562.29.6.1.3.1.2
Short name	**nnExtAlarmMessageDateAndTime**
Long name	**iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.**nnExtAlarmMessageDateAndTime
OID	.1.3.6.1.4.1.562.29.6.1.3.1.3
Short name	**nnExtAlarmMessageDocumentationPointer**
Long name	**iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.**nnExtAlarmMessageDocumentationPointer
OID	.1.3.6.1.4.1.562.29.6.1.3.1.4
Short name	**nnExtAlarmMessageInfo**
Long name	**iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nnExtAlarmMIB.nnExtAlarmObjects.nnExtAlarmMessageTable.nnExtAlarmMessageEntry.**nnExtAlarmMessageInfo
OID	.1.3.6.1.4.1.562.29.6.1.3.1.5

Call Agent Core

This section contains IEMS Northbound log samples and device documentation references for the Call Agent Core.

Call Agent Core Fault Interface

Fault documentation for Call Agent Core :

- NN10087-911 - Call Agent Fault Management
- NN10275-909 - Carrier VoIP Fault Management Logs Reference
- NN10083-911 - Communication Server 2000 Fault Management

Fault Mapping for Call Agent Core

The following criteria can be used for looking up information on specific faults for Call Agent Core.

Fault Correlation for Call Agent Core

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Call Agent Core	log name and log number	log name and log number	log name and log number	log name and log number	see section " Fault documentation for Call Agent Core :"

Northbound Fault Formats for Call Agent Core

SCC2

The following is an example of a Call Agent Core log in SCC2 format:

```
  56 LINE138 3778 INFO TRMT
        SLOA 21 1 02 01    DN 2145202111
        TREATMENT SET = BUSY   CALLED NO =                          5202111
        CALLID= 01BE 036D
```

NTSTD

The following is an example of a Call Agent Core log in NTSTD format:

```
RTPU07BR     LINE138 Jan23 16:56:30 3778 INFO TRMT
        SLOA 21 1 02 01    DN 2145202111
        TREATMENT SET = BUSY   CALLED NO =                          5202111
        CALLID= 01BE 036D
```

SNMP

The following is an example of a Call Agent Core log in SNMP format:

```
system.sysUpTime.0 => 19:51:46
snmpTrapOID.0 => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr;
nnExtAlarmMessageDateAndTime => 2004-1-23,11:56:30.0,
nnExtAlarmMessageDocumentationPointer => LINE138
nnExtAlarmMessageInfo =>   56 LINE138 3778 INFO TRMT                SLOA 21 1 02 01
DN 2145202111
        TREATMENT SET = BUSY   CALLED NO =                          5202111
        CALLID= 01BE 036D
```

Syslog

The following is an example of a Call Agent Core log in Syslog format:

```
Feb 23 11:57:27 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=3835~~ LINE138 NONE INFO
TRMT^M        SLOA 21 1 02 01    DN 2145202111 ^M        TREATMENT SET = BUSY   CALLED
NO =                          5202111 ^M        CALLID= 01BE 036D
```

Performance

OM and PM Documentation references for Call Agent Core

- NN10149-711 - Communications Server 2000 Performance Management
- NN10087-911 - Call Agent Fault Management
- NN10264-709 - Carrier VoIP Performance Management Operational Measurements Reference

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

Performance measurements for Call Agent Core are available from the CS2K Core Manager. See NN10149-711 - Communications Server 2000 Performance Management for more information.

XML

The following is an example of Performance data for Call Agent Core in XML format:

Note: *The IEMS northbound performance interface does not support this device..*

CSV

The following is an example of Performance data for Call Agent Core in CSV format:

Note: *The IEMS northbound performance interface does not support this device..*

GUI/CLUI Documentation for Call Agent Core

The Call Agent Core provides both command-line and MAP-based interfaces accessed through the CS2000 Core Manager.

GUI/CLUI Launching and User procedures

- NN10018-111 - CS2000 Core Manager Basics

  see section “Accessing the Core”

Related documents

- NN10448-111 - Communication Server 2000 Basics
- NN10188-511 - Communication Server 2000 Configuration Management
- NN10083-911 - Communication Server 2000 Fault Management
- NN10149-711 - Communication Server 2000 Performance Management
- NN10171-611 - Communication Server 2000 Security and Administration
- 297-8403-901 - Operator Services System Advanced Intelligent Network (OSSAIN) User’s Guide
- NN10324-509 - Carrier Voice over IP Operational Configuration: Data Schema Reference Vol. 1-2
- 297-8021-808 - DMS-100 SERVORD Reference Manual Vol. 1-2
- NN10264-709 - Carrier Voice over IP Performance Management Operational Measurements Reference Vol. 1-4
- NN10275-909 - Carrier Voice over IP Fault Management Logs Reference Vol. 1-6
- 297-8991-810 - XA-Core Reference Manual

Call Agent Platform

This section contains IEMS Northbound log samples and device documentation references for the Call Agent Platform.

Call Agent Platform Fault Interface

Fault documentation for Call Agent Platform :

- NN10087-911 - Call Agent Fault Management

Fault Mapping for Call Agent Platform

The following criteria can be used for looking up information on specific faults for Call Agent Platform.

Note: All Call Agent logs are treated as INFO events by the IEMs and are associated to the CS2000 Manager when the CS2000 Manager is configured in IEMs.

Fault Correlation for Call Agent Platform

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Call Agent Platform	logname and number	logname and number	logname and number	logname and number	NN10087-911 Call Agent Fault Management

Northbound Fault Formats for Call Agent Platform

SCC2

The following is an example of a Call Agent Platform log in SCC2 format:

```
* 41 CCA 355 6064 FLT  Jam Inactive Unit
        Unit Number : 0, ACTIVE
        Description : Inactive JAMMED
```

NTSTD

The following is an example of a Call Agent Platform log in NTSTD format:

```
COMPACT06BT   *  CCA355 JAN21 18:41:14 1864 FLT   Jam Inactive Unit
        Unit Number : 0, ACTIVE
        Description : Inactive JAMMED
```

SNMP

The following is an example of a Call Agent Platform log in SNMP format:

```
system.sysUpTime.0 => 1 day, 4:49:05
snmpTrapOID.0 => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.49.44.54.58.52.49.58.49.52.46.48.44.8995
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => DeviceSpecificInfo=Unavailable;Unit Number : 0, ACTIVE
Description : Inactive JAMMED
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => CCA 355
nnExtAlarmActiveResourceDescription => IEMS=47.142.128.16-CS2K-Mgr;
nnExtAlarmActiveManualClear => 3
nnExtAlarmActiveSequenceNumber => 9104
```

Syslog

The following is an example of a Call Agent Platform log in Syslog format:

```
Jan 21 19:41:06 wnc0s0qh IEMS: _V2_~I=~H=wnc0s0qh~A=IEMS~S=2860~~  CCA355 MINOR FLT
Jam Inactive Unit^M      Unit Number : 0, ACTIVE ^M      Description : Inactive JAMMED
```

Performance

OM and PM Documentation references for Call Agent Platform

- NN10153-711 - Call Agent Performance Management

Northbound OM/PM Formats

Performance measurements for Call Agent Platform are available only from the Call Agent Manager interface. See NN10153-711 - Call Agent Performance Management for more information.

XML

The following is an example of Performance data for Call Agent Platform in XML format:

***Note:** The IEMS northbound performance interface does not support this device..*

CSV

The following is an example of Performance data for Call Agent Platform in CSV format:

***Note:** The IEMS northbound performance interface does not support this device..*

GUI/CLUI Documentation for Call Agent Platform

GUI Launching and User procedures

- NN10175-611 - Call Agent Security and Administration

Related documents

- NN10023-111 - Call Agent Basics
- NN10109-511 - Call Agent Configuration Management

Core Element Manager (CEM)

This section contains IEMS Northbound log samples and device documentation references for the Core Element Manager.

CEM Fault Interface

This section provides references to customer documentation for Fault Management for CEM.

Fault documentation for CEM :

The document that describes CEM faults is IEMS Fault Management, NN10334-911.

Fault Mapping for CEM

The following criteria can be used for looking up information on specific faults for CEM.

Table 1 Fault Correlation for CEM

NB format -> Device/EM	SCC2	NTStd	SNMP	Syslog	Document Reference
CEM	Description log name and log number	Description log name and log number	Device specific info	Description log name and log number	NN10334-911

Northbound Fault Formats for CEM

SCC2

The following is an example of a CEM log in SCC2 format:

info event:

```
58 CSEM600 0069 INFO Log
    Equip Id: 250Q C7SP
    Notification Id: 0000042693
    Category: communications
    Cause: unableToSSTreply
    ComponentId: C7SP
    LogKey: CCS224
    Description:
    "RTPU08AZ| |   | |CCS224|JAN19|13:57:30|8844|INFO|No reply SST Invd CGPA

          SSN  = 100,
          CGPA: VALID    ANSI7  43 0 1 ANSI7 252 050 006
              GTNAME: INVALID  UNKNOWN  208 164 94 00 OCTET
              DIGITS:
    |1106161126"
```

alarm raise or clear:

```
  * 00 CSEM300 0083 TBL  Alarm set
        Equip Id: 250Q SDM-0
        Notification Id: 0000042700
        Category: processingError
        Cause: applStatusChange
        ComponentId: SDM-0
        LogKey: SDM550
        Description:
        "RTPU08AZ| |** | |SDM550|JAN19|13:59:04|8861|INFO|Node Status Change
              Node:   SDM 0
              Status:  ** ISTb      from  ** ISTb
              Reason: DCE unavailable alarm
        |1106161220"
```

NTStd

The following is an example of a CEM log in NTStd format:

info event:

```
znc0s0jh     CSEM600 JAN19 13:58:58 0071 INFO Log
        Equip Id: 250Q MPC-1
        Notification Id: 0000042694
        Category: equipment
        Cause: mpcINFO
        ComponentId: MPC-1
        LogKey: MPC101
        Description:
        "RTPU08AZ| |   | |MPC101|JAN19|13:57:43|8845|INFO|MPC_INFORMATION_REPORT
            REASON = 19
               UNABLE TO DOWNLOAD MPC.  FILE-ID NOT FOUND.
               MPC = 1

        |1106161138"
```

alarm raise or clear:

```
znc0s0jh   * CSEM300 JAN19 14:00:20 0083 TBL  Alarm set
        Equip Id: 250Q SDM-0
        Notification Id: 0000042700
        Category: processingError
        Cause: applStatusChange
        ComponentId: SDM-0
        LogKey: SDM550
        Description:
        "RTPU08AZ| |** | |SDM550|JAN19|13:59:04|8861|INFO|Node Status Change
              Node:   SDM 0
              Status:  ** ISTb      from  ** ISTb
              Reason: DCE unavailable alarm
        |1106161220"
```

SNMP

The following is an example of a CEM log in SNMP format for **event**:

info event:

sysUpTime. => 1:56:59

snmpTrapOID. => nnExtAlarmMessage

nnExtAlarmMessageResource => .0.0

nnExtAlarmMessageResourceDescription =>
IEMS=250Q@rtpu@47.142.94.68;MPC-1

nnExtAlarmMessageDateAndTime => 2005-1-19,1:58:58.0

nnExtAlarmMessageDocumentationPointer => MPC101

nnExtAlarmMessageInfo => 58 CSEM600 0071 INFO Log

"RTPU08AZ| | |
|MPC101|JAN19|13:57:43|8845|INFO|MPC_INFORMATION_REPORT
REASON = 19

UNABLE TO DOWNLOAD MPC. FILE-ID NOT FOUND.

MPC = 1

|110616

clear alarm:

sysUpTime. => 4:50:21

snmpTrapOID. => nnExtAlarmClear

mib-2. =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.20.50.48.48.53.45.49.45.49.57.44.49.58.53.51.58.53.50.46.48.44.45906

mib-2. => Õ54

mib-2. => DeviceSpecificInfo=;"RTPU08AZ| |** |
|SDM550|JAN19|13:52:37|8807|INFO|Node Status Change

Node: SDM 0

Status: ** ISTb from ** ISTb

Reason: DCE unavailable alarm

|1106160832"

nnExtAlarmActiveEventType => 3

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer =>

nnExtAlarmActiveResourceDescription =>
IEMS=250Q@rtpu@47.142.128.85;

nnExtAlarmActiveSequenceNumber => 4629

minor alarm:

sysUpTime. => 1:58:22

snmpTrapOID. => nnExtAlarmMinor

mib-2. =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.19.50.48.48.53.45.49.45.49.57.44.50.58.48.58.50.48.46.48.44.2

mib-2. => Õ

mib-2. => DeviceSpecificInfo=applStatusChange;"RTPU08AZ| |** |
|SDM550|JAN19|13:59:04|8861|INFO|Node Status Change

Node: SDM 0

Status: ** ISTb from ** ISTb

Reason: DCE unavailable alarm

|1106161220"

nnExtAlarmActiveEventType => 3

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => SDM550

nnExtAlarmActiveResourceDescription =>
IEMS=250Q@rtpu@47.142.94.68;SDM-0

nnExtAlarmActiveManualClear => 2

nnExtAlarmActiveSequenceNumber => 3

major alarm:

sysUpTime. => 4:50:22

snmpTrapOID. => nnExtAlarmMajor

mib-2. =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.19.50.48.48.53.45.49.45.49.57.44.50.58.48.58.50.49.46.48.44.45917

mib-2. => Õ

mib-2. => DeviceSpecificInfo=sdmBaseMaintenance;"RTPU08AZ| |** |
|SDM317|JAN19|14:00:19|8862|TBL | SDM Base Maintenance

DCE problem detected

Reason: sec client service failed: Waited for 5 minutes and DCED had

not initia

nnExtAlarmActiveEventType => 3

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => SDM317

nnExtAlarmActiveResourceDescription =>
IEMS=250Q@rtpu@47.142.128.85;SDM-0

nnExtAlarmActiveManualClear => 4

nnExtAlarmActiveSequenceNumber => 4630

critical alarm:

Syslog

The following is an example of a CEM log in Syslog format:

info event:

Aug 1 18:30:17 znc0s0jh IEMS:
_V2_~I=~H=znc0s0jh~A=IEMS~S=0444~~ CSEM600 NONE INFO
Log^M Equip Id: 250Q C7SP^M Notification Id: 0000048176^M
Category: communications^M Cause: unableToSSTreply^M
ComponentId: C7SP^M LogKey: CCS224^M Description:^M
"RTPU08AZ| | | |CCS224|JAN20|00:32:43|8642|INFO|No reply SST Invd
CGPA^M ^M SSN = 100,^M CGPA: VALID ANSI7
43 0 1 ANSI7 252 050 006 ^M GTNAME: INVALID
UNKNOWN 208 164 94 00 OCTET ^M DIGITS: ^M
|1106199239"

alarm raise or clear:

Aug 1 18:30:27 znc0s0jh IEMS:
_V2_~I=~H=znc0s0jh~A=IEMS~S=0451~~ CSEM300 MINOR TBL Alarm
set^M Equip Id: 250Q SDM-0^M Notification Id: 0000048178^M
Category: processingError^M Cause: applStatusChange^M
ComponentId: SDM-0^M LogKey: SDM550^M Description:^M
"RTPU08AZ| |** | |SDM550|JAN20|00:32:53|8644|INFO|Node Status Change
^M Node: SDM 0^M Status: ** ISTb from ** ISTb
^M Reason: DCE unavailable alarm^M |1106199249"

Performance

OM and PM Documentation references for CEM

- Not supported in SN09

Northbound OM/PM Formats

N/A

GUI/CLUI Documentation for CEM

GUI Launching and User procedures

- Adding a Core Element Manager - IEMS Configuration Management NN10330-511
- Launching a Core Element Manager - IEMS Basics, NN10329-111
- CEM Overview and GUI description - IEMS Basics, NN10329-111

Related documents

- Adding a Core Element Manager - IEMS Configuration Management NN10330-511
- Launching a Core Element Manager - IEMS Basics, NN10329-111
- CEM Logs and OMs - IEMS Fault Management, NN10334-911-
- CEM Overview and GUI description - IEMS Basics, NN10329-111
- CEM Restore - ATM/IP Solution level Security and Administration, NN10402-600
- Synchronous Backup Manager procedures - ATM/IP Solution level Security and Administration, NN10402-600

Centrex IP Call Manager (CICM)

This section contains IEMS Northbound log samples and device documentation references for the CICM.

CICM Fault Interface

Fault documentation for CICM :

- NN10334-911-- IEMS Fault Management

Fault Mapping for CICM

The following criteria can be used for looking up information on specific faults for CICM.

Fault Correlation for CICM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
CICM	logname and number	logname and number	logname and number	logname and number	NN10334-911 - IEMS Fault Management

Northbound Fault Formats for CICM

SCC2

The following is an example of a CICM log in SCC2 format:

```
* 02 CICM359 0001 FLT  CICM Fault
      Location: 47.165.168.120
      Notification Id: 7
      State: Raised
      Category: equipment
      Cause: equipmentMalfunction(15)
      Time: Jun 17 09:02:08 2004
      Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Card;Card=7
      Specific Problem:  Card 7 has an alarm.
      Description: Card Alarm
?
**02 CICM500 0002 FLT  CICM Fault
      Location: 47.165.168.120
      Notification Id: 5
      State: Raised
      Category: equipment
      Cause: unspecifiedReason(118)
      Time: Jun 17 09:02:08 2004
      Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Chassis
      Specific Problem:  Chassis card state change report for slot 7 in state
      1
      Description: Chassis Card State Change
?
**02 CICM339 0003 FLT  CICM Fault
      Location: 47.165.168.120
      Notification Id: 6
      State: Raised
```

Category: equipment

Cause: lANError(25)

Time: Jun 17 09:02:13 2004

Component Id: CICM=CICM-120A;NodeType=Cicm

Specific Problem: Have not received a message from Node B for 1.5*ALARM _POLL_PERIOD Seconds. CPU_CARD_DOMAIN_A

Description: No Message Received From B

NTSTD

The following is an example of a CICM log in NTSTD format:

```
test   * CICM359 JUN17 09:02:08 0004 FLT  CICM Fault
         Location: 47.165.168.120
         Notification Id: 7
         State: Raised
         Category: equipment
         Cause: equipmentMalfunction(15)
         Time: Jun 17 09:02:08 2004
         Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Card;Card=7
         Specific Problem:  Card 7 has an alarm.
         Description: Card Alarm


test  ** CICM500 JUN17 09:02:08 0005 FLT  CICM Fault
         Location: 47.165.168.120
         Notification Id: 5
         State: Raised
         Category: equipment
         Cause: unspecifiedReason(118)
         Time: Jun 17 09:02:08 2004
         Component Id: CICM=CICM-120A;NodeType=Cicm;Component=Chassis
         Specific Problem:  Chassis card state change report for slot 7 in state
         1
         Description: Chassis Card State Change


test  ** CICM339 JUN17 09:02:13 0006 FLT  CICM Fault
         Location: 47.165.168.120
```

```
Notification Id: 6
State: Raised
Category: equipment
Cause: lANError(25)
Time: Jun 17 09:02:13 2004
Component Id: CICM=CICM-120A;NodeType=Cicm
Specific Problem:  Have not received a message from Node B for 1.5*ALARM
_POLL_PERIOD Seconds. CPU_CARD_DOMAIN_A
Description: No Message Received From B
```

SNMP

The following is an example of a CICM log in SNMP format:

```
sysUpTime. => 19:40:37
snmpTrapOID. => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.
20.50.48
.48.52.45.54.45.50.57.44.49.48.58.50.57.58.48.46.52.44.11925
alarmActiveDateAndTime => 2004-6-29,10:29:0.4
alarmActiveDescription => DeviceSpecificInfo=softwareProgramError(48);Backup
Fail.
nnExtAlarmActiveEventType => 4
nnExtAlarmActiveProbableCause => 1024
nnExtAlarmActiveAdditionalText => Scheduled/on-demand backup failed during
last iteration.
nnExtAlarmActiveDocumentationPointer => CICM341
nnExtAlarmActiveResourceDescription => IEMS=47.142.86.95-CICM-
Mgr_Card_A;CICM=CICMEM-000-A;NodeType=Platform
nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a CICM log in Syslog format:

Jun 29 10:40:34 2004 ComponentId: 47.165.168.74-CICM-Mgr_Card_B Specific Problem: Connection Lost Description: IEMS Unable to communicate with managed device

Jun 29 10:50:40 2004 ComponentId: 47.165.168.120-CICM_Card_A Description: IEMS regained communication with the managed device

Performance

OM and PM Documentation references for CICM

- N10327-711 - IEMS Performance Management

Northbound OM/PM Formats

Performance measurements for CICM are available only from the CICM Manager interface. See NN10327-711 - IEMS Performance Management for more information.

XML

The following is an example of Performance data for CICM in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T12:30:00EST</FileCreationTime>
- <System>
<SystemId>NortelNetworks/IEMS</SystemId>
- <Entity Type="CICM">
<EntityId>47.165.168.120</EntityId>
- <Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry</TableId>
<CaptureTime>2004-06-23T12:25:01EST</CaptureTime>
- <Labels>
<Label>usrHistoryControlInterval</Label>
<Label>usrHistoryControlIndex</Label>
<Label>usrHistoryControlStatus</Label>
<Label>usrHistoryControlOwner</Label>
</Labels>
- <RowOfValues>
- <RowValue>
<Value>900</Value>
</RowValue>
- <RowValue>
<Value>5</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
```

<RowValue>

<Value>CICM-120A</Value>

</RowValue>

</RowOfValues>

</Table>

</Entity>

</System>

</PMFile>

CSV

The following is an example of Performance data for CICM in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-28T17:30:02EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
47.165.168.125,CICM

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5,2005-03-
28T17:30:00EST
Label,Label,Label,Label
usrHistoryControlIndex,usrHistoryControlInterval,usrHistoryControlOwner,usrHistoryCo
ntrolStatus
Value,Value,Value,Value
5,900,CICM-120B,1
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
```

```
.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.
nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot,5,2005-03-
28T17:30:00EST

Label,Label,Label,Label,Label,Label

nnPerfMetricRefIndex,nnPerfMetricName,nnPerfMetricGroup,nnPerfMetricDataType,nnPerfM
etricSources,nnPerfMetricValue

Value,Value,Value,Value,Value,Value

5,ActiveConnections,CICM,1,2,0

4,PercentageCpuUsed,CICM,1,2,0

3,PercentageMemoryUsed,CICM,1,2,38

2,NumberOfLogs,CICM,1,2,0

1,ActiveSessions,CICM,1,2,671047275

Table=End


Entity=End


System=End


PMFile=End
```

GUI/CLUI Documentation for CICM

GUI Launching and User procedures

Related documents

Ethernet Routing Switch 8600 (formerly Passport 8600)

This section contains IEMS Northbound log samples and device documentation references for the ERS 8600.

ERS 8600 Fault Interface

Fault documentation for ERS 8600 :

- 241-6001-011 Multiservice Data Manager Fault Management Tools
- 241-6001-501 Multiservice Data Manager Alarms Reference

Fault Mapping for ERS 8600

The following criteria can be used for looking up information on specific faults for ERS 8600.

Fault Correlation for ERS 8600

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
ERS 8600	logname and number	logname and number	logname and number	logname and number	241-6001-500 Multiservice Data Manager Alarms Reference

Northbound Fault Formats for Ethernet Routing Switch 8600

SCC2

The following is an example of an ERS 8600 log in SCC2 format:

```
**59 PP  330 0010 TBL  PP Fault
        Location: pp8600;47.142.106.1
        State: Raised
        Category: equipment
        Cause: Link Oscillation detected
        Time: Aug 09 15:59:14 2004
        Component ID: PP8600=47.142.106.1; portIndex=198
        Specific Problem: RC Link Oscillation
        Description: LinkOscillation: portIndex = 198
        .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.8
        .1.3.6.1.2.1.1.3.0: 50 days, 17 hours, 4 minutes, 39 seconds.


  03 PP  318 0011 INFO PP Fault
        Location: pp8600;47.142.106.1
        State: Cleared
        Category: communications
        Cause: communication regained
        Time: Aug 09 16:03:38 2004
        Component ID: PP8600=47.142.106.1; ifIndex=89
        Specific Problem: Generic Link Status
        Description: Link Up: ifIndex = 89( AdminStatus = up OperationStatus = u
```

```
        p)
        .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0
        .1.3.6.1.2.1.1.3.0: 50 days, 17 hours, 9 minutes, 3 seconds
```

NTSTD

The following is an example of an ERS 8600 log in NTSTD format:

```
MY_OFFICE  **   PP330 AUG09 15:59:14 0010 TBL  PP Fault
        Location: pp8600;47.142.106.1
        State: Raised
        Category: equipment
        Cause: Link Oscillation detected
        Time: Aug 09 15:59:14 2004
        Component ID: PP8600=47.142.106.1; portIndex=198
        Specific Problem: RC Link Oscillation
        Description: LinkOscillation: portIndex = 198
        .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.0.8
        .1.3.6.1.2.1.1.3.0: 50 days, 17 hours, 4 minutes, 39 seconds.


MY_OFFICE       PP318 AUG09 16:03:38 0011 INFO PP Fault
        Location: pp8600;47.142.106.1
        State: Cleared
        Category: communications
        Cause: communication regained
        Time: Aug 09 16:03:38 2004
        Component ID: PP8600=47.142.106.1; ifIndex=89
        Specific Problem: Generic Link Status
        Description: Link Up: ifIndex = 89( AdminStatus = up OperationStatus = u
        p)
        .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0
        .1.3.6.1.2.1.1.3.0: 50 days, 17 hours, 9 minutes, 3 seconds.
```

SNMP

The following is an example of an ERS 8600 log in SNMP format:

```
sysUpTime.0 => 2:55:28
```

snmpTrapOID.0 => nnExtAlarmMajor

alarmActiveResourceId =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.50.45.52.44.53.58.53.56.58.52.54.46.54.44.90024

alarmActiveDateAndTime => 2004-2-4,5:58:46.6

alarmActiveDescription => DeviceSpecificInfo=;Link Down: ifIndex = 175 (AdminStatus = down OpeationStatus = down)

nnExtAlarmActiveEventType => 5

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => PP 398

nnExtAlarmActiveResourceDescription => IEMS=47.142.130.66-PP8600;3

nnExtAlarmActiveSequenceNumber => 2709

Syslog

The following is an example of an ERS 8600 log in Syslog format:

```
Aug  9 15:58:57 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=3342~~   PP317 MAJOR TBL
PP Fault^M      Location: pp8600;47.142.106.1^M      State: Raised^M      Category:
com

munications^M     Cause: loss of communication^M     Time: Aug 09 15:58:56 2004^M
Component ID: PP8600=47.142.106.1; ifIndex=89^M       Specific Problem: Generic Li

nk Status^M       Description: Link Down: ifIndex = 89( AdminStatus = down
OperationStatus^M         = down)^M       .1.3.6.1.6.3.1.1.4.1.0:
.1.3.6.1.6.3.1.1.5.3.0^M       .1.

3.6.1.2.1.1.3.0: 50 days, 17 hours, 4 minutes, 22 seconds.


Aug  9 15:59:14 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=3343~~   PP318 NONE INFO
PP Fault^M      Location: pp8600;47.142.106.1^M      State: Cleared^M      Category:
co

mmunications^M       Cause: communication regained^M       Time: Aug 09 15:59:14
2004^M      Component ID: PP8600=47.142.106.1; ifIndex=198^M      Specific Problem:
Generic

 Link Status^M       Description: Link Up: ifIndex = 198( AdminStatus = up
OperationStatus = ^M    up)^M    .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0^M
.1.3.

6.1.2.1.1.3.0: 50 days, 17 hours, 4 minutes, 39 seconds.
```

Performance

OM and PM Documentation references for ERS 8600

- 241-6001-031, Multiservice Data Manager Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance for ERS 8600 in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T17:35:01EST</FileCreationTime>
- <System>
<SystemId>NortelNetworks/IEMS</SystemId>
- <Entity Type="PP8600">
<EntityId>47.142.130.66</EntityId>
- <SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
- <SingleValue>
<CaptureTime>2004-06-23T17:30:01EST</CaptureTime>
<MeasureId>snmpInvalidMsgs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.snmpV2.snmpModules.snmpMPDMIB.snmpMPDMIBObject
s.snmpMPDStats</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:30:01EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>311026</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:30:01EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
```

- <SingleValue>
<CaptureTime>2004-06-23T17:30:01EST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>15</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:30:02EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>320467</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:30:03EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>1412075</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:30:03EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>2</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:30:03EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:30:04EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>

```
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance for ERS 8600 in CSV format:

Note: The following CSV output file are captured using ERS8600_IP_30_minute_data.xml template.

```
PMFile=Begin
MeasurementCategorynoNamespaceSchemaLocationFileCreationTime
PM commonPerfRecord_V2.0.xsd2005-12-20T21:48:39EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.142.86.32-PP8600_1

Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatTable.rcStat
EntrySnapshot52005-12-20T21:37:19EST
LabelLabelLabelLabelLabel
rcStatPortIndexrcStatRouteInDiscardsrcStatStgForwardTransitionsrcStatFrameTooShorts
rcStatBridgeInDiscards
ValueValueValueValueValue
70 0  0   0   0
2650  0   0   0
2640  0   0   0
2630  0   0   0
2620  0   0   0
```

```
2610  0   0   0
2600  0   0   0
4590  0   0   0
4580  0   0   0
69 0  0   0   0
4570  0   0   0
68 0  0   8   1292802
4560  0   0   0
67 0  0   0   0
4550  0   0   0
66 0  0   0   0
4540  0   0   0
65 0  0   0   0
4530  0   0   0
64 0  0   0   11534
2590  0   0   0
4520  0   0   0
2580  0   0   0
4510  0   0   0
2570  0   0   0
4500  0   0   0
2560  0   0   0
4490  0   0   0
4480  0   0   0
2390  0   0   0
2380  0   0   0
2370  0   0   0
2360  0   0   0
2350  0   0   0
2340  0   0   0
2330  0   0   0
2320  0   0   0
2310  0   2   0
1990  0   0   0
2300  0   2   0
1980  0   0   0
1970  0   0   0
1960  0   0   0
```

```
1950  0   0   0
1940  0   0   0
1930  0   0   0
1920  0   0   0
2290  0   0   0
5830  0   0   0
2280  0   0   0
5820  0   0   0
2270  0   0   0
5810  0   0   0
2260  0   0   0
5800  0   0   0
2250  0   0   0
2240  0   0   0
2230  0   0   0
2220  0   0   0
2210  0   0   0
2200  0   0   0
5790  0   0   0
5780  0   0   2561114
5770  0   0   0
5760  0   0   10984
2190  0   0   0
2180  0   0   0
2170  0   0   0
2160  0   0   0
2150  0   0   0
2140  0   0   0
2130  0   0   0
2120  0   0   0
2110  0   0   0
2100  0   0   0
2090  0   0   0
2080  0   0   0
2070  0   0   0
2060  0   0   0
2050  0   0   0
2040  0   0   0
```

```
2030  0   0   0
2020  0   0   0
2010  0   0   0
2000  0   0   0
1610  0   0   0
1600  0   0   0
5590  0   0   0
5580  0   0   0
5570  0   0   0
5560  0   0   0
5550  0   0   0
5540  0   0   0
5530  0   0   0
5520  0   0   0
5510  0   0   0
5500  0   0   0
1590  0   0   0
1580  0   0   0
1570  0   0   0
1560  0   0   0
1550  0   0   0
1540  0   2   0
1530  0   0   0
1520  0   0   0
1510  0   0   0
1500  0   0   0
5490  0   0   0
5480  0   0   0
5470  0   0   0
5460  0   0   0
5450  0   0   0
5440  0   0   0
5430  0   0   0
5420  0   0   0
5410  0   0   0
5400  0   0   0
1490  0   0   0
1480  0   0   0
```

```
1470  0   0   0
1460  0   0   0
1450  0   0   0
1440  0   0   0
1430  0   0   0
1420  0   0   0
1410  0   0   0
1400  0   0   0
5390  0   0   0
5380  0   0   0
5370  0   0   8
5360  0   0   0
5350  0   0   0
5340  0   0   0
5330  0   4   0
5320  0   0   0
5310  0   0   0
5300  0   0   0
4950  0   0   0
4940  0   0   0
1390  0   0   0
4930  0   0   0
1380  0   0   0
4920  0   0   0
1370  0   0   0
2990  0   0   0
4910  0   0   0
1360  0   0   0
2980  0   0   0
4900  0   0   0
1350  0   0   0
2970  0   0   0
1340  0   0   0
2960  0   0   0
1330  0   0   0
2950  0   0   0
1320  0   0   0
2940  0   0   0
```

```
1310  0   0   0
2930  0   0   0
1300  0   0   0
2920  0   0   0
2910  0   0   0
2900  0   0   0
5290  0   0   0
5280  0   0   0
5270  0   0   3
5260  0   0   0
5250  0   0   0
5240  0   0   0
5230  0   1   0
5220  0   0   0
5210  0   0   0
5200  0   0   0
4890  0   0   0
4880  0   0   0
4870  0   0   0
4860  0   0   0
4850  0   0   0
4840  0   0   3709801
1290  0   32  163
4830  0   0   0
1280  0   0   115
4820  0   0   0
2890  0   0   0
4810  0   0   0
2880  0   0   0
4800  0   0   0
2870  0   230966142
2860  0   0   0
2850  0   9   0
2840  0   801180
2830  0   22634230
2820  0   22930420
2810  0   7   0
2800  0   23074430
```

```
5190  0   0   0
5180  0   0   0
5170  0   0   0
5160  0   0   0
5150  0   0   0
5140  0   0   0
5130  0   0   0
5120  0   0   0
4790  0   0   0
4780  0   0   0
4770  0   0   0
4760  0   0   0
4750  0   0   0
4740  0   0   0
4730  0   0   3
4720  0   0   0
2790  0   0   0
4710  0   0   0
2780  0   0   0
4700  0   0   0
2770  0   0   0
2760  0   0   0
2750  0   1   0
2740  0   29  0
2730  0   0   0
2720  0   0   0
2710  0   0   0
2700  0   0   0
4690  0   0   0
4680  0   0   0
4670  0   0   0
4660  0   0   0
4650  0   0   0
3030  0   0   0
4640  0   0   0
3020  0   0   0
4630  0   0   0
3010  0   0   0
```

```
4620  0   0   0
2690  0   0   0
3000  0   0   0
4610  0   0   0
2680  0   0   0
2670  0   0   0
4600  0   0   0
71 0  0   0   0
2660  0   0   0
Table=End
                        ""


Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
.iso.org.dod.internet.mgmt.mib-2.ospf.ospfIfTable.ospfIfEntrySnapshot52005-12-
20T21:37:12EST
LabelLabelLabel
ospfIfIpAddressospfIfEventsospfAddressLessIf
ValueValueValue
10.56.131.110
172.20.2.19510
172.16.0.310
172.16.128.310
172.30.252.310
47.142.85.13110
10.56.130.110
47.142.85.19500
172.16.109.110
172.30.242.16610
47.142.86.3210
172.30.252.1010
10.60.127.310
192.168.223.11050
10.10.3.310
172.16.17.3710
172.30.252.5110
10.10.0.310
Table=End
                    ""
```

```
Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStg.rcStgPortTable.rcStgPortEntrySnapshot52005-12-20T21:38:14EST
LabelLabel
rcStgPortrcStgPortForwardTransitions
ValueValue
2350
5770
1440
4860
2330
1420
4840
1295
2310
2180
1400
2890
4690
1980
2160
5580
4800
2870
4670
1960
2140
5560
2850
4650
3030
1940
2120
5540
2830
4630
3010
```

1920
2100
5520
5390
2810
4610
2680
4480
5500
5370
71 0
2660
5350
2640
5330
2620
1580
5310
5180
2600
1560
5160
1540
5140
1520
4940
1390
5120
5830
2280
1500
4920
1370
2990
4790
5810
2260
4900

```
1350
2970
4770
2240
1330
2950
4750
2220
2090
2930
1310
4730
2200
2070
5490
2910
4710
2780
4580
2050
5470
2760
68 48
4560
2030
5450
2740
66 0
4540
2010
5430
2720
64 0
2590
4520
5410
5280
2700
```

2570
4500
5260
5240
1490
5220
2380
1600
1470
5200
4890
2360
57848
1450
4870
2340
5760
1430
4850
2320
2190
1410
4830
1280
1990
2300
2170
5590
4810
2880
4680
1970
2150
5570
2860
4660
1950
2130

```
5550
2840
4640
3020
1930
2110
5530
2820
4620
2690
3000
4490
5510
5380
2800
2670
4600
5360
70 0
2650
5340
2630
1590
5320
5190
2610
1570
5300
5170
1550
5150
1530
4950
5130
2290
1510
4930
1380
```

```
5820
2270
4910
1360
2980
4780
5800
2250
1340
2960
4760
2230
2940
1320
4740
2210
2080
2920
1300
4720
2790
4590
2060
5480
2900
4700
2770
69 0
4570
2040
2750
67 0
4550
2020
5440
2730
65 0
4530
```

```
2000
5420
5290
2710
2580
4510
5400
5270
2560
5250
5230
2392
1610
1480
5210
2370
5790
1460
4880
Table=End
                    ""


Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
.iso.org.dod.internet.mgmt.mib-2.ospf.ospfNbrTable.ospfNbrEntrySnapshot52005-12-
20T21:37:15EST
LabelLabelLabel
ospfNbrIpAddrospfNbrAddressLessIndexospfNbrEvents
ValueValueValue
172.30.252.105
172.30.252.1105
172.30.242.16505
172.30.252.205
Table=End
                        ""


Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
```

```
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatGigTable.rcS
tatGigEntrySnapshot52005-12-20T21:37:40EST

LabelLabelLabelLabelLabel

rcStatGigPortIndexrcStatGigLinkFailuresrcStatGigPacketErrorsrcStatGigCarrierErrors
rcStatGigLinkInactiveErrors

ValueValueValueValueValue

70 0  0   0   0

2651  0   0   0

2641  0   0   0

2631  0   0   0

2621  0   0   0

2611  0   0   0

2601  0   0   0

4591  0   0   0

4581  0   0   0

69 24 0   0   0

4571  0   0   0

68 34 0   0   0

4561  0   0   0

67 0  0   0   0

4551  0   0   0

66 0  0   0   0

4541  0   0   0

65 0  0   0   0

4531  0   0   0

64 0  0   0   0

2591  0   0   0

4521  0   0   0

2581  0   0   0

4511  0   0   0

2571  0   0   0

4501  0   0   0

2562  0   0   0

4491  0   0   0

4482  0   0   0

2394  0   0   0

2381  0   0   0

2371  0   0   0

2363  0   0   0
```

```
2351  0   0   0
2341  0   0   0
2331  0   0   0
2321  0   0   0
2311220   0   0
1991  0   0   0
2301210   0   0
1981  0   0   0
1971  0   0   0
1961  0   0   0
1951  0   0   0
1941  0   0   0
1931  0   0   0
1921  0   0   0
2291  0   0   0
5830  0   0   0
2281  0   0   0
5820  0   0   0
2271  0   0   0
5810  0   0   0
2261  0   0   0
5803  0   0   0
2251  0   0   0
2242  0   0   0
2231  0   0   0
22212 0   0   0
2211  0   0   0
2201  0   0   0
5792  0   0   0
57838 0   0   0
5771  0   0   0
5761  0   0   0
2191  0   0   0
2181  0   0   0
2171  0   0   0
2161  0   0   0
2151  0   0   0
2141  0   0   0
```

```
2131  0   0   0
2121  0   0   0
2111  0   0   0
2101  0   0   0
2091  0   0   0
2081  0   0   0
2071  0   0   0
2061  0   0   0
2051  0   0   0
2041  0   0   0
2031  0   0   0
2021  0   0   0
2011  0   0   0
2001  0   0   0
1611  0   0   0
1601  0   0   0
5595  0   0   0
5581  0   0   0
5571  0   0   0
5561  0   0   0
5555  0   0   0
5541  0   0   0
5531  0   0   0
5521  0   0   0
5511  0   0   0
5501  0   0   0
1591  0   0   0
1581  0   0   0
1571  0   0   0
1561  0   0   0
1551  0   0   0
1542  0   0   0
1531  0   0   0
1521  0   0   0
1513  0   0   0
1501  0   0   0
5491  0   0   0
5481  0   0   0
```

```
5475  0   0   0
5462  0   0   0
5453  0   0   0
5442  0   0   0
5431  0   0   0
5421  0   0   0
5411  0   0   0
5401  0   0   0
1491  0   0   0
1481  0   0   0
1471  0   0   0
1461  0   0   0
1451  0   0   0
14410050 0   0
1431  0   0   0
1421  0   0   0
1411  0   0   0
1401  0   0   0
5391  0   0   0
5381  0   0   0
53751 0   0   0
5361  0   0   0
5351  0   0   0
5341  0   0   0
53316 0   0   0
5321  0   0   0
5311  0   0   0
5301  0   0   0
4954  0   0   0
4944  0   0   0
1391  0   0   0
4931  0   0   0
1383  0   0   0
4921  0   0   0
1371  0   0   0
2991  0   0   0
4911  0   0   0
1361  0   0   0
```

```
2981  0   0   0
4901  0   0   0
1351  0   0   0
2971  0   0   0
1341  0   0   0
2962  0   0   0
1331  0   0   0
2951  0   0   0
1321  0   0   0
2941  0   0   0
1311  0   0   0
2931  0   0   0
1301  0   0   0
2921  0   0   0
2911  0   0   0
2901  0   0   0
5291  0   0   0
5281  0   0   0
5271  0   0   0
5261  0   0   0
5251  0   0   0
5241  0   0   0
52351 0   0   0
5221  0   0   0
5211  0   0   0
5201  0   0   0
4891  0   0   0
4881  0   0   0
4871  0   0   0
4861  0   0   0
4851  0   0   0
4848  0   0   0
1297  0   0   0
4831  0   0   0
1283  0   0   0
4823  0   0   0
2891  0   0   0
4811  0   0   0
```

```
2881  0   0   0
4801  0   0   0
2873710   0   0
2861  0   0   0
2857  0   0   0
2845200   0   0
28312 0   0   0
28214 0   0   0
28112 0   0   0
28012 0   0   0
5191  0   0   0
5181  0   0   0
5171  0   0   0
5161  0   0   0
5151  0   0   0
5141  0   0   0
5131  0   0   0
5121  0   0   0
4791  0   0   0
4781  0   0   0
4771  0   0   0
4761  0   0   0
4751  0   0   0
4741  0   0   0
4738  0   0   0
4721  0   0   0
2791  0   0   0
4711  0   0   0
2782  0   0   0
4701  0   0   0
2778  0   0   0
2767  0   0   0
2759  0   0   0
2749  0   0   0
2738  0   0   0
27211 0   0   0
2711  0   0   0
2701  0   0   0
```

```
4691  0   0   0
4681  0   0   0
4671  0   0   0
4661  0   0   0
4657  0   0   0
3033  0   0   0
4641  0   0   0
3023  0   0   0
4632  0   0   0
3011  0   0   0
4622  0   0   0
2691  0   0   0
3001  0   0   0
4611  0   0   0
2681  0   0   0
2671  0   0   0
4601  0   0   0
71 0  0   0   0
2661  0   0   0
Table=End
                        " "


Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
.iso.org.dod.internet.mgmt.mib-
2.vrrp.vrrpMIB.vrrpStatistics.vrrpRouterStatsTable.vrrpRouterStatsEntrySnapshot5
2005-12-20T21:39:22EST
LabelLabelLabel
vrrpStatsIfIndexvrrpStatsVrIdvrrpStatsBecomeMaster
ValueValueValue
21777 1
208710129
20951401
20911201
20851001
21116 1
2083601
2185511
20891101
```

```
21072468
20971501
20931301
2055111
21052458
Table=End
                                        ""


Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntrySnapshot52005-12-
20T21:38:29EST
LabelLabelLabelLabelLabelLabelLabelLabel
ifIndexifInOctetsifInDiscardsifInErrorsifOutOctetsifOutDiscardsifDescrifOutErrors
ValueValueValueValueValueValueValueValue
70 27469103800311337888801000GbicLx Port 1/7 Name ToM40-00
2650  0   0   0   0   10/100BaseTX Port 4/10 Name GWC_41_Unit10
2640  0   0   0   0   10/100BaseTX Port 4/9 Name GWC_40_Unit10
2630  0   0   0   0   10/100BaseTX Port 4/8 Name 0
2620  0   0   0   0   10/100BaseTX Port 4/7 Name GWC_42_Unit10
2610  0   0   0   0   10/100BaseTX Port 4/6 Name 0
2600  0   0   0   0   10/100BaseTX Port 4/5 Name GWC_36_Unit10
4590  0   0   0   0   10/100BaseTX Port 7/12 Name 0
4580  0   0   0   0   10/100BaseTX Port 7/11 Name 0
69 99691800  42110163601000GbicSx Port 1/6 Name IW-SPM0
4570  0   0   0   0   10/100BaseTX Port 7/10 Name 0
68 109405980912928021026163068330 1000GbicLx Port 1/5 Name Acme-Enterprise0
4560  0   0   0   0   10/100BaseTX Port 7/9 Name 0
67 31018507600535819520 1000GbicSx Port 1/4 Name 0
4550  0   0   0   0   10/100BaseTX Port 7/8 Name 0
66 24118836580022314805001000GbicSx Port 1/3 Name Alteon 6614_1 Port 100
4540  0   0   0   0   10/100BaseTX Port 7/7 Name 0
65 29543349640093224557 01000GbicLx Port 1/2 Name 0
4530  0   0   0   0   10/100BaseTX Port 7/6 Name 0
64 16778053991153408997934 1201000GbicSx Port 1/1 Name IST0
2590  0   0   0   0   10/100BaseTX Port 4/4 Name GWC_35_Unit10
4520  0   0   0   0   10/100BaseTX Port 7/5 Name 0
2580  0   0   0   0   10/100BaseTX Port 4/3 Name GWC_34_Unit10
4510  0   0   0   0   10/100BaseTX Port 7/4 Name 0
```

```
2570  0   0   0   0  10/100BaseTX Port 4/2 Name GWC_33_Unit10
4500  0   0   0   0  10/100BaseTX Port 7/3 Name 0
25680000 0  443328010/100BaseTX Port 4/1 Name GWC_32_Unit12
4490  0   0   0   0  10/100BaseTX Port 7/2 Name 0
4480  0   0  2107090800100BaseTX Port 7/1 Name AMS_0_11
2392005591721001904915850100BaseTX Port 3/48 Name 5
2380  0   0  522442880100BaseTX Port 3/47 Name a802996
2370  0   0   0   0  10/100BaseTX Port 3/46 Name 0
2360  0   0  69359133010/100BaseTX Port 3/45 Name 7
2350  0   0   0   0  10/100BaseTX Port 3/44 Name SDM0
2340  0   0   0   0  10/100BaseTX Port 3/43 Name HIOP0
2330  0   0   0   0  10/100BaseTX Port 3/42 Name 0
2320  0   0   0   0  10/100BaseTX Port 3/41 Name 0
2311284278418022543091666010 0BaseTX Port 3/40 Name CICM-2_Callp143
1990  0   0   0   0  10/100BaseTX Port 3/8 Name GWC_07_Unit10
2305733126250228419564420100BaseTX Port 3/39 Name CICM-2_OAM123
1980  0   0   0   0  10/100BaseTX Port 3/7 Name 0
1970  0   0   0   0  10/100BaseTX Port 3/6 Name GWC_05_Unit10
1960  0   0   0   0  10/100BaseTX Port 3/5 Name GWC_04_Unit10
1950  0   0   0   0  10/100BaseTX Port 3/4 Name GWC_03_Unit10
1940  0   0   0   0  10/100BaseTX Port 3/3 Name GWC_02_Unit10
1930  0   0   0   0  10/100BaseTX Port 3/2 Name GWC_01_Unit10
1920  0   0   0   0  10/100BaseTX Port 3/1 Name GWC_00_Unit10
2290  0   0   0   0  10/100BaseTX Port 3/38 Name 0
5830  0   0   0   0  Gbic1000BaseT Port 9/8 Name 0
2280  0   0   0   0  10/100BaseTX Port 3/37 Name SAM21-8_SC10
5820  0   0   0   0  Gbic1000BaseT Port 9/7 Name 0
2270  0   0   0   0  10/100BaseTX Port 3/36 Name SAM21-01_SC10
5810  0   0   0   0  1000Gbic Port 9/6 Name 0
2260  0   0   0   0  10/100BaseTX Port 3/35 Name SAM21-01_SC00
5800  0   0  20933896001000GbicSx Port 9/5 Name 0
2250  0   0   0   0  10/100BaseTX Port 3/34 Name SAM21-03_SC10
22429873800056841591010/100BaseTX Port 3/33 Name SAM21-03_SC01
2230  0   0   0   0  10/100BaseTX Port 3/32 Name GWC_31_Unit10
22212796670066058705010/100BaseTX Port 3/31 Name GWC_30_Unit114
2210  0   0   0   0  10/100BaseTX Port 3/30 Name GWC_29_Unit10
2200  0   0   0   0  10/100BaseTX Port 3/29 Name GWC_28_Unit10
5790  0   0  34799744010 0GbicSx Port 9/4 Name 0
```

```
57810348921222561114747679413010000GbicLx Port 9/3 Name 0
5776239639200306261444010000GbicSx Port 9/2 Name OM3500 OAM0
576177257817710984033863425700 1000GbicSx Port 9/1 Name IST-OM35000
2190  0   0   0   0   10/100BaseTX Port 3/28 Name GWC_27_Unit10
2180  0   0   0   0   10/100BaseTX Port 3/27 Name GWC_26_Unit10
2170  0   0   0   0   10/100BaseTX Port 3/26 Name GWC_25_Unit10
2160  0   0   0   0   10/100BaseTX Port 3/25 Name GWC_24_Unit10
2150  0   0   0   0   10/100BaseTX Port 3/24 Name GWC_23_Unit10
2140  0   0   0   0   10/100BaseTX Port 3/23 Name GWC_22_Unit10
2130  0   0   0   0   10/100BaseTX Port 3/22 Name GWC_21_Unit10
2120  0   0   0   0   10/100BaseTX Port 3/21 Name GWC_20_Unit10
2110  0   0   0   0   10/100BaseTX Port 3/20 Name 0
2100  0   0   0   0   10/100BaseTX Port 3/19 Name GWC_18_Unit10
2090  0   0   0   0   10/100BaseTX Port 3/18 Name GWC_17_Unit10
2080  0   0   0   0   10/100BaseTX Port 3/17 Name GWC_16_Unit10
2070  0   0   0   0   10/100BaseTX Port 3/16 Name GWC_15_Unit10
2060  0   0   0   0   10/100BaseTX Port 3/15 Name GWC_14_Unit10
2050  0   0   0   0   10/100BaseTX Port 3/14 Name 0
2040  0   0   0   0   10/100BaseTX Port 3/13 Name GWC_12_Unit10
2030  0   0   0   0   10/100BaseTX Port 3/12 Name 0
2020  0   0   0   0   10/100BaseTX Port 3/11 Name GWC_10_Unit10
2010  0   0   0   0   10/100BaseTX Port 3/10 Name 0
2000  0   0   0   0   10/100BaseTX Port 3/9 Name 0
1610  0   0   0   0   1000GbicSx Port 2/34 Name IST-OM35000
1600  0   0   0   0   1000GbicSx Port 2/33 Name IST0
5592308201  2693490010/100BaseTX Port 8/48 Name CABLE_RKS3
5580  0   0   0   0   10/100BaseTX Port 8/47 Name CABLE_RKS0
5570  0   0   0   0   10/100BaseTX Port 8/46 Name CABLE_RKS0
5560  0   0   0   0   10/100BaseTX Port 8/45 Name 0
55517629900 2183427010/100BaseTX Port 8/44 Name 6
5540  0   0   0   0   10/100BaseTX Port 8/43 Name 0
5530  0   0   0   0   10/100BaseTX Port 8/42 Name 0
5520  0   0   0   0   10/100BaseTX Port 8/41 Name 0
5510  0   0   0   0   10/100BaseTX Port 8/40 Name 0
5500  0   0   0   0   10/100BaseTX Port 8/39 Name 0
15914114771000275967344010 0BaseTX Port 2/32 Name S1K_TLAN-test8
15812647058800216802176010 0BaseTX Port 2/31 Name S1K_ELAN-test9
1570  0   0   0   0   10/100BaseTX Port 2/30 Name 0
```

```
1561218983028592275279077010 0BaseTX Port 2/29 Name 0
1550  0   0   28763139860100BaseTX Port 2/28 Name 0
1541206394027702275191399010 0BaseTX Port 2/27 Name 1
1530  0   0   28763567200100BaseTX Port 2/26 Name 0
1520  0   0   0   0   10/100BaseTX Port 2/25 Name 0
1518972977280522337221960 0BaseTX Port 2/24 Name MCS0
1506578869580022661333780 0BaseTX Port 2/23 Name MCS0
5490  0   0   0   0   10/100BaseTX Port 8/38 Name 0
5480  0   0   0   0   10/100BaseTX Port 8/37 Name 0
5472051203800002364705881010 0BaseTX Port 8/36 Name RTP4-SPC-U1-LinkB4
5464747654909828598777001 0/100BaseTX Port 8/35 Name 1
5451510604918042210673952010 0BaseTX Port 8/34 Name RTP4-SPC-U0-LinkB2
5440  0   0   348216320100BaseTX Port 8/33 Name 1
5430  0   0   0   0   10/100BaseTX Port 8/32 Name 0
5420  0   0   0   0   10/100BaseTX Port 8/31 Name 0
5410  0   0   0   0   10/100BaseTX Port 8/30 Name 0
5400  0   0   0   0   10/100BaseTX Port 8/29 Name 0
1496582188160022657775380 0BaseTX Port 2/22 Name MCS0
1481363957033002682961418010BaseTX Port 2/21 Name MCS0
1476581356800024105683860 0BaseTX Port 2/20 Name MCS0
1466581623680022657787540 0BaseTX Port 2/19 Name MCS0
1452383113600027130876095801 0BaseTX Port 2/18 Name MCS0
1449563307980110270214408601 0BaseTX Port 2/17 Name MCS0
1430  0   0   0   0   10/100BaseTX Port 2/16 Name 0
1420  0   0   0   0   10/100BaseTX Port 2/15 Name OLD_CMT_T14000
1410  0   0   0   0   10/100BaseTX Port 2/14 Name 0
1400  0   0   0   0   10/100BaseTX Port 2/13 Name 0
5390  0   0   0   0   10/100BaseTX Port 8/28 Name 3PC_temp0
5380  0   0   0   0   10/100BaseTX Port 8/27 Name 0
5372799420838938724075830 0/100BaseTX Port 8/26 Name 3PC53
5360  0   0   0   0   10/100BaseTX Port 8/25 Name 0
5350  0   0   0   0   10/100BaseTX Port 8/24 Name 0
5340  0   0   0   0   10/100BaseTX Port 8/23 Name 0
5331044530280511828044001 0/100BaseTX Port 8/22 Name 21
5320  0   0   0   0   10/100BaseTX Port 8/21 Name 0
5310  0   0   0   0   10/100BaseTX Port 8/20 Name 0
5300  0   0   0   0   10/100BaseTX Port 8/19 Name CBM 1 Port 30
4950  0   0   287232010/100BaseTX Port 7/48 Name 2
```

```
4940  0   0   59714390010/100BaseTX Port 7/47 Name NGSS_line_reserved2
1390  0   0   0   0   10/100BaseTX Port 2/12 Name 0
4930  0   0   0   0   10/100BaseTX Port 7/46 Name 0
13821527692800292795202801 00BaseTX Port 2/11 Name 2
4920  0   0   0   0   10/100BaseTX Port 7/45 Name NGSS_line_reserved0
13757786620002274234980010 0BaseTX Port 2/10 Name 0
2990  0   0   0   0   10/100BaseTX Port 4/44 Name 0
4910  0   0   0   0   10/100BaseTX Port 7/44 Name 0
1360  0   0   0   0   10/100BaseTX Port 2/9 Name 0
2980  0   0   28764616160100BaseTX Port 4/43 Name MCS-Media1
4900  0   0   0   0   10/100BaseTX Port 7/43 Name NGSS_lines0
1350  0   0   0   0   10/100BaseTX Port 2/8 Name 0
2970  0   0   0   0   10/100BaseTX Port 4/42 Name MCS-Media0
13414639863920013311197110100BaseTX Port 2/7 Name 0
29655512396101279344631201 00BaseTX Port 4/41 Name MCS-Media11
1330  0   0   0   0   10/100BaseTX Port 2/6 Name 0
2950  0   0   0   0   10/100BaseTX Port 4/40 Name MCS-Media0
1320  0   0   0   0   10/100BaseTX Port 2/5 Name 0
2940  0   0   0   0   10/100BaseTX Port 4/39 Name MCS-Media0
13143391072900262271012001 00BaseTX Port 2/4 Name 0
2930  0   0   0   0   10/100BaseTX Port 4/38 Name NGSS-Port0
1300  0   0   0   0   10/100BaseTX Port 2/3 Name 0
2920  0   0   0   0   10/100BaseTX Port 4/37 Name NGSS-Port0
2910  0   0   0   0   10/100BaseTX Port 4/36 Name 0
2900  0   0   0   0   10/100BaseTX Port 4/35 Name SAM21-07_SC00
5290  0   0   0   0   10/100BaseTX Port 8/18 Name 0
5280  0   0   0   0   10/100BaseTX Port 8/17 Name CBM 0 Port 30
52735034479703020473726450100BaseTX Port 8/16 Name cs2kprovEMS1-link10
52626185383960013267709500100BaseTX Port 8/15 Name cs2kprovEMS0-link10
5250  0   0   0   0   10/100BaseTX Port 8/14 Name 0
5240  0   0   0   0   10/100BaseTX Port 8/13 Name 0
5230  0   1   168960 10/100BaseTX Port 8/12 Name 90
5220  0   0   348595840100BaseTX Port 8/11 Name 1
5210  0   0   0   0   10/100BaseTX Port 8/10 Name 0
5200  0   0   0   0   10/100BaseTX Port 8/9 Name 0
4890  0   0   0   0   10/100BaseTX Port 7/42 Name 0
4880  0   0   0   0   10/100BaseTX Port 7/41 Name NGSS_lines0
4870  0   0   0   0   10/100BaseTX Port 7/40 Name NGSS_trunks_reserved0
```

```
4860  0   0   0   0   10/100BaseTX Port 7/39 Name STORM-XTS_interlink0
4850  0   0   0   0   10/100BaseTX Port 7/38 Name NGSS_trunks_reserved0
484237440704371001103482560001 00BaseTX Port 7/37 Name STORM-XTS_interlink7
1291049071252163332778421731 0100BaseTX Port 2/2 Name MG9K_EM476
4830  0   0   0   0   10/100BaseTX Port 7/36 Name RTP4-SPC-U1-Link10
1282108735115034661130 10/100BaseTX Port 2/1 Name 1
4826608896500237491280 10/100BaseTX Port 7/35 Name STORM-XTS6
2890  0   0   0   0   10/100BaseTX Port 4/34 Name SAM21-06_SC10
4810  0   0   0   0   10/100BaseTX Port 7/34 Name RTP4-SPC-U0-Link10
2880  0   0   0   0   10/100BaseTX Port 4/33 Name SAM21-06_SC00
4800  0   0   0   0   10/100BaseTX Port 7/33 Name STORM-XTS0
2873300697826422333568330325113801 00BaseTX Port 4/32 Name 428
2860  0   0   0   0   10/100BaseTX Port 4/31 Name 0
2855957699109947487316 10/100BaseTX Port 4/30 Name 22
2840  0   801182880138 10/100BaseTX Port 4/29 Name 27211
2837183456802286853949204604 10/100BaseTX Port 4/28 Name 35
2827179367102316780945642174 10/100BaseTX Port 4/27 Name 20
2817176224308945507165 10/100BaseTX Port 4/26 Name 13
2807173795902331332947420628 10/100BaseTX Port 4/25 Name GWC_PUBLIC_KEYMILE20
5190  0   0   0   0   10/100BaseTX Port 8/8 Name 0
5180  0   0   0   0   10/100BaseTX Port 8/7 Name 0
51764 0   0   4846230540100BaseTX Port 8/6 Name cs2kssNE1-link10
5163101343184001039229436 0100BaseTX Port 8/5 Name cs2kssNE1-link00
5150  0   0   4858527430100BaseTX Port 8/4 Name cs2kssNE2-link10
5141958019447003794189240100BaseTX Port 8/3 Name cs2kssNE2-link00
5130  0   0   0   0   10/100BaseTX Port 8/2 Name Alteon OAM firewall_10
5121601331309003437214806 0100BaseTX Port 8/1 Name AMS_0_10
4790  0   0   0   0   10/100BaseTX Port 7/32 Name MC0
4780  0   0   0   0   10/100BaseTX Port 7/31 Name CMT_interlink0
4770  0   0   0   0   10/100BaseTX Port 7/30 Name MC0
4760  0   0   0   0   10/100BaseTX Port 7/29 Name 0
4750  0   0   0   0   10/100BaseTX Port 7/28 Name 3PC0
4740  0   0   0   0   10/100BaseTX Port 7/27 Name CMT0
4738686246003135332079248570 10/100BaseTX Port 7/26 Name 3PC8
4720  0   0   0   0   10/100BaseTX Port 7/25 Name 0
2790  0   0   0   0   10/100BaseTX Port 4/24 Name  0
4710  0   0   0   0   10/100BaseTX Port 7/24 Name NFS0
2781553723017360392201 0/100BaseTX Port 4/23 Name GWC_60_Unit10
```

```
4700  0   0   0   0   10/100BaseTX Port 7/23 Name CBM_interlink0
2777179925300943314829010/100BaseTX Port 4/22 Name 8
2767070262100910419026010/100BaseTX Port 4/21 Name 12
2757169427501943525849010/100BaseTX Port 4/20 Name 6
2741311870029960339889010/100BaseTX Port 4/19 Name 8
2737164854900941680405010/100BaseTX Port 4/18 Name 6
2727149273200941113294010/100BaseTX Port 4/17 Name 10
2710  0   0   0   0   10/100BaseTX Port 4/16 Name GWC_47_Unit10
2700  0   0   0   0   10/100BaseTX Port 4/15 Name GWC_46_Unit10
4690  0   0   0   0   10/100BaseTX Port 7/22 Name USPc0
4680  0   0   0   0   10/100BaseTX Port 7/21 Name 0
4670  0   0   0   0   10/100BaseTX Port 7/20 Name 3PC_SC10
4660  0   0   0   0   10/100BaseTX Port 7/19 Name CBM 1 Port 10
4657056376017546452300l0/100BaseTX Port 7/18 Name 3PC_SC08
3031321458779003545960176010 0BaseTX Port 4/48 Name CICM_Client5
4640  0   0   0   0   10/100BaseTX Port 7/17 Name CBM 0 Port 10
3021420714860001844966438010 0BaseTX Port 4/47 Name CICM_Client3
4630  0   0   22370932150100BaseTX Port 7/16 Name cs2kprovEMS1-link01
3010  0   0   0   0   10/100BaseTX Port 4/46 Name CICM_EM0
4620  0   0   22370842230100BaseTX Port 7/15 Name cs2kprovEMS0-link03
2690  0   0   0   0   10/100BaseTX Port 4/14 Name GWC_45_Unit10
3000  0   0   0   0   10/100BaseTX Port 4/45 Name Acme_01_OAM0
4610  0   0   0   0   10/100BaseTX Port 7/14 Name MC0
2680  0   0   0   0   10/100BaseTX Port 4/13 Name GWC_44_Unit10
2670  0   0   0   0   10/100BaseTX Port 4/12 Name GWC_43_Unit10
4600  0   0   0   0   10/100BaseTX Port 7/13 Name 0
71 0  0   0   0   0   1000Gbic Port 1/8 Name Acme-Carrier0
2660  0   0   0   0   10/100BaseTX Port 4/11 Name 0
Table=End
                                    ""


SingleValues=Begin
MeasurementKindIntervalDuration
Snapshot5
MeasureIdCaptureTimeMeasureSuppId1ValueReliability
rcStatSmltIstDownCnt2005-12-20T21:38:07EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt1Valid
rcStatSmltSmltDownRxMsgCnt2005-12-20T21:38:07EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt2Valid
```

sysObjectID2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.system
.iso.org.dod.internet.private.enterprises.rapidCity.rcA8610Valid

sysDescr2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.systemPassport-8610
(3.7.2.2)Valid

sysLocation2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.system4655 Great
America Parkway Santa Clara CA 95054Valid

sysUpTime2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.system2790795Valid

sysName2005-12-20T21:38:24EST.iso.org.dod.internet.mgmt.mib-2.systemSuperman-C2Valid

ipOutRequests2005-12-20T21:39:16EST.iso.org.dod.internet.mgmt.mib-2.ip103000479Valid

ipInReceives2005-12-20T21:39:16EST.iso.org.dod.internet.mgmt.mib-2.ip2639631467Valid

ipInDiscards2005-12-20T21:39:16EST.iso.org.dod.internet.mgmt.mib-2.ip0Valid

ipOutDiscards2005-12-20T21:39:16EST.iso.org.dod.internet.mgmt.mib-2.ip0Valid

snmpInvalidMsgs2005-12-20T21:37:07EST
.iso.org.dod.internet.snmpV2.snmpModules.snmpMPDMIB.snmpMPDMIBObjects.snmpMPDStats0
Valid

snmpOutPkts2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp4685310Valid

snmpOutTraps2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0Valid

snmpInTotalSetVars2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0Valid

snmpInPkts2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp4685410Valid

snmpInTotalReqVars2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp
20367670Valid

snmpInASNParseErrs2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0Valid

snmpInBadVersions2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0Valid

snmpInBadCommunityUses2005-12-20T21:37:08EST.iso.org.dod.internet.mgmt.mib-2.snmp0
Valid

rcSysBufferUtilPeakTime2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid

rcSysSwitchFabricUtil2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid

rcSysNVRamUsed2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid

rcSysBufferUtilPeak2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid

rcSysCpuUtil2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem11Valid

rcSysBufferUtil2005-12-20T21:37:17EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcSystem0Valid

rcStatSmltSmltDownTxMsgCnt2005-12-20T21:38:07EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt2Valid

rcStatSmltSmltUpRxMsgCnt2005-12-20T21:38:07EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt18Valid

rcStatSmltSmltUpTxMsgCnt2005-12-20T21:38:07EST
.iso.org.dod.internet.private.enterprises.rapidCity.rcMgmt.rcStat.rcStatMlt18Valid

SingleValues=End

```
                        " "
Entity=End
                        " "
System=End
                        " "
PMFile=End
```

GUI/CLUI Documentation for ERS 8600

GUI Launching and User procedures

- 316341-B Rev 00 - Installing and Using Device Manager
- 314723-C - Configuring Network Management

Related documentation

- 314724-C - Configuring and Managing Security
- 314997-C - Read Me for Security
- 316341-B - Installing and Using Device Manager
- 313189-D - Getting Started
- 315545-C - Managing Platform Operations and Using Diagnostics Tools
- 314723-C - Configuring Network Management
- 314721-C - Configuring BGP Services
- 316433-C - Configuring QoS and IP Filtering
- 314720-D - Configuring IP Routing Operations
- 314725-C - Configuring Layer 2 Operations: "VLANs," Spanning "Tree," Multilink Trunking
- 314719-C - Configuring IP Multicast Routing Protocols
- 316343-B - Configuring IGMP for User Authentication (IGAP)
- 314722-B - Configuring IPX Routing Operations
- 314995-B - Configuring the Web Switching Module with Device Manager
- 315015-C - System Messaging Platform Reference Guide
- 315023-C - Using the Packet Capture Tool

Gateway Controller (GWC)

This section contains IEMS Northbound log samples and device documentation references for the GWC.

GWC Fault Interface

Fault documentation for GWC :

- NN10202-911 - GWC Fault Management

Fault Mapping for GWC

The following criteria can be used for looking up information on specific faults for GWC.

Fault Correlation for GWC

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
GWC	logname and number	logname and number	logname and number	logname and number	NN10202-911 GWC Fault Management

Northbound Fault Formats for GWC

SCC2

The following is an example of a GWC log in SCC2 format:

```
**14 GWC 307 7250 TBL  GWC Fault
        Location: GWC-2-UNIT-0
        NotificationID: 4
        State: Raise
        Category: Communications
        Cause: Communications subsystem failure
        Time: Jan 23 15:15:59 2004
        Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Unit=unit_0;Software=NODE
        MTC
        Specific Problem: EM not responding, provisioned data loaded from local
        Flash
        Description: Element Manager communication failure.
```

NTSTD

The following is an example of a GWC log in NTSTD format:

```
COMPACT06BT  **  GWC307 Jan23 20:14:38 7250 TBL  GWC Fault
        Location: GWC-2-UNIT-0
        NotificationID: 4
        State: Raise
        Category: Communications
        Cause: Communications subsystem failure
        Time: Jan 23 15:15:59 2004
        Component Id: GWC=GWC-2-UNIT-0;Version=PGC92BA;Unit=unit_0;Software=NODE
        MTC
        Specific Problem: EM not responding, provisioned data loaded from local
        Flash
        Description: Element Manager communication failure.
```

SNMP

The following is an example of a GWC log in SNMP format:

```
system.sysUpTime.0 => 23:10:15
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.
20.50.48
.48.52.45.49.45.50.51.44.51.58.49.52.58.51.56.46.48.44.42848
alarmActiveDateAndTime => 2004-1-23,3:14:38.0,
alarmActiveDescription => Communication with a gateway is down.
nnExtAlarmActiveEventType => 2
nnExtAlarmActiveProbableCause => 554
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => GWC304
nnExtAlarmActiveResourceDescription => IEMS=0x00000063000000a1ac101127-GWC-
19-UNIT-1;GWC=GWC-19-UNIT-1;Version=GN090CD;Unit=unit_1;Software=SSC
nnExtAlarmActiveManualClear => 0
nnExtAlarmActiveSequenceNumber => 9028
```

Syslog

The following is an example of a GWC log in Syslog format:

```
Feb 23 15:15:56 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7307~~  GWC307 MAJOR TBL
GWC Fault^M        Location: GWC-2-UNIT-0^M        NotificationID: 4^M        State:
Raise^M        Category: Communications^M        Cause: Communications subsystem
failure^M        Time: Jan 23 15:15:59 2004^M        Component Id: GWC=GWC-2-UNIT-
0;Version=PGC92BA;Unit=unit_0;Software=NODE^M       MTC^M       Specific Problem: EM
not responding, provisioned data loaded from local^M       Flash^M       Description:
Element Manager communication failure.^M
```

Performance

OM and PM Documentation references for GWC

- NN10208-711 - GWC Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for GWC in XML format:

```
<TableId>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPe
rfRefMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry</TableId>

<CaptureTime>2004-12-15T00:11:58EST</CaptureTime>

- <Labels>

<Label>nnPerfMetricRefIndex</Label>

<Label>nnPerfMetricName</Label>

<Label>nnPerfMetricGroup</Label>

<Label>nnPerfMetricDataType</Label>

<Label>nnPerfMetricSources</Label>

<Label>nnPerfMetricValue</Label>

</Labels>

- <RowOfValues>

- <RowValue>

<Value>13</Value>

</RowValue>

- <RowValue>

<Value>Peer connections attempted during interval</Value>

</RowValue>

- <RowValue>

<Value>Measurement</Value>

</RowValue>

- <RowValue>
```

```
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>2937</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>4</Value>
</RowValue>
- <RowValue>
<Value>Total Gateways Provisioned</Value>
</RowValue>
- <RowValue>
<Value>Measurement</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>10</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>12</Value>
</RowValue>
- <RowValue>
<Value>Peer connections completed during interval</Value>
</RowValue>
- <RowValue>
<Value>Measurement</Value>
```

```
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>2936</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>11</Value>
</RowValue>
- <RowValue>
<Value>Peer connections failed during interval</Value>
</RowValue>
- <RowValue>
<Value>Communications</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>Large GWs in Disabled State</Value>
</RowValue>
```

```
- <RowValue>
<Value>Communications</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>8</Value>
</RowValue>
</RowOfValues>
</Table>
```


CSV

The following is an example of performance data for GWC in CSV format:

```
PMFile=Begin
MeasurementCategory          noNamespaceSchemaLocation    FileCreationTime
PM                           commonPerfRecord_V2.0.xsd    2005-06-29T06:30:06EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId
47.165.172.140-GWC-212

Table=Begin
TableId                      MeasurementKind              IntervalDuration  CaptureTime
.iso.org.dod.internet.private.e
nterprises.nortel.nortelGener
icMIBs.nortelPerfRefMIB.nn
PerfMetricReferenceTable.n   Snapshot                                    5 2005-06-29T06:30:01EST
Label                        Label                        Label             Label
nnPerfMetricRefIndex         nnPerfMetricName             nnPerfMetricGroup nnPerfMetricValue
Value                        Value                        Value             Value
                          17 Calls failed for MP: MP2     Measurement                0
                          16 Calls passed for MP: MP2     Measurement                0
                          15 Total Media Proxies Provisioned Measurement             1
                          14 Media Proxies in Disabled State Communications          0
                             Media Proxy calls failed during
                          97 interval for GWC             Measurement                0
                           4 Total Gateways Provisioned   Measurement                2
                             Media Proxy calls passed during
                          96 interval for GWC             Measurement                0
                           2 Trunk GWs in Disabled State  Communications             0
Table=End

Entity=End

System=End

PMFile=End
```

GUI/CLUI Documentation for GWC

GUI Launching and User procedures

- NN10189-111 - GWC Basics
- NN10205-511 - GWC Configuration Management
- NN10213-611 - GWC Security and Administration

Related documents

Keymile UNEM and UMUX

Keymile UNEM and UMUX Fault Interface

This section provides references to customer documentation for Fault, Performance, Topology, GUI/CLUI, and Security for Keymile UNEM and UMUX.

Fault documentation for Keymile UNEM and UMUX:

- KEYMILE001, Keymile Documentation and Support

Fault Mapping for Keymile UNEM and UMUX

The following criteria can be used for looking up information on specific faults for Keymile UNEM and UMUX devices.

Table 1 Fault Correlation for Keymile Traps

Trap Name	Log Name & No.	Document Reference
alarmRaisedTrap (communicationAlarm)	UMUX300 UNEM300	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmRaisedTrap (equipmentAlarm)	UMUX301 UNEM301	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmRaisedTrap (environmentalAlarm)	UMUX302 UNEM302	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmRaisedTrap (processingErrorAlarm)	UMUX303 UNEM303	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmRaisedTrap (qualityOfServiceAlarm)	UMUX304 UNEM304	Keymile UMUX User's Guide Keymile UNEM User's Guide
alarmClearedTrap	UMUX500 UNEM500	Keymile UMUX User's Guide Keymile UNEM User's Guide
neOpStatModified trap	UMUX501	Keymile UNEM User's Guide
nePollStatModified	UMUX502	Keymile UNEM User's Guide
alarmAckTrap	UMUX600 UNEM600	Keymile UMUX User's Guide Keymile UNEM User's Guide

Trap Name	Log Name & No.	Document Reference
neAdded	UMUX601	Keymile UNEM User's Guide
neDeleted	UMUX602	Keymile UNEM User's Guide
neNameModified	UMUX603	Keymile UNEM User's Guide
cardAdded	UMUX604	Keymile UMUX User's Guide
cardDeleted	UMUX605	Keymile UMUX User's Guide

Northbound Fault Formats for Keymile

SCC2

The following is an example of a Keymile log in SCC2 format:

```
54 UMUX601 0023 INFO UMUX Added
        Location: OTT_UMUX_TESTING
        State: INFO
        Time: Mar 31 03:54:48 2005
        Component Id: OTT_UMUX_TESTING 47.134. 44.110
        Description: OTT_UMUX_TESTING NE Added

**46 UMUX300 0009 TBL  UMUX FLT
        Location: OTT_UMUX_1200
        Notification ID: 0
        State: Raised
        Category: communication
        Cause: others
        Time: Mar 17 13:46:27 2005
        Component Id: LOMIF <12> 2Mbit/s-1 / E12
        Specific Problem:  others
        Description: Loss of Signal
```

NTSTD

The following is an example of a Keymile log in NTSTD format:

```
wnc0s0jn     UMUX601 MAR29 05:35:35 INFO UMUX Added
        Location: OTT_UMUX_1200_Test
```

```
        State: INFO
        Time: Mar 29 05:35:35 2005
        Component Id: OTT_UMUX_1200_Test797322492
        Description: OTT_UMUX_1200_Test NE Added


wnc0s0jn *** UMUX300 MAR29 05:09:44 0482 TBL  UMUX FLT
        Location: OTT_UMUX_1200
        Notification ID: 0
        State: Raised
        Category: communication
        Cause: others
        Time: Mar 29 05:09:44 2005
        Component Id: LOMIF <12> 2Mbit/s-1 / E12
        Specific Problem:  others
        Description: AIS Received
```

SNMP

The following is an example of a Keymile log in SNMP format:

```
.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0:  TimeTicks:  2 hours, 48 minutes, 38
seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0:  Object ID:  .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1:  STRING:  .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2:  STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-37;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3:  STRING:  ^G^E,^F^B:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4:  STRING:  UMUX601:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING:   44 UMUX601 0047 INFO UMUX
Added :
UMUX_TESTING( 10. 10.  1.  1) NE Added :


.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0:  TimeTicks:  3 hours, 11 minutes, 8
seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0:  Object ID:  .1.3.6.1.4.1.562.29.6.1.0.305:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10:  STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.18.50.48.48.53.45.5
2.45.56.44.54.58.51.52.58.48.46.48.44.23905:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2:  07 d5 04 08 06 22 00 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11:  STRING:  DeviceSpecificInfo=;AIS Received:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1:  INTEGER:  5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2:  INTEGER:  1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3:  STRING:  :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4:  STRING:  UMUX300:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5:  STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
```

```
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6:  INTEGER:  1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7:  INTEGER:  16:
```

Syslog

The following is an example of a Keymile log in Syslog format:

```
Apr  8 00:59:37 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=9434~~ UMUX601 NONE INFO
UMUX Added^M       Location: MYTest^M       State: INFO^M       Time: Apr 08 00:59:37
2005^M       Component Id: MYTest 10.  1.  5.  1^M       Description: MYTest NE Added


Apr  8 01:27:24 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=9447~~ UMUX300 CRIT TBL
UMUX FLT^M       Location: OTT_UMUX_1200^M       Notification ID: 0^M       State:
Raised^M       Category: communication^M       Cause: others^M       Time: Apr 08
01:54:45 2005^M       Component Id: LOMIF <12> 2Mbit/s-1 / E12^M       Specific
Problem:  others^M       Description: AIS Received
```

Performance

Performance metrics are not available through the IEMS. Please refer to the Keymile UNEM User's Guide.

GUI Documentation for Keymile

GUI Launching and User procedures

- Keymile UNEM UNEM User's Guide
- Keymile UCST System Opeartion Basics

Media Application Server (MAS)

MAS Fault Interface

This section provides references to customer documentation for Fault Management for MAS.

Fault documentation for MAS :

- NN10383-900 - Fault Management: Alarm and Logs
- NN10375-113 - MAS Unified Communications Service Guide

- NN100388-111 - MAS Ad Hoc Audio Conferencing Service Guide
- NN10433-111 - MAS Meet Me Audio Conferencing Service Guide
- NN10429-113 - MAS IM Chat Service Guide
- NN10430-113 - MAS Music On Hold Service Guide
- NN10428-113 - MAS Announcements Service Guide

Fault Mapping for MAS

The following criteria can be used for looking up information on specific faults for MAS.

Fault Correlation for MAS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MAS	Event Id Logname and Log number	Event Id Logname and Log number	Event Id Logname and Log number	Event Id Logname and Log number	NN10383-900 - Fault Management: Alarm and Logs Also refer to the documents listed above

Northbound Fault Formats for MAS

SCC2

The following is an example of a MAS log in SCC2 format:

```
*C00 MAS 330 2515 FLT  Fault
        Location: 47.104.11.120
        Notification Id: 1001
        State: Raised
        Category: processingError
        Cause: applicationSubsystemFailure
        Time: Mar 23 10:46:51 2004
        Component Id: MediaServer_CStore
        Specific Problem: MAS;330
        Description: Component Shutdown
```

NTSTD

The following is an example of a MAS log in NTSTD format:

```
RTPU07CAPT ***  MAS330 MAR23 17:00:18 2310 FLT  Fault
        Location: 47.104.11.120
        Notification Id: 1001
        State: Raised
        Category: processingError
        Cause: applicationSubsystemFailure
        Time: Mar 23 10:46:51 2004
        Component Id: MediaServer_CStore
        Specific Problem: MAS;330
        Description: Component Shutdown
```

SNMP

The following is an example of a MAS log in SNMP format:

```
sysUpTime.0 => 1:52:16
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.51.45.50.51.44.48.58.48.58.49.56.46.54.44.
2572
alarmActiveDateAndTime => 2004-3-23,0:0:18.6
alarmActiveDescription => Location: 47.104.11.120
Notification Id: 1001
State: Raised
Category: processingError
Cause: applicationSubsystemFailure
Time: Mar 23 10:46:51 2004
Component Id: MediaServer_CStore
Specific Problem: MAS;330
Description: Component Shutdown

nnExtAlarmActiveEventType => 3
nnExtAlarmActiveProbableCause => 2
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => MAS 330
nnExtAlarmActiveResourceDescription => IEMS=47.104.11.120-MAS;MediaServer_CStore
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a MAS log in Syslog format:

```
Mar 23 12:00:19 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=3629~~  MAS330 CRIT FLT
Fault^M        Location: 47.104.11.120^M       Notification Id: 1001^M       State:
Raised^M       Category: processingError^M Cause: applicationSubsystemFailure^M
Time: Mar 23 10:46:51 2004^M       Component Id: MediaServer_CStore^M       Specific
Problem: MAS;330^M        Description: Component Shutdown
```

Performance

OM and PM Documentation references for MAS

- NN10384-700 - Performance Management : OM

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for MAS in XML format:

Not available at time of publication

CSV

The following is an example of Performance data for MAS in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2004-07-02T05:55:54EST
System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
47.104.11.120,MAS

SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
CreateConf,2004-07-02T05:13:44EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:44EST,ConfMP,40,Valid
```

```
CreateConf,2004-07-02T05:13:45EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:45EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:46EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:46EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:47EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:47EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:48EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:48EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:49EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:49EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:50EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:50EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:51EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:51EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:52EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:52EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:53EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:53EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:54EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:54EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:55EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:55EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:56EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:56EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:57EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:57EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:58EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:58EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:59EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:13:59EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:00EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:00EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:01EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:01EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:02EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:02EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:03EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:03EST,ConfMP,40,Valid
```

```
CreateConf,2004-07-02T05:14:04EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:04EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:05EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:05EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:06EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:06EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:07EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:07EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:08EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:08EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:09EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:09EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:10EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:10EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:11EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:11EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:12EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:12EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:13EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:13EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:14EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:14EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:15EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:15EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:16EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:16EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:17EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:17EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:18EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:18EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:19EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:19EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:20EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:20EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:21EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:21EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:22EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:22EST,ConfMP,40,Valid
```

```
CreateConf,2004-07-02T05:14:23EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:23EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:24EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:24EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:25EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:25EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:26EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:26EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:27EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:27EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:28EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:28EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:29EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:29EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:30EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:30EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:31EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:31EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:32EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:32EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:33EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:33EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:34EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:34EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:35EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:35EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:36EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:36EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:37EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:37EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:38EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:38EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:39EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:39EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:40EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:40EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:41EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:41EST,ConfMP,40,Valid
```

```
CreateConf,2004-07-02T05:14:42EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:42EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:43EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:43EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:44EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:44EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:45EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:45EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:46EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:46EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:47EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:47EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:48EST,ConfMP,40,Valid
CreateConf,2004-07-02T05:14:48EST,ConfMP,40,Valid
SingleValues=End
Entity=End
System=End
PMFile=End
```

GUI/CLUI Documentation for MAS

GUI Launching and User procedures

- NN10006-100 - MCS 5200 Basics

Related Documents

None

Multimedia Communication Server (MCS)

MCS Fault Interface

This section provides references to customer documentation for Fault Management for MCS.

Fault documentation for MCS :

- NN10383-900, Fault Management: Alarm and Log

Fault Mapping for MCS

The following criteria can be used for looking up information on specific faults for MCS.

Fault Correlation for MCS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MCS	Event Id Logname and Log number	Event Id Logname and Log number	Event Id Logname and Log number	Event Id Logname and Log number	NN10383-900, Fault Management: Alarm and Log

Northbound Fault Formats for MCS

SCC2

The following is an example of a MCS log in SCC2 format:

```
**55 LAM 102 0447 FLT  Fault
        Location: 47.104.23.117
        Notification Id: 1199
        State: Raised
        Category: communications
        Cause: communicationsSubsystemFailure
        Time: Mar 23 11:55:13 2004
        Component Id: Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.
        Appsvr.Services.appsvr.BillingTransferAgent.BtaPrimaryConnectToAmLost
        Specific Problem: LAM;102
        Description: severity=MAJOR;probableCause=communications subsystem failu
        re;addedText=Communication Error : Primary stream cannot connect to CAM;
```

NTSTD

The following is an example of a MCS log in NTSTD format:

```
RTPU07CAPT  **  LAM102 MAR23 16:55:13 0242 FLT  Fault
        Location: 47.104.23.117
        Notification Id: 1199
        State: Raised
        Category: communications
        Cause: communicationsSubsystemFailure
        Time: Mar 23 11:55:13 2004
        Component Id: Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.
```

```
Appsvr.Services.appsvr.BillingTransferAgent.BtaPrimaryConnectToAmLost
Specific Problem: LAM;102
Description: severity=MAJOR;probableCause=communications subsystem failu
re;addedText=Communication Error : Primary stream cannot connect to CAM;
```

SNMP

The following is an example of a MCS log in SNMP format:

```
sysUpTime.0 => 2:19:58
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.
21.50.48
.48.52.45.51.45.50.51.44.49.49.58.53.53.58.49.51.46.
48.44.2616
alarmActiveDateAndTime => 2004-3-23,11:55:13.0
alarmActiveDescription => severity=MAJOR;probableCause=communications
subsystem
failure;addedText=Communication Error : Primary stream cannot connect to CAM;
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 6
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => LAM 102
nnExtAlarmActiveResourceDescription => IEMS=47.104.23.117-
CSE;Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.Appsvr.Service
s.appsvr
.BillingTransferAge
nt.BtaPrimaryConnectToAmLost
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 533
```

Syslog

The following is an example of a MCS log in Syslog format:

```
Mar 23 12:17:08 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=1558~~  LAM102 MAJOR FLT
Fault^M        Location: 47.104.23.117^M        Notification Id: 1199^M        State:
Raised^M    Category: communications^M    Cause: communicationsSubsystemFailure^M
Time: Mar 23 11:55:13 2004^M        Component Id:
Site=MgmtSite;Server=AppSvr;System.Sites.MgmtSite.Servers.^M
Appsvr.Services.appsvr.BillingTransferAgent.BtaPrimaryConnectToAmLost^M
Specific Problem: LAM;102^M        Description:
severity=MAJOR;probableCause=communications subsystem failu^M
re;addedText=Communication Error : Primary stream cannot connect to CAM;
```

Performance

OM and PM Documentation references for MCS

- NN10384-700 - Performance Management: OM

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for MCS in XML format:

Not available at time of publication

CSV

The following is an example of Performance data for MAS in CSV format:

Not available at time of publication

GUI/CLUI Documentation for MCS

GUI Launching and User procedures

- NN10006-100 - MCS 5200 Basics
- NN10247-111 - Multimedia Communication Server 5200 System Management Console User Guide

Related Documents

None

Media Gateway 3200 (MG 3200)

MG3200 Fault Interface

This section provides references to customer documentation for Fault Management for MG 3200.

Fault documentation for MG3200:

LTRT-72704: Media Gateway MG3200 H.248 User's Manual

Fault Mapping for MG3200

The following criteria can be used for looking up information on specific faults for MG3200.

Fault Correlation for MG 3200

Trap Name	LogKey	Customer Doc Ref (Media Gateway MG3200 H.248 User's Manual: LTRT-72704)
acBoardFatalError	MGTH301	Appendix I
acBoardConfigurationError	MGTH302	Appendix I
acBoardTemperatureAlarm	MGTH303	Appendix I
acBoardEvBoardStarted	MGTH500	Appendix I
acBoardEvResettingBoard	MGTH300	Appendix I
acgwAdminStateChange	MGTH501	Appendix I
acBoardEthernetLinkAlarm	MGTH307	Appendix I
acActiveAlarmTableOverflow	MGTH309	Appendix I
acOperationalStateChange	MGTH312	Appendix I
acKeepAlive	MGTH313	Appendix I
acNATTraversalAlarm	MGTH314	Appendix I
acEnhancedBITStatus	MGTH600	Appendix I
acPerformanceMonitoringThresholdCrossing	MGTH800	Appendix I
dsx1LineStatusChange	MGTH601	Appendix I

coldStart	Will not be sent to NB All prior alarms from the device will be cleared and "Re-sync" operation will be invoked as the device has been reset.	Appendix I
authenticationFailure	Will not be sent to NB	Appendix I

Northbound Fault Formats for MG 3200

SCC2

The following is an example of a MG 3200 Board Resetting log in SCC2 format:

*C36 MGTH300 0123 FLT MG3200 INFO

Location: mg32;47.142.106.106

State: Raised

Category: equipment

Cause: outOfService

Time: Mar 05 21:36:09 2000

Component Id: Board#1

Trap Name: 4

Description: User resetting board

NTStd

The following is an example of a MG 3200 Board Resetting Alarm log in NTStd format:

wnc0s0jn *** MGTH300 MAR05 21:40:04 0003 FLT MG3200 INFO

Location: mg32;47.142.106.106

State: Raised

Category: equipment

Cause: outOfService

Time: Mar 05 21:40:04 2000

Component Id: Board#1

Trap Name: 4

Description: User resetting board

SNMP

The following is an example of a MG 3200 Board Resetting Alarm log in SNMP format:

.1.3.6.1.2.1.1.3.0: 2 hours, 42 minutes, 17 seconds. ,
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.562.29.6.1.0.305,
.1.3.6.1.2.1.118.1.2.2.1.10:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.48.45.51.45
.53.44.56.58.51.52.58.53.49.46.48.44.4433,
.1.3.6.1.2.1.118.1.2.2.1.2: 7 d0 3 5 8 22 33 0 ,
.1.3.6.1.2.1.118.1.2.2.1.11: User resetting board,
.1.3.6.1.4.1.562.29.6.1.1.1.1: 4,
.1.3.6.1.4.1.562.29.6.1.1.1.2: 612,
.1.3.6.1.4.1.562.29.6.1.1.1.3: ,
.1.3.6.1.4.1.562.29.6.1.1.1.4: MGTH300 ,
.1.3.6.1.4.1.562.29.6.1.1.1.5: IEMS=47.142.106.106-MG_3200;Board#1,
.1.3.6.1.4.1.562.29.6.1.1.1.6: 4,
.1.3.6.1.4.1.562.29.6.1.1.1.7: 645

Syslog

The following is an example of a MG 3200 Board Started log in Syslog format:

Apr 13 11:16:37 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=5565~~ MGTH300 CRIT F

LT MG3200 FAULT^M Location: mg32;47.142.106.106^M State: Raised^M

Category: equipment^M Cause: outOfService^M Time: Mar 05 2

1:45:21 2000^M Component Id: Board#1^M Trap Name: 4^M Descr

iption: User resetting board

The following is an example of a MG 3200 dsx1LineStatusChange log in Syslog format:

Apr 13 10:39:07 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=2520~~ MGTH601 NONE I

NFO ^M Location: 47.142.106.106^M Event: .1.3.6.1.2.1.10.18.15.0.
1^M Varbind0: .1.3.6.1.2.1.1.3.0: 382^M Varbind1: .1.3.6.1.6.3.1.1
.4.1.0: .1.3.6.1.2.1.10.18.15.0.1^M Varbind2: .1.3.6.1.2.1.10.18.6.1.10.5
: 2

Performance

OM and PM Documentation references for MG 3200

LTRT-72704: Media Gateway MG3200 H.248 User's Manual

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for MG 3200 in XMLformat:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2005-05-13T11:53:53EST</FileCreationTime>
- <System>
<SystemId>NortelNetworks/IEMS</SystemId>
- <Entity Type="MG 3200">
<EntityId>47.142.106.106</EntityId>
- <SingleValues MeasurementKind="Snapshot" IntervalDuration="1440">
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>6399</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Product: Mediant 2000;SW Version: 4.60D.007.002</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>7415</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>1140</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
```

```
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>5260</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>82</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>tcpOutSegs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.tcp</MeasureSuppId1>
<Value>21</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>tcpInSegs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.tcp</MeasureSuppId1>
<Value>26</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>udpOutDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.udp</MeasureSuppId1>
<Value>54156</Value>
```

<Reliability>Valid</Reliability>

</SingleValue>

- <SingleValue>

<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>

<MeasureId>udpInDatagrams</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.udp</MeasureSuppId1>

<Value>901</Value>

<Reliability>Valid</Reliability>

</SingleValue>

- <SingleValue>

<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>

<MeasureId>snmpSilentDrops</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

- <SingleValue>

<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>

<MeasureId>acPerfCpMessageSendSuccesses</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

- <SingleValue>

<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>

<MeasureId>acPerfCpMessagesFromUntrustedSources</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

- <SingleValue>

<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>

<MeasureId>acPerfCpMessageRetransmissions</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>

<Value>292690</Value>

<Reliability>Valid</Reliability>

```
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageSendErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageMaxRetransmissionsExceeded</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>41812</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageReceiveSuccesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpNumDupsForCompletedTransactions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpMessageReceiveErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpNumDupsForOutstandingTransactions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfCpProtocolSyntaxErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfCp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSimplexInSessionsCurrent</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpReceiverOctets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSimplexOutSessionsTotal</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpRcvrLostPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSimplexOutSessionsCurrent</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSenderPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpFailedDueToLackOfResources</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpDuplexSessionsTotal</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSenderOctets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpSimplexInSessionsTotal</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpDuplexSessionsCurrent</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfRtpReceiverPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfRtp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfSystemPacketEndpoints</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfSystem</MeasureSuppId1>
<Value>300</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
- <SingleValue>
<CaptureTime>2005-05-13T11:53:53EST</CaptureTime>
<MeasureId>acPerfSystemPacketEndpointsInUse</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.
acPerfMediaGateway.acPerfSystem</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for MG 3200 in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-05-13T11:52:35EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
47.142.106.106,MG 3200

SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,1440
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
snmpOutPkts,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,6391,Valid
sysDescr,2005-05-13T11:52:32EST,.iso.org.dod.internet.mgmt.mib-
2.system,Product: Mediant 2000;SW Version: 4.60D.007.002,Valid
snmpInBadVersions,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInBadCommunityNames,2005-05-
13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInTotalReqVars,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,7376,Valid
```

```
snmpOutTraps,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,1140,Valid
snmpInBadCommunityUses,2005-05-
13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
snmpInPkts,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,5252,Valid
snmpInTotalSetVars,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,82,Valid
snmpInASNParseErrs,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
tcpOutSegs,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.tcp,21,Valid
tcpInSegs,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.tcp,26,Valid
udpOutDatagrams,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.udp,54145,Valid
udpInDatagrams,2005-05-13T11:52:33EST,.iso.org.dod.internet.mgmt.mib-
2.udp,901,Valid
snmpSilentDrops,2005-05-13T11:52:34EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
acPerfCpMessageSendSuccesses,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,0,Valid
acPerfCpMessagesFromUntrustedSources,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,0,Valid
acPerfCpMessageRetransmissions,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,292674,Valid
acPerfCpMessageSendErrors,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,0,Valid
acPerfCpMessageMaxRetransmissionsExceeded,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,41810,Valid
acPerfCpMessageReceiveSuccesses,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,0,Valid
acPerfCpNumDupsForCompletedTransactions,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,0,Valid
acPerfCpMessageReceiveErrors,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,0,Valid
```

```
acPerfCpNumDupsForOutstandingTransactions,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,0,Valid
acPerfCpProtocolSyntaxErrors,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfCp,0,Valid
acPerfRtpSimplexInSessionsCurrent,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpReceiverOctets,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpSimplexOutSessionsTotal,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpRcvrLostPackets,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpSimplexOutSessionsCurrent,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpSenderPackets,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpFailedDueToLackOfResources,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpDuplexSessionsTotal,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpSenderOctets,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpSimplexInSessionsTotal,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpDuplexSessionsCurrent,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfRtpReceiverPackets,2005-05-
13T11:52:34EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfRtp,0,Valid
acPerfSystemPacketEndpoints,2005-05-
13T11:52:35EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfSystem,300,Valid
```

```
acPerfSystemPacketEndpointsInUse,2005-05-
13T11:52:35EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerfor
mances.acPerfMediaGateway.acPerfSystem,0,Valid
SingleValues=End

Entity=End

System=End

PMFile=End
```

GUI/CLUI Documentation for MG 3200

Reference the LTRT-72704: Media Gateway MG3200 H.248 User's Manual for information about launching the MG 3200 configuration GUI.GUI Launching and User procedures

Related documents

Other customer documents related to the MG 3200 are:

- LTRT73804, MG 3200 H.248 SIP Fast Track Installation Guide
- LTRT72904, MG 3200 Configuration Guide

Media Gateway 9000 (MG9000)

This section contains IEMS Northbound log samples and device documentation references for the MG9000.

MG 9000 Fault Interface

Fault documentation for MG 9000 :

- NN10074-911 MG9000 Fault Management
- NN10409-500 ATM/IP Solution-level Fault Management

Fault Mapping for MG 9000

The following criteria can be used for looking up information on specific faults for MG 9000.

Fault Correlation for MG 9000

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MG 9000	logname and number	logname and number	logname and number	logname and number	NN10074-911 MG9000 Fault Management

Northbound Fault Formats for MG 9000

SCC2

The following is an example of a MG 9000 log in SCC2 format:

```
* 37 SWLN302 4259 TBL  MG9K NorLineFault
        Location: Port.frame0.shelf1.slot5.WL32.port21
        Notification Id: 330712652810
        State: UnAcknowledged
        Category: processingError
        Cause: Underlying Resource Unavailable
              NorLineFault - Line Protection Fault
        Component Id: Port.frame0.shelf1.slot5.WL32.port21
        specificProblem: NorLineFault - Line Protection Fault
        Description: Line Protection HighVoltageError      : 0,1,5,21 [suspect b
        ad LineCard]
```

NTSTD

The following is an example of a MG 9000 log in NTSTD format:

```
RTPU07BU   * SWLN302 Jan23 17:37:31 4259 TBL  MG9K NorLineFault
        Location: Port.frame0.shelf1.slot5.WL32.port21
        Notification Id: 330712652810
        State: UnAcknowledged
        Category: processingError
        Cause: Underlying Resource Unavailable
              NorLineFault - Line Protection Fault
        Component Id: Port.frame0.shelf1.slot5.WL32.port21
        specificProblem: NorLineFault - Line Protection Fault
```

```
        Description: Line Protection HighVoltageError      : 0,1,5,21 [suspect b
        ad LineCard]
```

SNMP

The following is an example of a MG 9000 log in SNMP format:

```
system.sysUpTime.0 => 17:59:11
snmpTrapOID.0 => nnExtAlarmClearalarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.49.45.50.51.44.49.48.58.52.58.50.46.54.44.41817
alarmActiveDateAndTime => 2004-1-23,10:4:2.6,
alarmActiveDescription => Underlying Resource Unavailable
        NorLineFault - Line Protection Fault

nnExtAlarmActiveEventType => 3
nnExtAlarmActiveProbableCause => 56
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SWLN302
nnExtAlarmActiveResourceDescription => IEMS=CC07;Port.frame0.shelf1.slot5.WL32.port21
nnExtAlarmActiveSequenceNumber => 7240
```

Syslog

The following is an example of a MG 9000 log in Syslog format:

```
Feb 23 12:40:26 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=4323~~ SWLN302 NONE TBL
MG9K NorLineFault^M        Location: Port.frame0.shelf1.slot5.WL32.port21^M
Notification Id: 330712652810^M        State: Cleared^M        Category:
processingError^M        Cause: Underlying Resource Unavailable^M
NorLineFault - Line Protection Fault^M        Component Id:
Port.frame0.shelf1.slot5.WL32.port21^M        specificProblem: NorLineFault - Line
Protection Fault^M       Description: Line Protection HighVoltageError     : 0,1,5,21
[suspect b^M        ad LineCard]
```

Performance

OM and PM Documentation references for MG 9000

- NN10140-711 MG9000 Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for MG 9000 in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2005-01-18T15:45:34EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity Type="MG9K Mgr">
<EntityId>172.31.125.226</EntityId>
<SubEntity>
<SubEntityId>172.31.125.226</SubEntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoOMECANIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoOMECANnumResrceReq</Label>
<Label>nnMegacoOMECANnumResrceReqFail</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoOMDSPIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoOMDSPnumCMRmodemReq</Label>
<Label>nnMegacoOMDSPnumCMRmodemReqFail</Label>
<Label>nnMegacoOMDSPnumToneGenReq</Label>
<Label>nnMegacoOMDSPnumToneGenReqFail</Label>
<Label>nnMegacoOMDSPnumToneRcvrReq</Label>
<Label>nnMegacoOMDSPnumToneRcvrReqFail</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoQoSIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoQoSIntervalBadCalls</Label>
<Label>nnMegacoQoSIntervalCalls</Label>
<Label>nnMegacoQoSIntervalJitter</Label>
<Label>nnMegacoQoSIntervalLatency</Label>
<Label>nnMegacoQoSIntervalPktLossPct</Label>
<Label>nnMegacoQoSIntervalPktsLost</Label>
<Label>nnMegacoQoSIntervalPktsRecvd</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

```
<RowValue>
<Value>Frame008.Shelf1.Slot12.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnIpsecOmIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnIpsecConfigInterfaceId</Label>
<Label>nnIpsecConfigSecLinkId</Label>
<Label>nnIpsecOmIntervalPacketsDiscardedIn</Label>
<Label>nnIpsecOmIntervalPacketsDiscardedOut</Label>
<Label>nnIpsecOmIntervalPacketsRx</Label>
<Label>nnIpsecOmIntervalPacketsTx</Label>
</Labels>
```

```
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
```

```
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnPmOvldRscIntervTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
```

```
<Label>nnPmOvldRscIntervCbvMsgRAvg</Label>
<Label>nnPmOvldRscIntervCbvMsgRPeak</Label>
<Label>nnPmOvldRscIntervConQDelAvg</Label>
<Label>nnPmOvldRscIntervConQDelPeak</Label>
<Label>nnPmOvldRscIntervCpuUtilAvg</Label>
<Label>nnPmOvldRscIntervCpuUtilPeak</Label>
<Label>nnPmOvldRscIntervPduRateAvg</Label>
<Label>nnPmOvldRscIntervPduRatePeak</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>514</Value>
</RowValue>
<RowValue>
<Value>552</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
</RowOfValues>
```

```
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>494</Value>
</RowValue>
<RowValue>
<Value>498</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>435</Value>
</RowValue>
<RowValue>
<Value>449</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>451</Value>
```

```
</RowValue>
<RowValue>
<Value>476</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>8</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>545</Value>
</RowValue>
<RowValue>
<Value>567</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>591</Value>
</RowValue>
<RowValue>
<Value>649</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>9</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>428</Value>
</RowValue>
<RowValue>
<Value>483</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>27</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>554</Value>
</RowValue>
<RowValue>
<Value>995</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>25</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnBwShelfIntervalSloaBandwResrvdTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnBwShelfIntervalSloaBandwReserved</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1</Value>
</RowValue>
<RowValue>
<Value>897</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>sonetPathIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>sonetPathIntervalCVs</Label>
<Label>sonetPathIntervalESs</Label>
<Label>sonetPathIntervalSESs</Label>
```

```
<Label>sonetPathIntervalUASs</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
```

```
<TableId>nnBwAbiIntervalBandwResrvdEntry</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnBwAbiIntervalBandwReserved</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>6000</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>7000</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>6612</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>7000</Value>
</RowValue>
</RowOfValues>
```

```
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnPmUtilOmIntervTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnPmUtilIntervChanAvg</Label>
<Label>nnPmUtilIntervChanPeak</Label>
<Label>nnPmUtilIntervCpuAvg</Label>
<Label>nnPmUtilIntervCpuPeak</Label>
<Label>nnPmUtilIntervFlashAvg</Label>
<Label>nnPmUtilIntervFlashPeak</Label>
<Label>nnPmUtilIntervRamAvg</Label>
<Label>nnPmUtilIntervRamPeak</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
```

```
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>5</Value>
```

```
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>17</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot15</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>19</Value>
</RowValue>
<RowValue>
<Value>19</Value>
```

```
</RowValue>
<RowValue>
<Value>36</Value>
</RowValue>
<RowValue>
<Value>36</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot14</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>36</Value>
</RowValue>
<RowValue>
<Value>36</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

```
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>24</Value>
</RowValue>
<RowValue>
<Value>24</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>24</Value>
</RowValue>
<RowValue>
<Value>24</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>47</Value>
</RowValue>
```

```
<RowValue>
<Value>47</Value>
</RowValue>
<RowValue>
<Value>37</Value>
</RowValue>
<RowValue>
<Value>37</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>10</Value>
</RowValue>
<RowValue>
<Value>23</Value>
</RowValue>
<RowValue>
<Value>23</Value>
</RowValue>
<RowValue>
<Value>38</Value>
</RowValue>
<RowValue>
<Value>38</Value>
</RowValue>
```

```
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnRelMsgSctpAssocOmIntervTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnRelMsgSctpAscIntervAbort</Label>
<Label>nnRelMsgSctpAscIntervClosed</Label>
<Label>nnRelMsgSctpAscIntervCongCleared</Label>
<Label>nnRelMsgSctpAscIntervCongCount</Label>
<Label>nnRelMsgSctpAscIntervDiscPacks</Label>
<Label>nnRelMsgSctpAscIntervInPacks</Label>
<Label>nnRelMsgSctpAscIntervOutPacks</Label>
<Label>nnRelMsgSctpAscIntervRetranPacks</Label>
<Label>nnRelMsgSctpAscIntervT1expires</Label>
<Label>nnRelMsgSctpAscIntervT2expires</Label>
<Label>nnRelMsgSctpAscIntervT3expires</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>467</Value>
</RowValue>
<RowValue>
<Value>487</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>465</Value>
</RowValue>
<RowValue>
<Value>485</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>761</Value>
</RowValue>
<RowValue>
<Value>697</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>792</Value>
</RowValue>
<RowValue>
<Value>726</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>sonetLineIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>sonetLineIntervalCVs</Label>
<Label>sonetLineIntervalESs</Label>
<Label>sonetLineIntervalSESs</Label>
<Label>sonetLineIntervalUASs</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoOMCESIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoOMCESnumChnlAllocInter</Label>
<Label>nnMegacoOMCESnumChnlAllocInterFail</Label>
<Label>nnMegacoOMCESnumChnlAllocIntra</Label>
<Label>nnMegacoOMCESnumChnlAllocIntraFail</Label>
</Labels>
<RowOfValues>

```
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnBwAbiCurrentBandwResrvdTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnBwAbiCapacityBandwReserved</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>

```
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>sonetSectionIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>sonetSectionIntervalCVs</Label>
<Label>sonetSectionIntervalESs</Label>
<Label>sonetSectionIntervalSEFSs</Label>
<Label>sonetSectionIntervalSESs</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
```

<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnClkSyncRefTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnClkSyncRefId</Label>
<Label>nnClkSyncRefLossOfFrameCount</Label>

```
<Label>nnClkSyncRefLossOfSignalCount</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnBwShelfCurrentSloaBandwResrvdTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnBwShelfCapacitySloaBandwReserved</Label>
</Labels>
```

```
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1</Value>
</RowValue>
<RowValue>
<Value>48960</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>norCarrSonetMediumIntervalTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnorCarrSonetMedIntervalLBC</Label>
<Label>norCarrSonetMedIntervalOpt</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
<RowValue>
<Value>106</Value>
</RowValue>
<RowValue>
<Value>99</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>103</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
```

```
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnPmOvldConnDenyIntervTable</TableId>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnPmOvldConnDenyIntervCount</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot17</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot13</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>apsChanStatusTable</TableId>
```

```
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>apsChanSignalDegrades</Label>
<Label>apsChanSignalFailures</Label>
<Label>apsChanSwitchovers</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot11.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot10.Port1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="15">
<TableId>nnMegacoOMMedGwyIntervalTable</TableId>
```

```
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<Labels>
<Label>Source</Label>
<Label>nnMegacoOMMedGwyAvrgInMsgRate</Label>
<Label>nnMegacoOMMedGwyAvrgOutMsgRate</Label>
<Label>nnMegacoOMMedGwyMaxInMsgRate</Label>
<Label>nnMegacoOMMedGwyMaxOutMsgRate</Label>
<Label>nnMegacoOMMedGwyNumInMessages</Label>
<Label>nnMegacoOMMedGwyNumInOctets</Label>
<Label>nnMegacoOMMedGwyNumOutMessages</Label>
<Label>nnMegacoOMMedGwyNumOutOctets</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot4.Port1</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>438</Value>
</RowValue>
<RowValue>
<Value>25752</Value>
</RowValue>
<RowValue>
<Value>438</Value>
</RowValue>
<RowValue>
```

```
<Value>36018</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot16.Port1</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>440</Value>
</RowValue>
<RowValue>
<Value>25867</Value>
</RowValue>
<RowValue>
<Value>440</Value>
</RowValue>
<RowValue>
<Value>33229</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Frame008.Shelf1.Slot12.Port1</Value>
</RowValue>
<RowValue>
<Value>53</Value>
```

```
</RowValue>
<RowValue>
<Value>53</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>805</Value>
</RowValue>
<RowValue>
<Value>50834</Value>
</RowValue>
<RowValue>
<Value>805</Value>
</RowValue>
<RowValue>
<Value>52001</Value>
</RowValue>
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="15">
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>snmpInvalidMsgs</MeasureId>
<MeasureSuppId1>Miscellaneous</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>Miscellaneous</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>Miscellaneous</MeasureSuppId1>
<Value>124921</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnPmSnmpIntervReqPeak</MeasureId>
<MeasureSuppId1>nnPmSnmpOmIntervTable</MeasureSuppId1>
<Value>40</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnPmSnmpIntervReqAvg</MeasureId>
<MeasureSuppId1>nnPmSnmpOmIntervTable</MeasureSuppId1>
<Value>126</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnPmSnmpIntervNotifPeak</MeasureId>
<MeasureSuppId1>nnPmSnmpOmIntervTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnPmSnmpIntervNotifAvg</MeasureId>
<MeasureSuppId1>nnPmSnmpOmIntervTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
```

```
<MeasureId>nnClkSyncSignalId</MeasureId>
<MeasureSuppId1>nnClkSyncSignalTable</MeasureSuppId1>
<Value>5</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnClkSyncSignalLossOfSignalCount</MeasureId>
<MeasureSuppId1>nnClkSyncSignalTable</MeasureSuppId1>
<Value>3</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnClkSyncSignalLossOfFrameCount</MeasureId>
<MeasureSuppId1>nnClkSyncSignalTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwBandwUtilIntervalInCellRate</MeasureId>
<MeasureSuppId1>nnBwIntervalBandwUtilTable</MeasureSuppId1>
<Value>878</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwBandwUtilIntervalOutCellRate</MeasureId>
<MeasureSuppId1>nnBwIntervalBandwUtilTable</MeasureSuppId1>
<Value>936</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwBandwUtilIntervalInDslCellRate</MeasureId>
<MeasureSuppId1>nnBwIntervalBandwUtilTable</MeasureSuppId1>
<Value>0</Value>
```

```
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwBandwUtilIntervalOutDslCellRate</MeasureId>
<MeasureSuppId1>nnBwIntervalBandwUtilTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalTotal</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalCbr</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalRtVbr</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalNrtVbr</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
```

```
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalUbr</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalUbrPlus</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-18T15:45:00EST</CaptureTime>
<MeasureId>nnBwQueueFillIntervalControl</MeasureId>
<MeasureSuppId1>nnBwIntervalQueueFillTable</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</SubEntity>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for MG 9000 in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-22T15:37:33EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
10.32.128.11,MG9K Mgr
```

```
SubEntity=Begin
SubEntityId
10.32.128.11

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnPmUtilOmIntervTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label,Label,Label,Label,Label,Label,Label,Label
Source,nnPmUtilIntervChanAvg,nnPmUtilIntervChanPeak,nnPmUtilIntervCpuAvg,nnPmUtilInt
ervCpuPeak,nnPmUtilIntervFlashAvg,nnPmUtilIntervFlashPeak,nnPmUtilIntervRamAvg,nnPmU
tilIntervRamPeak
Value,Value,Value,Value,Value,Value,Value,Value,Value
Frame011.Shelf0.Slot13,0,0,12,13,47,47,74,74
Frame011.Shelf0.Slot12,4,4,15,16,47,47,73,73
Frame011.Shelf1.Slot13,10,10,22,24,24,24,75,75
Frame011.Shelf1.Slot12,0,0,15,16,24,24,77,77
Frame011.Shelf2.Slot13,10,10,14,15,24,24,76,76
Frame011.Shelf2.Slot12,0,0,12,12,24,24,77,77
Frame013.Shelf0.Slot13,0,0,19,22,25,25,79,80
Frame013.Shelf0.Slot12,12,12,21,24,25,25,78,78
Frame011.Shelf3.Slot13,0,0,10,10,24,24,76,76
Frame011.Shelf3.Slot12,6,6,12,13,45,45,75,75
Frame013.Shelf1.Slot13,0,0,18,19,25,25,79,79
Frame013.Shelf1.Slot12,6,6,31,34,25,25,79,79
Frame010.Shelf0.Slot19,10,10,21,21,51,51,52,52
Frame010.Shelf0.Slot18,0,0,14,16,52,52,52,52
Frame010.Shelf0.Slot17,0,0,5,6,18,18,35,35
Frame010.Shelf0.Slot16,0,0,5,5,22,22,35,35
Frame010.Shelf0.Slot15,0,0,4,4,19,19,35,35
Frame010.Shelf0.Slot14,0,0,5,6,18,18,35,35
Frame013.Shelf2.Slot13,5,5,16,17,25,25,75,75
Frame010.Shelf0.Slot13,1,1,8,9,24,24,68,68
Frame013.Shelf2.Slot12,0,0,15,16,25,25,75,75
Frame010.Shelf0.Slot12,0,0,8,11,47,47,68,68
Frame010.Shelf0.Slot11,0,0,58,59,44,44,73,73
Frame010.Shelf0.Slot10,200,229,70,80,38,38,73,73
Frame013.Shelf3.Slot13,3,3,19,21,25,25,73,73
Frame010.Shelf1.Slot13,5,5,13,15,48,48,77,77
```

```
Frame013.Shelf3.Slot12,0,0,14,16,24,24,74,74
Frame010.Shelf1.Slot12,0,0,10,10,25,25,78,78
Frame010.Shelf2.Slot13,2,2,11,12,25,25,77,77
Frame010.Shelf2.Slot12,0,0,11,13,25,25,78,78
Frame012.Shelf0.Slot13,6,6,18,21,48,48,77,77
Frame010.Shelf3.Slot13,3,3,12,14,25,25,77,77
Frame012.Shelf0.Slot12,0,0,13,14,25,25,78,78
Frame010.Shelf3.Slot12,0,0,10,11,25,25,78,78
Frame012.Shelf1.Slot13,7,7,18,20,25,25,76,76
Frame012.Shelf1.Slot12,0,0,14,15,25,25,77,77
Frame012.Shelf2.Slot13,5,5,22,24,25,25,76,76
Frame012.Shelf2.Slot12,0,0,16,17,25,25,77,77
Frame010.Shelf0.Slot9,0,0,44,44,18,18,53,53
Frame010.Shelf0.Slot8,29,29,86,88,18,18,53,53
Frame010.Shelf0.Slot5,7,7,24,26,51,51,52,52
Frame010.Shelf0.Slot4,0,0,14,15,51,51,52,52
Frame010.Shelf0.Slot3,13,13,23,26,51,51,52,52
Frame012.Shelf3.Slot13,9,9,23,25,25,25,76,76
Frame010.Shelf0.Slot2,0,0,14,14,51,51,52,52
Frame012.Shelf3.Slot12,0,0,18,19,25,25,77,77
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnBwAbiCurrentBandwResrvdTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label
Source,nnBwAbiCapacityBandwReserved
Value,Value
Frame010.Shelf0.Slot5,0
Frame010.Shelf0.Slot4,0
Frame010.Shelf0.Slot3,0
Frame010.Shelf0.Slot2,0
Frame010.Shelf0.Slot19,0
Frame010.Shelf0.Slot18,0
Frame010.Shelf0.Slot9,0
Frame010.Shelf0.Slot8,0
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnMegacoOMDSPIntervalTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label,Label,Label,Label,Label,Label
Source,nnMegacoOMDSPnumCMRmodemReq,nnMegacoOMDSPnumCMRmodemReqFail,nnMegacoOMDSPnumToneGenReq,nnMegacoOMDSPnumToneGenReqFail,nnMegacoOMDSPnumToneRcvrReq,nnMegacoOMDSPnumToneRcvrReqFail
Value,Value,Value,Value,Value,Value,Value
Frame011.Shelf0.Slot13,0,0,69,0,46,0
Frame011.Shelf0.Slot12,0,0,69,0,46,0
Frame011.Shelf1.Slot13,0,0,69,0,93,0
Frame011.Shelf1.Slot12,0,0,69,0,93,0
Frame011.Shelf2.Slot13,0,0,12,0,33,0
Frame011.Shelf2.Slot12,0,0,12,0,33,0
Frame013.Shelf0.Slot13,0,0,22,0,51,0
Frame013.Shelf0.Slot12,0,0,22,0,51,0
Frame011.Shelf3.Slot13,0,0,10,0,24,0
Frame011.Shelf3.Slot12,0,0,10,0,24,0
Frame013.Shelf1.Slot13,0,0,175,0,0,0
Frame013.Shelf1.Slot12,0,0,175,0,0,0
Frame010.Shelf0.Slot19,0,0,0,0,0,0
Frame010.Shelf0.Slot18,0,0,0,0,0,0
Frame013.Shelf2.Slot13,0,0,11,0,28,0
Frame010.Shelf0.Slot13,0,0,9,0,0,0
Frame013.Shelf2.Slot12,0,0,11,0,28,0
Frame010.Shelf0.Slot12,0,0,9,0,0,0
Frame013.Shelf3.Slot13,0,0,3,0,9,0
Frame010.Shelf1.Slot13,0,0,8,0,18,0
Frame013.Shelf3.Slot12,0,0,3,0,9,0
Frame010.Shelf1.Slot12,0,0,8,0,18,0
Frame010.Shelf2.Slot13,0,0,3,0,9,0
Frame010.Shelf2.Slot12,0,0,3,0,9,0
Frame012.Shelf0.Slot13,0,0,39,0,57,0
Frame010.Shelf3.Slot13,0,0,4,0,9,0
Frame012.Shelf0.Slot12,0,0,39,0,57,0
Frame010.Shelf3.Slot12,0,0,4,0,9,0
Frame012.Shelf1.Slot13,0,0,25,0,35,0
```

```
Frame012.Shelf1.Slot12,0,0,25,0,35,0
Frame012.Shelf2.Slot13,0,0,50,0,88,0
Frame012.Shelf2.Slot12,0,0,50,0,88,0
Frame010.Shelf0.Slot9,0,0,0,0,0,0
Frame010.Shelf0.Slot8,0,0,0,0,0,0
Frame010.Shelf0.Slot5,0,0,0,0,0,0
Frame010.Shelf0.Slot4,0,0,0,0,0,0
Frame010.Shelf0.Slot3,0,0,0,0,0,0
Frame010.Shelf0.Slot2,0,0,0,0,0,0
Frame012.Shelf3.Slot13,0,0,62,0,91,0
Frame012.Shelf3.Slot12,0,0,62,0,91,0
Table=End



Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnMegacoOMCESIntervalTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label,Label,Label,Label
Source,nnMegacoOMCESnumChnlAllocInter,nnMegacoOMCESnumChnlAllocInterFail,nnMegacoOMC
ESnumChnlAllocIntra,nnMegacoOMCESnumChnlAllocIntraFail
Value,Value,Value,Value,Value
Frame011.Shelf0.Slot13,53,0,46,0
Frame011.Shelf0.Slot12,53,0,46,0
Frame011.Shelf1.Slot13,120,0,50,0
Frame011.Shelf1.Slot12,120,0,50,0
Frame011.Shelf2.Slot13,48,0,18,0
Frame011.Shelf2.Slot12,48,0,18,0
Frame013.Shelf0.Slot13,66,0,36,0
Frame013.Shelf0.Slot12,66,0,36,0
Frame011.Shelf3.Slot13,30,0,12,0
Frame011.Shelf3.Slot12,30,0,12,0
Frame013.Shelf1.Slot13,135,0,64,0
Frame013.Shelf1.Slot12,135,0,64,0
Frame010.Shelf0.Slot19,149,0,168,0
Frame010.Shelf0.Slot18,149,0,168,0
Frame013.Shelf2.Slot13,33,0,13,0
Frame010.Shelf0.Slot13,0,0,0,0
Frame013.Shelf2.Slot12,33,0,13,0
Frame010.Shelf0.Slot12,0,0,0,0
```

```
Frame010.Shelf0.Slot11,3152,0,1216,0
Frame010.Shelf0.Slot10,3152,0,1216,0
Frame013.Shelf3.Slot13,24,0,1,0
Frame010.Shelf1.Slot13,12,0,24,0
Frame013.Shelf3.Slot12,24,0,1,0
Frame010.Shelf1.Slot12,12,0,24,0
Frame010.Shelf2.Slot13,12,0,3,0
Frame010.Shelf2.Slot12,12,0,3,0
Frame012.Shelf0.Slot13,26,0,74,0
Frame010.Shelf3.Slot13,15,0,3,0
Frame012.Shelf0.Slot12,26,0,74,0
Frame010.Shelf3.Slot12,15,0,3,0
Frame012.Shelf1.Slot13,66,0,24,0
Frame012.Shelf1.Slot12,66,0,24,0
Frame012.Shelf2.Slot13,177,0,7,0
Frame012.Shelf2.Slot12,177,0,7,0
Frame010.Shelf0.Slot9,1563,0,416,0
Frame010.Shelf0.Slot8,1563,0,416,0
Frame010.Shelf0.Slot5,288,0,86,0
Frame010.Shelf0.Slot4,288,0,86,0
Frame010.Shelf0.Slot3,238,0,120,0
Frame010.Shelf0.Slot2,238,0,120,0
Frame012.Shelf3.Slot13,130,0,53,0
Frame012.Shelf3.Slot12,130,0,53,0
Table=End



Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnIpsecOmIntervalTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label,Label,Label,Label,Label,Label
Source,nnIpsecConfigInterfaceId,nnIpsecConfigSecLinkId,nnIpsecOmIntervalPacketsDiscarded
dedIn,nnIpsecOmIntervalPacketsDiscardedOut,nnIpsecOmIntervalPacketsRx,nnIpsecOmInte
rvalPacketsTx
Value,Value,Value,Value,Value,Value,Value
Frame011.Shelf0.Slot13,1,1,0,0,0,0
Frame011.Shelf0.Slot12,1,1,0,0,1684,1795
Frame011.Shelf1.Slot13,1,1,0,0,2710,2884
Frame011.Shelf1.Slot12,1,1,0,0,0,0
```

```
Frame011.Shelf2.Slot13,1,1,0,0,1056,1119
Frame011.Shelf2.Slot12,1,1,0,0,0,0
Frame013.Shelf0.Slot13,1,1,0,0,0,0
Frame013.Shelf0.Slot12,1,1,0,0,1483,1585
Frame011.Shelf3.Slot13,1,1,0,0,0,0
Frame011.Shelf3.Slot12,1,1,0,0,885,936
Frame013.Shelf1.Slot13,1,1,0,0,0,0
Frame013.Shelf1.Slot12,1,1,0,0,4264,4469
Frame010.Shelf0.Slot19,1,1,0,0,7454,5419
Frame010.Shelf0.Slot18,1,1,0,0,0,1514
Frame013.Shelf2.Slot13,1,1,0,0,997,1046
Frame010.Shelf0.Slot13,1,1,0,0,210,210
Frame013.Shelf2.Slot12,1,1,0,0,0,0
Frame010.Shelf0.Slot12,1,1,0,0,0,0
Frame010.Shelf0.Slot11,1,1,0,0,0,0
Frame010.Shelf0.Slot10,1,1,0,0,362,381
Frame013.Shelf3.Slot13,1,1,0,0,501,521
Frame010.Shelf1.Slot13,1,1,0,0,717,756
Frame013.Shelf3.Slot12,1,1,0,0,0,0
Frame010.Shelf1.Slot12,1,1,0,0,0,0
Frame010.Shelf2.Slot13,1,1,0,0,442,460
Frame010.Shelf2.Slot12,1,1,0,0,0,0
Frame012.Shelf0.Slot13,1,1,0,0,1541,1640
Frame010.Shelf3.Slot13,1,1,0,0,480,501
Frame012.Shelf0.Slot12,1,1,0,0,0,0
Frame010.Shelf3.Slot12,1,1,0,0,0,0
Frame012.Shelf1.Slot13,1,1,0,0,1502,1599
Frame012.Shelf1.Slot12,1,1,0,0,0,0
Frame012.Shelf2.Slot13,1,1,0,0,2840,3028
Frame012.Shelf2.Slot12,1,1,0,0,0,0
Frame010.Shelf0.Slot9,1,1,0,0,0,8370
Frame010.Shelf0.Slot8,1,1,0,0,39696,24384
Frame010.Shelf0.Slot5,1,1,0,0,8884,5222
Frame010.Shelf0.Slot4,1,1,0,0,0,2451
Frame010.Shelf0.Slot3,1,1,0,0,8626,5080
Frame010.Shelf0.Slot2,1,1,0,0,0,2014
Frame012.Shelf3.Slot13,1,1,0,0,2689,2851
Frame012.Shelf3.Slot12,1,1,0,0,0,0
```

```
Table=End



Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

nnPmOvldRscIntervTable,Snapshot,5,2005-03-22T15:35:00EST

Label,Label,Label,Label,Label,Label,Label,Label,Label

Source,nnPmOvldRscIntervCbvMsgRAvg,nnPmOvldRscIntervCbvMsgRPeak,nnPmOvldRscIntervCon
QDelAvg,nnPmOvldRscIntervConQDelPeak,nnPmOvldRscIntervCpuUtilAvg,nnPmOvldRscIntervCp
uUtilPeak,nnPmOvldRscIntervPduRateAvg,nnPmOvldRscIntervPduRatePeak

Value,Value,Value,Value,Value,Value,Value,Value,Value

Frame011.Shelf0.Slot13,34,47,25,30,1212,1289,1,1

Frame011.Shelf0.Slot12,34,47,94,129,1497,1587,7,9

Frame011.Shelf1.Slot13,61,82,231,417,2173,2393,12,15

Frame011.Shelf1.Slot12,61,82,38,44,1478,1592,1,2

Frame011.Shelf2.Slot13,19,32,188,299,1441,1529,5,7

Frame011.Shelf2.Slot12,21,32,22,30,1199,1246,1,1

Frame013.Shelf0.Slot13,38,60,38,62,1853,2218,1,2

Frame013.Shelf0.Slot12,35,52,408,585,2087,2393,8,9

Frame011.Shelf3.Slot13,13,21,17,28,1008,1045,1,1

Frame011.Shelf3.Slot12,13,21,88,221,1236,1296,4,5

Frame013.Shelf1.Slot13,63,70,25,27,1777,1896,1,1

Frame013.Shelf1.Slot12,61,72,361,415,3105,3368,17,19

Frame010.Shelf0.Slot19,104,119,593,737,2063,2139,37,40

Frame010.Shelf0.Slot18,107,120,39,42,1356,1618,24,27

Frame013.Shelf2.Slot13,11,22,198,319,1609,1727,4,7

Frame010.Shelf0.Slot13,0,0,0,0,762,857,1,4

Frame013.Shelf2.Slot12,11,22,24,39,1539,1627,1,2

Frame010.Shelf0.Slot12,0,0,0,0,823,1123,1,2

Frame010.Shelf0.Slot11,0,0,1395,1567,5813,5904,216,247

Frame010.Shelf0.Slot10,1474,1526,809,900,7014,7904,249,279

Frame013.Shelf3.Slot13,6,13,33,59,1870,2108,3,4

Frame010.Shelf1.Slot13,8,14,118,232,1335,1496,3,4

Frame013.Shelf3.Slot12,6,12,10,23,1438,1589,1,2

Frame010.Shelf1.Slot12,9,14,12,20,1012,1039,1,2

Frame010.Shelf2.Slot13,5,12,15,33,1103,1181,2,3

Frame010.Shelf2.Slot12,5,12,9,24,1063,1260,1,2

Frame012.Shelf0.Slot13,33,52,433,1031,1752,2064,7,11

Frame010.Shelf3.Slot13,7,23,37,86,1209,1381,3,5
```

```
Frame012.Shelf0.Slot12,32,51,26,36,1260,1379,1,2
Frame010.Shelf3.Slot12,7,23,9,24,1017,1098,1,2
Frame012.Shelf1.Slot13,31,52,331,860,1818,2017,6,9
Frame012.Shelf1.Slot12,23,31,32,46,1376,1538,1,1
Frame012.Shelf2.Slot13,59,63,90,144,2245,2355,13,14
Frame012.Shelf2.Slot12,60,65,32,38,1630,1676,1,1
Frame010.Shelf0.Slot9,641,651,104,118,4376,4415,137,139
Frame010.Shelf0.Slot8,650,685,16644,21690,8520,8733,204,207
Frame010.Shelf0.Slot5,122,141,430,581,2401,2579,44,47
Frame010.Shelf0.Slot4,123,141,47,55,1399,1529,29,31
Frame010.Shelf0.Slot3,112,120,510,611,2329,2624,42,44
Frame010.Shelf0.Slot2,125,138,46,50,1365,1411,29,31
Frame012.Shelf3.Slot13,58,68,362,862,2264,2477,13,15
Frame012.Shelf3.Slot12,57,68,36,46,1805,1916,1,2
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnRelMsgSctpAssocOmIntervTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label
Source,nnRelMsgSctpAscIntervAbort,nnRelMsgSctpAscIntervClosed,nnRelMsgSctpAscIntervC
ongCleared,nnRelMsgSctpAscIntervCongCount,nnRelMsgSctpAscIntervDiscPacks,nnRelMsgSct
pAscIntervInPacks,nnRelMsgSctpAscIntervOutPacks,nnRelMsgSctpAscIntervRetranPacks,nnR
elMsgSctpAscIntervT1expires,nnRelMsgSctpAscIntervT2expires,nnRelMsgSctpAscIntervT3ex
pires
Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value
Frame010.Shelf0.Slot5,0,0,0,0,0,4387,1816,0,0,0,0
Frame010.Shelf0.Slot4,0,0,0,0,0,1535,2398,0,0,0,0
Frame010.Shelf0.Slot3,0,0,0,0,0,4036,1838,0,0,0,0
Frame010.Shelf0.Slot2,0,0,0,0,0,1748,1736,0,0,0,0
Frame010.Shelf0.Slot19,0,0,0,0,0,3650,2193,0,0,0,0
Frame010.Shelf0.Slot18,0,0,0,0,0,755,1346,0,0,0,0
Frame010.Shelf0.Slot9,0,0,0,0,0,5141,8278,0,0,0,0
Frame010.Shelf0.Slot8,0,0,0,0,0,21327,8865,0,0,0,0
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
```

```
nnBwAbiIntervalBandwResrvdEntry,Snapshot,5,2005-03-22T15:35:00EST
Label,Label
Source,nnBwAbiIntervalBandwReserved
Value,Value
Frame010.Shelf0.Slot5,6000
Frame010.Shelf0.Slot4,10078
Frame010.Shelf0.Slot3,6000
Frame010.Shelf0.Slot2,14900
Frame010.Shelf0.Slot19,10993
Frame010.Shelf0.Slot18,7000
Frame010.Shelf0.Slot9,22013
Frame010.Shelf0.Slot8,6000
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnPmOvldConnDenyIntervTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label
Source,nnPmOvldConnDenyIntervCount
Value,Value
Frame011.Shelf0.Slot13,0
Frame011.Shelf0.Slot12,0
Frame011.Shelf1.Slot13,0
Frame011.Shelf1.Slot12,0
Frame011.Shelf2.Slot13,0
Frame011.Shelf2.Slot12,0
Frame013.Shelf0.Slot13,0
Frame013.Shelf0.Slot12,0
Frame011.Shelf3.Slot13,0
Frame011.Shelf3.Slot12,0
Frame013.Shelf1.Slot13,0
Frame013.Shelf1.Slot12,0
Frame010.Shelf0.Slot19,0
Frame010.Shelf0.Slot18,0
Frame013.Shelf2.Slot13,0
Frame010.Shelf0.Slot13,0
Frame013.Shelf2.Slot12,0
```

```
Frame010.Shelf0.Slot12,0
Frame010.Shelf0.Slot11,0
Frame010.Shelf0.Slot10,0
Frame013.Shelf3.Slot13,0
Frame010.Shelf1.Slot13,0
Frame013.Shelf3.Slot12,0
Frame010.Shelf1.Slot12,0
Frame010.Shelf2.Slot13,0
Frame010.Shelf2.Slot12,0
Frame012.Shelf0.Slot13,0
Frame010.Shelf3.Slot13,0
Frame012.Shelf0.Slot12,0
Frame010.Shelf3.Slot12,0
Frame012.Shelf1.Slot13,0
Frame012.Shelf1.Slot12,0
Frame012.Shelf2.Slot13,0
Frame012.Shelf2.Slot12,0
Frame010.Shelf0.Slot9,0
Frame010.Shelf0.Slot8,0
Frame010.Shelf0.Slot5,0
Frame010.Shelf0.Slot4,0
Frame010.Shelf0.Slot3,0
Frame010.Shelf0.Slot2,0
Frame012.Shelf3.Slot13,0
Frame012.Shelf3.Slot12,0
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnMegacoOMECANIntervalTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label,Label
Source,nnMegacoOMECANnumResrceReq,nnMegacoOMECANnumResrceReqFail
Value,Value,Value
Frame011.Shelf0.Slot13,99,0
Frame011.Shelf0.Slot12,99,0
Frame011.Shelf1.Slot13,171,0
Frame011.Shelf1.Slot12,171,0
```

```
Frame011.Shelf2.Slot13,66,0
Frame011.Shelf2.Slot12,66,0
Frame013.Shelf0.Slot13,102,0
Frame013.Shelf0.Slot12,102,0
Frame011.Shelf3.Slot13,45,0
Frame011.Shelf3.Slot12,45,0
Frame013.Shelf1.Slot13,199,0
Frame013.Shelf1.Slot12,199,0
Frame010.Shelf0.Slot19,317,0
Frame010.Shelf0.Slot18,317,0
Frame013.Shelf2.Slot13,49,0
Frame010.Shelf0.Slot13,0,0
Frame013.Shelf2.Slot12,49,0
Frame010.Shelf0.Slot12,0,0
Frame013.Shelf3.Slot13,25,0
Frame010.Shelf1.Slot13,36,0
Frame013.Shelf3.Slot12,25,0
Frame010.Shelf1.Slot12,36,0
Frame010.Shelf2.Slot13,15,0
Frame010.Shelf2.Slot12,15,0
Frame012.Shelf0.Slot13,98,0
Frame010.Shelf3.Slot13,18,0
Frame012.Shelf0.Slot12,98,0
Frame010.Shelf3.Slot12,18,0
Frame012.Shelf1.Slot13,90,0
Frame012.Shelf1.Slot12,90,0
Frame012.Shelf2.Slot13,184,0
Frame012.Shelf2.Slot12,184,0
Frame010.Shelf0.Slot9,1979,0
Frame010.Shelf0.Slot8,1979,0
Frame010.Shelf0.Slot5,374,0
Frame010.Shelf0.Slot4,374,0
Frame010.Shelf0.Slot3,358,0
Frame010.Shelf0.Slot2,358,0
Frame012.Shelf3.Slot13,179,0
Frame012.Shelf3.Slot12,179,0
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnBwShelfCurrentSloaBandwResrvdTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label
Source,nnBwShelfCapacitySloaBandwReserved
Value,Value
Frame012.Shelf2,27680
Frame012.Shelf1,27680
Frame012.Shelf0,27680
Frame011.Shelf3,27680
Frame011.Shelf2,27680
Frame011.Shelf1,27680
Frame010.Shelf3,27680
Frame011.Shelf0,27680
Frame010.Shelf2,27680
Frame010.Shelf1,27680
Frame010.Shelf0,27680
Frame013.Shelf3,27680
Frame013.Shelf2,27680
Frame013.Shelf1,27680
Frame013.Shelf0,27680
Frame012.Shelf3,27680
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
nnBwShelfIntervalSloaBandwResrvdTable,Snapshot,5,2005-03-22T15:35:00EST
Label,Label
Source,nnBwShelfIntervalSloaBandwReserved
Value,Value
Frame012.Shelf2,3351
Frame012.Shelf1,5950
Frame012.Shelf0,3864
Frame011.Shelf3,5232
Frame011.Shelf2,7182
Frame011.Shelf1,5745
```

```
Frame010.Shelf3,2872

Frame011.Shelf0,2770

Frame010.Shelf2,1846

Frame010.Shelf1,4035

Frame010.Shelf0,684

Frame013.Shelf3,2394

Frame013.Shelf2,4651

Frame013.Shelf1,4035

Frame013.Shelf0,8310

Frame012.Shelf3,6771

Table=End



SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

nnBwBandwUtilIntervalInCellRate,2005-03-
22T15:35:00EST,nnBwIntervalBandwUtilTable,66409,Valid

nnBwBandwUtilIntervalOutCellRate,2005-03-
22T15:35:00EST,nnBwIntervalBandwUtilTable,66339,Valid

nnBwBandwUtilIntervalInDslCellRate,2005-03-
22T15:35:00EST,nnBwIntervalBandwUtilTable,0,Valid

nnBwBandwUtilIntervalOutDslCellRate,2005-03-
22T15:35:00EST,nnBwIntervalBandwUtilTable,0,Valid

nnBwQueueFillIntervalTotal,2005-03-22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid

nnBwQueueFillIntervalCbr,2005-03-22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid

nnBwQueueFillIntervalRtVbr,2005-03-22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid

nnBwQueueFillIntervalNrtVbr,2005-03-
22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid

nnBwQueueFillIntervalUbr,2005-03-22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid

nnBwQueueFillIntervalUbrPlus,2005-03-
22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid

nnBwQueueFillIntervalControl,2005-03-
22T15:35:00EST,nnBwIntervalQueueFillTable,0,Valid

SingleValues=End


SubEntity=End


Entity=End
```

```
System=End


PMFile=End
```

GUI/CLUI Documentation for MG 9000

GUI Launching and User procedures

- NN10096-511 MG9000 Configuration Management

Related documents

- NN10409-500 ATM/IP Solution-level Configuration Management

MultiService Switch 7400, 15000, 20000

This section contains IEMS Northbound log samples and device documentation references for the MSS 7400, 15000, 20000.

MSS 7400, 15000, 20000 Fault Interface

Fault documentation for MSS 7400, 15000, 20000 :

- NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
- NN10600-715 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management
- NN10600-520 - Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting

Fault Mapping for MSS 7400, 15000, 20000

The following criteria can be used for looking up information on specific faults for MS 7400, 15000, 20000.

Fault Correlation for MS 7400, 15000, 20000

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MS 7400, 15000, 20000	logname and number	logname and number	logname and number	logname and number	NN10600-715 - Nortel Networks Multiservice Switch 7400/ 15000/20000 ATM Fault and Performance Management

Northbound Fault Formats for MSS 7400, 15000, 20000

SCC2

The following is an example of a MSS 7400, 15000, 20000 log in SCC2 format:

```
19 PPEM302 8013 TBL
       time: 2004 01 27 14 19 53
       event: message
       compId: EM PP04 LP 8
       severity: indeterminate
       faultcode: 70560000
       alarmType: other
       commentData: 1-7-200
       0000
       1;DBG_WARNING:R:21-L:18 stats timeout.
```

NTSTD

The following is an example of a MSS 7400, 15000, 20000 log in NTSTD format:

```
RTPU07BU     PPEM302 Jan27 19:19:53 7467 TBL
        time: 2004 01 27 14 19 53
        event: message
        compId: EM PP04 LP 8
        severity: indeterminate
```

```
faultcode: 70560000
alarmType: other
commentData: 1-7-200
0000
1;DBG_WARNING:R:21-L:18 stats timeout.
```

SNMP

The following is an example of a MSS 7400, 15000, 20000 log in SNMP format:

```
sysUpTime. => 0:28:39
snmpTrapOID. => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.
20.50.48
.48.52.45.54.45.50.52.44.51.58.53.51.58.52.49.46.48.44.5248
alarmActiveDateAndTime => 2004-6-24,3:53:41.0
alarmActiveDescription => Far end has raised a Line Remote Failure Indication
alarm (rxRfiAlarm).
Check the operational attributes of the far-end.
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => 70115203
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m3.us.nortel.com-MDM-
Mgr;EM MANTEO
LP 3 SONET 2
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1375
```

Syslog

The following is an example of a MSS 7400, 15000, 20000 log in Syslog format:

```
Feb 27 13:19:58 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=2202~~ PPEM302 NONE TBL ^M
time: 2004 01 27 14 19 53^M       event: message^M       compId: EM PP04 LP 8^M
severity: indeterminate^M       faultcode: 70560000^M       alarmType: other^M
commentData: 1-7-200^M       0000 ^M       1;DBG_WARNING:R:21-L:18 stats timeout.
```

Performance

OM and PM Documentation references for MSS 7400, 15000, 20000

- NN10600-710 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Configuration Management
- NN10600-582 - Nortel Networks Multiservice Switch 7400/15000/20000 IP VPN Configuration Management
- NN10600-520 - Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting

Northbound OM/PM Formats

Performance measurements for MSS 7400, 15000, 20000 are available only from the MDM directly. *Please refer to Section " Northbound OM/PM Formats" on page 715.*

XML

The following is an example of Performance data for MSS 7400, 15000, 20000 in XML format:

Note: *The IEMS northbound performance interface does not support this device..*

CSV

The following is an example of Performance data for MSS 7400, 15000, 20000 in CSV format:

Note: *The IEMS northbound performance interface does not support this device..*

GUI/CLUI Documentation for MSS 7400, 15000, 20000

GUI Launching and User procedures

Please refer to "GUI/CLUI Documentation for MDM" on page 725.

- NN10600-030 - Nortel Networks Multiservice Switch 7400/15000/20000 Overview
- NN10600-050 - Nortel Networks Multiservice Switch 7400/15000/20000 Commands Reference
- NN10600-053 - Nortel Networks Multiservice Switch 7400/15000/20000 Commands Job Aid

Related documents

Please refer to "Related documents" on page 726.

- NN10600-001 - Nortel Networks Multiservice Switch 7400/15000/20000 Using the Documentation
- NN10600-002 - Nortel Networks Multiservice Switch 7400/15000/20000 Using Task-based Documentation Job Aid
- NN10600-005 - Nortel Networks Multiservice Switch 7400/15000/20000 Terminology
- NN10600-030 - Nortel Networks Multiservice Switch 7400/15000/20000 Overview
- NN10600-270 - Nortel Networks Multiservice Switch 7400/15000/20000 Software Installation
- NN10600-271 - Nortel Networks Multiservice Switch 7400/15000/20000 Network Management Connectivity
- NN10600-272 - Nortel Networks Multiservice Switch 7400/15000/20000 Upgrading Software
- NN10600-300 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: SNMP
- NN10600-405 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Server
- NN10600-410 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Call Redirection Server
- NN10600-415 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Hunt Group Server
- NN10600-420 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Trunking
- NN10600-425 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Dynamic Packet Routing System
- NN10600-435 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Path-Oriented Routing System
- NN10600-440 - Nortel Networks Multiservice Switch 7400 Operations: Frame Relay Managed Cut-through Switching
- NN10600-445 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Multiprotocol Label Switching
- NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference

- NN10600-510 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Trace System
- NN10600-520 - Nortel Networks Multiservice Switch 7400/15000/20000 Fault and Performance Management: Troubleshooting
- NN10600-550 - Nortel Networks Multiservice Switch 7400/15000/20000 Common Configuration Procedures
- NN10600-551 - Nortel Networks Multiservice Switch 7400/15000/20000 FP Configuration Reference
- NN10600-560 - Nortel Networks Multiservice Switch 7400/15000/20000 Accounting
- NN10600-561 - Nortel Networks Multiservice Switch 7400/15000/20000 Data Management
- NN10600-581 - Nortel Networks Multiservice Switch 7400/15000/20000 IP VPN Technology Fundamentals
- NN10600-582 - Nortel Networks Multiservice Switch 7400/15000/20000 IP VPN Configuration Management
- NN10600-700 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Technology Fundamentals
- NN10600-702 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Routing and Signaling Fundamentals
- NN10600-705 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Traffic Management Fundamentals
- NN10600-706 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Traffic Shaping and Policing Fundamentals
- NN10600-707 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Queuing and Scheduling Fundamentals
- NN10600-708 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM CAC and Bandwidth Fundamentals
- NN10600-710 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Configuration Management
- NN10600-715 - Nortel Networks Multiservice Switch 7400/15000/20000 ATM Fault and Performance Management
- NN10600-720 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: AAL1 Circuit Emulation
- NN10600-730 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Inverse Multiplexing for ATMe
- NN10600-780 - Nortel Networks Media Gateway 7480/15000 Technology Fundamentals

- NN10600-781 - Nortel Networks Media Gateway 7480/15000 Non-switched Service Configuration Management
- NN10600-782 - Nortel Networks Media Gateway 7480/15000 Switched Service Configuration Management
- NN10600-800 - Nortel Networks Multiservice Switch 7400/15000/20000 IP Technology Fundamentals
- NN10600-801 - Nortel Networks Multiservice Switch 7400/15000/20000 IP Configuration Management
- NN10600-580 - Nortel Networks Multiservice Switch 7400/15000/20000 Operations: Ethernet Service
- NN10600-120 - Nortel Networks Multiservice Switch 15000/20000 Hardware Description
- NN10600-130 - Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade
- NN10600-170 - Nortel Networks Multiservice Switch 7400 Hardware Description
- NN10600-130 - Nortel Networks Multiservice Switch 15000/20000 Hardware Installation, Maintenance, and Upgrade
- NN10600-172 - Nortel Networks Multiservice Switch 7400 FP Cabling Reference
- NN10600-745 - Nortel Networks Multiservice Switch 7400 Operations: MPANL
- NN10600-750 - Nortel Networks Multiservice Switch 7400 Operations: Voice Transport
- NN10600-755 - Nortel Networks Multiservice Switch 7400 Operations: Voice Networking
- NN10600-765 - Nortel Networks Multiservice Switch 7400 Operations: Remote Server Agent
- NN10600-605 - Passport MDM Network Security: Operations
- NN10600-606 - Passport MDM Network Security: User Access Configuration
- NN10600-607 - Passport MDM Network Security: Secure Communications Configuration
- 241-6001-309 - Multiservice Data Manager Management Data Provider
- 241-6001-806 - Multiservice Data Manager Management Data Provider Data Formats Reference for DPN
- NN10600-060 - Nortel Networks Multiservice Switch 7400/15000/20000 Components Reference

MS2000 Series Node

This section contains IEMS Northbound log samples and device documentation references for the MS2000 Series Node.

MS2000 Series Node Fault Interface

Fault documentation for MS2000 Series Node :

- NN10328-911 Media Server 2000 Series Fault Management

Fault Mapping for MS2000 Series Node

The following criteria can be used for looking up information on specific faults for MS2000 Series Node.

Fault Correlation for MS2000 Series Node

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MS2000 Series Node	logname and number	logname and number	logname and number	logname and number	NN10328-911 MS2000 Series Fault Management

Northbound Fault Formats for MS2000 Series Node

SCC2

The following is an example of a MS2000 Series Node log in SCC2 format:

34 AMS 501 0035 INFO MS2000 INFO
Location: 47.142.134.127
State: Cleared
Time: 1086806097963

**34 AMS 501 0036 FLT MS2000 FAULT
Location: 47.142.134.127
State: Raised
Category: processingError
Cause: 71
Time: 1086806097964
Component Id: System#0
Trap Name: 6
Description: Network element admin state change alarm. Gateway is locked

NTSTD

The following is an example of a MS2000 Series Node log in NTSTD format:

```
Nortel-JH **  AMS501 JUN10 09:21:12 5707 FLT  MS2000 INFO
        Location: 47.142.134.127
        State: Raised
        Category: processingError
        Cause: 71
        Time: 1086873672171
        Component Id: System#0
        Trap Name: 6
        Description: Network element admin state change alarm. Gateway is shutti
        ngDown


Nortel-JH AMS501 JUN10 09:21:12 5708 INFO MS2000 INFO
        Location: 47.142.134.127
        State: Cleared
        Time: 1086873672172


Nortel-JH **  AMS501 JUN10 09:21:12 5709 FLT  MS2000 INFO
        Location: 47.142.134.127
        State: Raised
        Category: processingError
        Cause: 71
        Time: 1086873672174
```

```
        Component Id: System#0
        Trap Name: 6
        Description: Network element admin state change alarm. Gateway is locked


Nortel-JH AMS501 JUN10 09:21:25 5710 INFO MS2000 INFO
        Location: 47.142.134.127
        State: Cleared
        Time: 1086873685240
```

SNMP

The following is an example of a MS2000 Series Node log in SNMP format:

```
sysUpTime. => 1 day, 19:19:22
snmpTrapOID. => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=Unknown Device;
nnExtAlarmMessageDateAndTime => 2004-6-9,3:4:5.0
nnExtAlarmMessageDocumentationPointer => IEMS601
nnExtAlarmMessageInfo =>   04 IEMS601 3350 INFO

        Location: 10.5.0.17

        Event: .1.3.6.1.6.3.1.1.5.3

        Varbind0: .1.3.6.1.2.1.2.2.1.1.0: 132

        Varbind1: .1.3.6.1.2.1.2.2.1.7.0: 1

        Varbind2: .1.3.6.1.2.1.2.2.1.8.0: 2



sysUpTime. => 1 day, 19:19:25
snmpTrapOID. => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=Unknown Device;
nnExtAlarmMessageDateAndTime => 2004-6-9,3:4:7.9
```

```
nnExtAlarmMessageDocumentationPointer => IEMS601
nnExtAlarmMessageInfo =>   04 IEMS601 3351 INFO

        Location: 10.5.0.17

        Event: .1.3.6.1.6.3.1.1.5.4

        Varbind0: .1.3.6.1.2.1.2.2.1.1.0: 132

        Varbind1: .1.3.6.1.2.1.2.2.1.7.0: 1

        Varbind2: .1.3.6.1.2.1.2.2.1.8.0: 1
```

Syslog

The following is an example of a MS2000 Series Node log in Syslog format:

```
Jun  9 14:31:41 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=9643~~  AMS501 MAJOR FLT
MS2000 FAULT        Location: 47.142.134.127        State: Raised        Category:
processingError     Cause: 71     Time: 1086805901311     Component Id: System#0
Trap Name: 6       Description: Network element admin state change alarm. Gateway is
shuttingDown


Jun  9 14:31:41 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=9644~~  AMS501 NONE INFO
MS2000 FAULT        Location: 47.142.134.127        State: Cleared        Time:
1086805901313


Jun  9 14:31:41 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=9645~~  AMS501 MAJOR FLT
MS2000 FAULT        Location: 47.142.134.127        State: Raised        Category:
processingError     Cause: 71     Time: 1086805901314     Component Id: System#0
Trap Name: 6       Description: Network element admin state change alarm. Gateway is
locked
Jun  9 14:31:41 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=9646~~ IEMS601 NONE


Resetting board
```

Performance

OM and PM Documentation references for MS2000 Series Node

- NN10331-711 - Media Server 2000 Series Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided.

XML

The following is an example of Performance data for MS2000 Series Node in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T17:40:01EST</FileCreationTime>
- <System>
<SystemId>NortelNetworks/IEMS</SystemId>
- <Entity Type="MS2000">
<EntityId>47.142.92.107</EntityId>
- <SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
- <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Product: IPMedia 3000;SW Version: 4.30.380.12</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>4858</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
```

```
<CaptureTime>2004-06-23T17:35:01EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>9089</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>15</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>4844</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:02EST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
```

```
<Value>4</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>tcpOutSegs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.tcp</MeasureSuppId1>
<Value>3531</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>tcpInSegs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.tcp</MeasureSuppId1>
<Value>4359</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>udpOutDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.udp</MeasureSuppId1>
<Value>438175</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2004-06-23T17:35:03EST</CaptureTime>
<MeasureId>udpInDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.udp</MeasureSuppId1>
<Value>107768</Value>
<Reliability>Valid</Reliability>
</SingleValue>
```

```
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for MS2000 Series Node in CSV format:

```
PMFile=Begin
PM,commonFormat.xsd,2004-06-23T17:25:50EST
System=Begin
NortelNetworks/IEMS
Entity=Begin
47.142.92.104,MS2000
SingleValues=Begin
Snapshot,5
snmpOutPkts,2004-06-23T17:24:09EST,.iso.org.dod.internet.mgmt.mib-2.snmp,368,Valid
snmpInBadVersions,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInBadCommunityNames,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInTotalReqVars,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,959,Valid
snmpOutTraps,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,13,Valid
snmpInBadCommunityUses,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
snmpInPkts,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-2.snmp,356,Valid
snmpInTotalSetVars,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,12,Valid
snmpInASNParseErrs,2004-06-23T17:24:10EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
tcpOutSegs,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-2.tcp,195,Valid
tcpInSegs,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-2.tcp,13675,Valid
udpOutDatagrams,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-
2.udp,27702,Valid
udpInDatagrams,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-
2.udp,14797,Valid
snmpSilentDrops,2004-06-23T17:24:11EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid
acPerfCpMessageSendErrors,2004-06-
23T17:24:11EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid
```

```
acPerfCpNumDupsForCompletedTransactions,2004-06-
23T17:24:11EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageMaxRetransmissionsExceeded,2004-06-
23T17:24:11EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageReceiveErrors,2004-06-
23T17:24:12EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageRetransmissions,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,18,Valid

acPerfCpNumDupsForOutstandingTransactions,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessagesFromUntrustedSources,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpProtocolSyntaxErrors,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfRtpRcvrLostPackets,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfRtp,0,Valid

acPerfRtpFailedDueToLackOfResources,2004-06-
23T17:24:13EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfRtp,0,Valid

acPerfIvrPlayCollectRequests,2004-06-
23T17:24:14EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayRequests,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,88,Valid

acPerfBctRequests,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfBct,0,Valid

acPerfIvrPlayCollectFailedDueToLackOfResources,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlaySegmentFailedDueToProvMismatch,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,9,Valid

acPerfIvrContDigitCollectRequests,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayFailedDueToLackOfResources,2004-06-
23T17:24:15EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayCollectFailedDueToProvMismatch,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid
```

```
acPerfIvrContDigitCollectFailedDueToLackOfResources,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfBctFailedDueToLackOfResources,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfBct,0,Valid

acPerfConfRequests,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,11,Valid

acPerfConfPlays,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,36,Valid

acPerfConfAddFailedDueToLackOfResources,2004-06-
23T17:24:16EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfConfFailedDueToLackOfResources,2004-06-
23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfTtFailedDueToLackOfResources,2004-06-
23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfTt,0,Valid

acPerfTtRequests,2004-06-
23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfTt,0,Valid

acPerfSystemPacketEndpointsInUse,2004-06-
23T17:24:17EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfSystem,0,Valid

SingleValues=End

Entity=End

System=End

PMFile=End
```

GUI/CLUI Documentation for MS2000 Series Node

GUI Launching and User procedures

- NN10323-111 MS2000 Series Basics

Related documents

- NN10340-511 MS2000 Series Configuration Management
- NN10337-611 MS2000 Series Security and Administration

Session Server Manager

This section contains IEMS Northbound log samples and device documentation references for the Session Server Manager.

Session Server Manager Fault Interface

This section will provide references to customer documentation for Fault, Performance, Topology, GUI/CLUI, and Security for Session Server Manager.

Fault documentation for Session Server Manager:

- NN10332-911 - Session Server Fault Management

Fault Mapping for Session Server Manager

The following criteria can be used for looking up information on specific faults for Session Server Manager.

Fault Correlation for Session Server Manager

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Session Server Manager	logname and number	logname and number	logname and number	logname and number	NN10332-911 Session Server Fault Management

Northbound Fault Formats for Session Server Manager

SCC2

The following is an example of a Session Server Manager log in SCC2 format:

```
**57 SIPM302 2080 FLT  SIPM Fault
      Location: 47.142.123.43
      Notification Id: 111
      State: Raised
      Category: communications
      Cause: applicationSubsystemFailure
      Time: Apr 12 21:57:55 2004
      Component Id: NCGL=RTPF-SIP0;Unit=0;
      Specific Problem: SIP Gateway Application State Not Synced With Mate
      Description: SIP Gateway Application Mtc Out Of Sync
```

NTSTD

The following is an example of a Session Server Manager log in NTSTD format:

```
znc0s0jh  ** SIPM302 APR12 21:57:55 2080 FLT  SIPM Fault
        Location: 47.142.123.43
        Notification Id: 111
```

```
State: Raised
Category: communications
Cause: applicationSubsystemFailure
Time: Apr 12 21:57:55 2004
Component Id: NCGL=RTPF-SIP0;Unit=0;
Specific Problem: SIP Gateway Application State Not Synced With Mate
Description: SIP Gateway Application Mtc Out Of Sync
```

SNMP

The following is an example of a Session Server Manager log in SNMP format:

```
sysUpTime.0 => 2:34:22
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.
20.50.48.48.52.45.52.45.49.50.44.57.58.53.55.58.53.53.46.48.44.3070
alarmActiveDateAndTime => 2004-4-12,9:57:55.0
alarmActiveDescription => SIP Gateway Application Mtc Out Of Sync
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 2
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SIPM302
nnExtAlarmActiveResourceDescription => IEMS=47.142.123.48-SP2000-Unit-
0;NCGL=RTPFSIP0;
Unit=0;
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 35
```

Syslog

The following is an example of a Session Server Manager log in Syslog format:

```
Apr 12 22:13:03 znc0s0jh IEMS: V2_~I=~H=znc0s0jh~A=IEMS~S=6213~~ SIPM302 MAJOR FLT
SIPM Fault^M      Locationon:47.142.123.43^M      Notification Id: 111^M      State:
Raised^M     Category: communications^M     Cause: applicationSubsystemFailure^M
Time: Apr 12 21:57:55 2004^M        Component Id: NCGL=RTPF-SIP0;Unit=0;^M  Specific
Problem: SIP Gateway Application State Not Synced With Mate^M       Description: SIP
Gateway Application Mtc Out Of Sync
```

Performance

OM and PM Documentation references for Session Server Manager

- NN10342-711 Session Server Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance for Session Server Manager in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonPerfRecord_V2.0.xsd"
MeasurementCategory="PM">
<FileCreationTime>2006-01-16T01:28:11PST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity>
<EntityId>47.142.92.225-47.142.92.230-SS-Unit-0</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry</TableId>
<CaptureTime>2006-01-16T01:28:09PST</CaptureTime>
<Labels>
<Label>laNames</Label>
<Label>laLoad</Label>
<Label>laConfig</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>Load-15</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Load-5</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>Load-1</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTable.hrStorageEntry</TableId>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
<Labels>
<Label>hrStorageIndex</Label>
<Label>hrStorageType</Label>
<Label>hrStorageAllocationUnits</Label>
<Label>hrStorageSize</Label>
<Label>hrStorageUsed</Label>
<Label>hrStorageAllocationFailures</Label>
</Labels>
<RowOfValues>
<RowValue>
```

```
<Value>9</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>129872</Value>
</RowValue>
<RowValue>
<Value>216</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>8</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>179024</Value>
</RowValue>
<RowValue>
<Value>343</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>7</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>259584</Value>
</RowValue>
<RowValue>
<Value>198685</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>129872</Value>
</RowValue>
<RowValue>
<Value>29952</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>31568</Value>
</RowValue>
<RowValue>
<Value>6701</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>129872</Value>
</RowValue>
```

```
<RowValue>
<Value>95674</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>103</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageOther</Value>
</RowValue>
<RowValue>
<Value>256</Value>
</RowValue>
<RowValue>
<Value>51218</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1026</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
```

```
<RowValue>
<Value>179024</Value>
</RowValue>
<RowValue>
<Value>327</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>102</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory</Value>
</RowValue>
<RowValue>
<Value>1024</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1025</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>12</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
```

```
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>129872</Value>
</RowValue>
<RowValue>
<Value>81</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>101</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageRam</Value>
</RowValue>
<RowValue>
<Value>1024</Value>
</RowValue>
<RowValue>
<Value>2097151</Value>
</RowValue>
<RowValue>
<Value>2097151</Value>
</RowValue>
<RowValue>
<Value>769</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
```

```
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>1024</Value>
</RowValue>
<RowValue>
<Value>101018</Value>
</RowValue>
<RowValue>
<Value>80797</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>11</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>2561536</Value>
</RowValue>
<RowValue>
<Value>12352</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
```

```
<Value>1</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>1024</Value>
</RowValue>
<RowValue>
<Value>62941</Value>
</RowValue>
<RowValue>
<Value>51218</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>10</Value>
</RowValue>
<RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
<RowValue>
<Value>4096</Value>
</RowValue>
<RowValue>
<Value>382464</Value>
</RowValue>
<RowValue>
<Value>56117</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
<SingleValue>
<CaptureTime>2006-01-16T01:28:01PST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Linux RTP7NGSS-0 2.4.22-ncgl-9.51.1.0 #1 Wed Dec 21 03:52:40 EST 2005
i686</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>6433</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>20058</Value>
<Reliability>Valid</Reliability>
```

```
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>31</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>6428</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:02PST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
```

```
<MeasureId>hrSystemDate</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>2006-1-16,4:44:25.0,-5:0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
<MeasureId>hrSystemUptime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>229179</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
<MeasureId>hrSystemProcesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>194</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2006-01-16T01:28:03PST</CaptureTime>
<MeasureId>snmpSilentDrops</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance for Session Server Manager in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonPerfRecord_V2.0.xsd,2006-01-12T02:12:02PST
```

```
System=Begin

SystemId

NortelNetworks/IEMS


Entity=Begin

EntityId

47.142.92.225-47.142.92.230-SS-Unit-0


Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.private.enterprises.ucdavis.laTable.laEntry,Snapshot,5,2006-
01-12T02:12:01PST

Label,Label,Label

laNames,laLoad,laConfig

Value,Value,Value

Load-15,0,12

Load-5,0,12

Load-1,0,12

Table=End



Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTable.hrStorageEntry,Snapshot,5,2006-01-12T02:11:57PST

Label,Label,Label,Label,Label,Label

hrStorageIndex,hrStorageType,hrStorageAllocationUnits,hrStorageSize,hrStorageUsed,hr
StorageAllocationFailures

Value,Value,Value,Value,Value,Value

9,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,179024,342,0

8,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,179024,342,0

7,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,259584,198668,0

6,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,129872,26027,0

5,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,31568,6701,0

4,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,129872,89138,0
```

```
103,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageOther,256,48363,0,1026

3,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,179024,322,0

102,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory,1024,0,0,1025

12,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,129872,90,0

101,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageRam,1024,2097151,1125972,769

2,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,1024,101018,80797,0

11,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,2561536,11651,0

1,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,1024,62941,48363,0

10,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,4096,382464,55288,0

Table=End



SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

sysDescr,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-2.system,Linux
RTP7NGSS-0 2.4.22-ncgl-cca_image_7.09.2.1 #1 Wed Jul 13 15:33:06 EDT 2005 i686,Valid

snmpOutPkts,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-2.snmp,1913,Valid

snmpInBadVersions,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInBadCommunityNames,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,1,Valid

snmpInTotalReqVars,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,7179,Valid

snmpOutTraps,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-2.snmp,92,Valid

snmpInBadCommunityUses,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInPkts,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-2.snmp,2034,Valid

snmpInTotalSetVars,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInASNParseErrs,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

hrSystemDate,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,2006-1-12,5:28:17.0,-5:0,Valid
```

```
hrSystemUptime,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,56466,Valid

hrSystemProcesses,2006-01-12T02:11:56PST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,178,Valid

snmpSilentDrops,2006-01-12T02:11:57PST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

SingleValues=End


Entity=End


System=End


PMFile=End
```

GUI/CLUI Documentation for Session Server Manager

GUI Launching and User procedures

- NN10333-111 Session Server Basics

Related documents

- NN10338-511 - Session Server Configuration Management
- NN10346-611 - Session Server Security and Administration

SAM21 Shelf Controller

This section contains IEMS Northbound log samples and device documentation references for the SAM21 Shelf Controller.

SAM21 Shelf Controller Fault Interface

Fault documentation for SAM21 Shelf Controller :

- NN10089-911 - SAM21 Shelf Controller Fault Management

Fault Mapping for SAM21 Shelf Controller

The following criteria can be used for looking up information on specific faults for SAM21 Shelf Controller.

Fault Correlation for SAM21 Shelf Controller

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
SAM21 Shelf Controller	logname and number	logname and number	logname and number	logname and number	NN10089-911 SAM21 Shelf Controller Fault Management

Northbound Fault Formats for SAM21 Shelf Controller

SCC2

The following is an example of a SAM21 Shelf Controller log in SCC2 format:

```
**37 SCU 350 0009 FLT  Alarm Raised
        Location: SAM21 1:CSAM01-01:sled 3
        Time:     Wed Jan 14 13:55:52 EST 2004
        Reason:   Temperature in Sled 3 is high
```

NTSTD

The following is an example of a SAM21 Shelf Controller log in NTSTD format:

```
COMPACT06BT  **  SCU350 Jan15 00:37:17 0009 FLT  Alarm Raised
        Location: SAM21 1:CSAM01-01:sled 3
        Time:     Wed Jan 14 13:55:52 EST 2004
        Reason:   Temperature in Sled 3 is high
```

SNMP

The following is an example of a SAM21 Shelf Controller log in SNMP format:

```
sysUpTime.0 => 9:14:20
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.49.44.54.58.52.49.58.49.52.46.48.44.8995
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => DeviceSpecificInfo=;Location: SAM21 1:CSAM01-01:sled 3
Time:     Wed Jan 14 13:57:48 EST 2004
```

```
Reason:   Temperature in Sled 3 is high
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SCU 350
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0kz.us.nortel.com-SAM21-Mgr;
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a SAM21 Shelf Controller log in Syslog format:

```
Feb 12 18:30:19 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7929~~  SCU350 MAJOR FLT
Alarm Raised^M       Location: SAM21 1:CSAM01-01:sled 3^M       Time:     Mon Jan 12
12:49:06 EST 2004^M        Reason:   Temperature in Sled 3 is high
```

Performance

OM and PM Documentation references for SAM21 Shelf Controller

- There are no OMs or PMs associated with this device for IP solutions, only for ATM solutions.
- NN10155-711 - SAM21 Shelf Controller Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided (for ATM solutions only).

CSV

The following is an example of Performance for SAM21 Shelf Controller in CSV format.

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-16T10:55:01EST


System=Begin
SystemId
NortelNetworks/IEMS


Entity=Begin
```

```
EntityId,Type

172.16.144.134,SAM21


SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

totalBytesRxed,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,14792,Valid

rxedTimeoutCount,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,0,Valid

bytesSentPerSec,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,24,Valid

cellDropCount,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,0,Valid

oversizedPDUCount,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,0,Valid

bytesRxedPerSec,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,24,Valid

totalBytesSent,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,16765,Valid

SingleValues=End


Entity=End


System=End
```

GUI/CLUI Documentation for SAM21 Shelf Controller

GUI Launching and User procedures

- NN10025-111 - SAM21 Shelf Controller Basics
- NN10089-911 - SAM21 Shelf Controller Fault Management
- NN10111-511 - SAM21 Shelf Controller Configuration Management
- NN10177-611 - SAM21 Shelf Controller Administration and Security

Related documents

Storage Manager (STORM)

This section contains IEMS Northbound log samples and device documentation references for the STORM.

STORM Fault Interface

Fault documentation for STORM :

- NN10024-111 - STORM Basics
- NN10088-911 - STORM Fault Management

Fault Mapping for STORM

The following criteria can be used for looking up information on specific faults for STORM.

Fault Correlation for STORM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
STORM	logname and number eg: STM 800	logname and number	logname and number	logname and number	NN10088-911 STORM Fault Management

Northbound Fault Formats for STORM

SCC2

The following is an example of a STORM log in SCC2 format:

Sample Clear:

```
 19 STM 801 0595 INFO
       Location: 47.166.56.10
       Notification Id: 13
       State: Cleared
       Time: Jan 24 19:19:49 2004
```

Sample Raise:

```
**19 STM 801 0596 FLT  STM Fault
       Location: 47.166.56.10
```

```
        Notification Id: 14
        State: Raised
        Category: qualityOfService
        Cause: thresholdCrossed
        Time: Jan 24 19:19:49 2004
        Component Id: STORMIA=langley1
        Specific Problem:
        Description: Status: Alarm raised. Used memory percentage is 18.24. Majo
        r alarm threshold value is 6.00.
```

NTSTD

The following is an example of a STORM log in NTSTD format:

Sample Clear:

```
RTPU07BR      STM801 Jan25 00:19:49 0041 INFO
        Location: 47.166.56.10
        Notification Id: 13
        State: Cleared
        Time: Jan 24 19:19:49 2004
```

Sample Raise:

```
RTPU07BR  **  STM801 Jan25 00:19:49 0042 FLT  STM Fault
        Location: 47.166.56.10
        Notification Id: 14
        State: Raised
        Category: qualityOfService
        Cause: thresholdCrossed
        Time: Jan 24 19:19:49 2004
        Component Id: STORMIA=langley1
        Specific Problem:
        Description: Status: Alarm raised. Used memory percentage is 18.24. Majo
        r alarm threshold value is 6.00.
```

SNMP

The following is an example of a STORM log in SNMP format:

Sample Clear:

```
system.sysUpTime.0 => 8:01:55
snmpTrapOID.0 => nnExtAlarmClear
```

alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.52.44.55.58.49.57.58.52.57.46.48.44.312

alarmActiveDateAndTime => 2004-1-21,6:41:14.0,

alarmActiveDescription => DeviceSpecificInfo=;Status: Alarm cleared. A new alarm with higher severity will be raised.

nnExtAlarmActiveEventType => 2

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => STM 801

nnExtAlarmActiveResourceDescription => IEMS=zmdhh0jk.europe.nortel.com-STORM;STORMIA=langley1

nnExtAlarmActiveSequenceNumber => 24

Sample Raise:

system.sysUpTime.0 => 7:01:55

snmpTrapOID.0 => nnExtAlarmMajor

alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.52.44.55.58.49.57.58.52.57.46.48.44.329

alarmActiveDateAndTime => 2004-1-21,6:41:14.0,

alarmActiveDescription => Status: Alarm raised. Used memory percentage is 18.24. Major alarm threshold value is 6.00.

nnExtAlarmActiveEventType => 2

nnExtAlarmActiveProbableCause => 51

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => STM 801

nnExtAlarmActiveResourceDescription => IEMS=zmdhh0jk.europe.nortel.com-STORM;STORMIA=langley1

nnExtAlarmActiveManualClear => 2

nnExtAlarmActiveSequenceNumber => 25

Syslog

The following is an example of a STORM log in Syslog format:

Sample Clear:

```
Feb 24 19:19:43 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0618~~  STM801 NONE INFO
^M      Location: 47.166.56.10^M      Notification Id: 13^M      State: Cleared^M
Time: Jan 24 19:19:49 2004
```

Sample Raise:

```
Feb 24 19:19:43 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0619~~  STM801 MAJOR FLT
STM Fault^M       Location: 47.166.56.10^M       Notification Id: 14^M       State:
```

```
Raised^M      Category: qualityOfService^M      Cause: thresholdCrossed^M      Time:
Jan 24 19:19:49 2004^M       Component Id: STORMIA=langley1^M       Specific Problem:
^M      Description: Status: Alarm raised. Used memory percentage is 18.24. Majo^M
r alarm threshold value is 6.00.
```

Performance

OM and PM Documentation references for STORM

The SNMP based attributes that can be collected from the STORM device are documented in:

- NN10054-711 - STORM Performance Management Customer Document

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided.

XML

The following is an example of Performance data for STORM in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>

- <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">

<FileCreationTime>2005-03-15T15:35:04EST</FileCreationTime>

- <System>

<SystemId>NortelNetworks/IEMS</SystemId>

- <Entity Type="STORM">

<EntityId>47.166.56.10</EntityId>

- <Table MeasurementKind="Snapshot" IntervalDuration="5">

<TableId>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTable.hrStorageEntry</TableId>

<CaptureTime>2005-03-15T15:35:01EST</CaptureTime>

- <Labels>

<Label>hrStorageIndex</Label>

<Label>hrStorageType</Label>

<Label>hrStorageDescr</Label>

<Label>hrStorageAllocationUnits</Label>

<Label>hrStorageSize</Label>

<Label>hrStorageUsed</Label>

<Label>hrStorageAllocationFailures</Label>

</Labels>
```

- <RowOfValues>
- <RowValue>
<Value>14</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/5/cs</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>924496</Value>
</RowValue>
- <RowValue>
<Value>591998</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>13</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/4/mtc</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>

<Value>260944</Value>

</RowValue>

- <RowValue>

<Value>71434</Value>

</RowValue>

- <RowValue>

<Value>0</Value>

</RowValue>

</RowOfValues>

- <RowOfValues>

- <RowValue>

<Value>12</Value>

</RowValue>

- <RowValue>

<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>

</RowValue>

- <RowValue>

<Value>/nfsserv/3pc/4/cs</Value>

</RowValue>

- <RowValue>

<Value>4096</Value>

</RowValue>

- <RowValue>

<Value>924496</Value>

</RowValue>

- <RowValue>

<Value>505263</Value>

</RowValue>

- <RowValue>

<Value>0</Value>

</RowValue>

</RowOfValues>

- <RowOfValues>

- <RowValue>

<Value>11</Value>

</RowValue>

- <RowValue>

```
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/3/mtc</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>260944</Value>
</RowValue>
- <RowValue>
<Value>66727</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>10</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/3/cs</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>924496</Value>
</RowValue>
- <RowValue>
<Value>486565</Value>
</RowValue>
```

- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>103</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageOther</Value>
</RowValue>
- <RowValue>
<Value>Memory Buffers</Value>
</RowValue>
- <RowValue>
<Value>256</Value>
</RowValue>
- <RowValue>
<Value>53493</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
- <RowValue>
<Value>1026</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>102</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory</Value>
</RowValue>
- <RowValue>
<Value>Swap Space</Value>
</RowValue>

- <RowValue>
<Value>1024</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
- <RowValue>
<Value>1025</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>101</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageRam</Value>
</RowValue>
- <RowValue>
<Value>Real Memory</Value>
</RowValue>
- <RowValue>
<Value>1024</Value>
</RowValue>
- <RowValue>
<Value>514140</Value>
</RowValue>
- <RowValue>
<Value>381396</Value>
</RowValue>
- <RowValue>
<Value>769</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>

```
<Value>22</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/8/mtc</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>260944</Value>
</RowValue>
- <RowValue>
<Value>39840</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>21</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/8/cs</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>875344</Value>
</RowValue>
```

- <RowValue>
<Value>639076</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>9</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/2/mtc</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>260944</Value>
</RowValue>
- <RowValue>
<Value>41542</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>20</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>

- <RowValue>
<Value>/nfsserv/3pc/7/mtc</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>260944</Value>
</RowValue>
- <RowValue>
<Value>37878</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>8</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/2/cs</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>924496</Value>
</RowValue>
- <RowValue>
<Value>627594</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>

```
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>7</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/1/mtc</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>260944</Value>
</RowValue>
- <RowValue>
<Value>64177</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>6</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/1/cs</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
```

- <RowValue>
<Value>924496</Value>
</RowValue>
- <RowValue>
<Value>484559</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>5</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/0/mtc</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>260944</Value>
</RowValue>
- <RowValue>
<Value>41699</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>4</Value>
</RowValue>
- <RowValue>

<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>

</RowValue>

- <RowValue>

<Value>/nfsserv/3pc/0/cs</Value>

</RowValue>

- <RowValue>

<Value>4096</Value>

</RowValue>

- <RowValue>

<Value>924496</Value>

</RowValue>

- <RowValue>

<Value>667345</Value>

</RowValue>

- <RowValue>

<Value>0</Value>

</RowValue>

</RowOfValues>

- <RowOfValues>

- <RowValue>

<Value>3</Value>

</RowValue>

- <RowValue>

<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>

</RowValue>

- <RowValue>

<Value>/storm</Value>

</RowValue>

- <RowValue>

<Value>4096</Value>

</RowValue>

- <RowValue>

<Value>260944</Value>

</RowValue>

- <RowValue>

<Value>298</Value>

</RowValue>

- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>2</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/boot</Value>
</RowValue>
- <RowValue>
<Value>1024</Value>
</RowValue>
- <RowValue>
<Value>101018</Value>
</RowValue>
- <RowValue>
<Value>58993</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/</Value>
</RowValue>

- <RowValue>
<Value>1024</Value>
</RowValue>
- <RowValue>
<Value>59301</Value>
</RowValue>
- <RowValue>
<Value>53493</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>19</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/3pc/7/cs</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>875344</Value>
</RowValue>
- <RowValue>
<Value>551564</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>

<Value>18</Value>

</RowValue>

- <RowValue>

<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>

</RowValue>

- <RowValue>

<Value>/nfsserv/3pc/6/mtc</Value>

</RowValue>

- <RowValue>

<Value>4096</Value>

</RowValue>

- <RowValue>

<Value>260944</Value>

</RowValue>

- <RowValue>

<Value>41900</Value>

</RowValue>

- <RowValue>

<Value>0</Value>

</RowValue>

</RowOfValues>

- <RowOfValues>

- <RowValue>

<Value>17</Value>

</RowValue>

- <RowValue>

<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>

</RowValue>

- <RowValue>

<Value>/nfsserv/3pc/6/cs</Value>

</RowValue>

- <RowValue>

<Value>4096</Value>

</RowValue>

- <RowValue>

<Value>875344</Value>

</RowValue>

- <RowValue>
<Value>600004</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>16</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>
- <RowValue>
<Value>/nfsserv/usp</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>514896</Value>
</RowValue>
- <RowValue>
<Value>13871</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>15</Value>
</RowValue>
- <RowValue>
<Value>.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk</Value>
</RowValue>

- <RowValue>
<Value>/nfsserv/3pc/5/mtc</Value>
</RowValue>
- <RowValue>
<Value>4096</Value>
</RowValue>
- <RowValue>
<Value>260944</Value>
</RowValue>
- <RowValue>
<Value>37460</Value>
</RowValue>
- <RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
- <SingleValues MeasurementKind="**Snapshot**" IntervalDuration="**5**">
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>sysDescr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.system</MeasureSuppId1>
<Value>Linux langley40 2.4.19-xfs #1 SMP Fri Nov 7 11:18:05 EST 2003 i686</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpOutPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>106051</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInBadVersions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>

```
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInBadCommunityNames</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>7</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInTotalReqVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>559860</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpOutTraps</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>13442</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInBadCommunityUses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInPkts</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>97188</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
```

```
<MeasureId>snmpInTotalSetVars</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpInASNParseErrs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:00EST</CaptureTime>
<MeasureId>snmpSilentDrops</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.snmp</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:01EST</CaptureTime>
<MeasureId>hrSystemDate</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>2005-3-15,20:35:1.0,+0:0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:01EST</CaptureTime>
<MeasureId>hrSystemUptime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>1642231</Value>
<Reliability>Valid</Reliability>
</SingleValue>
- <SingleValue>
<CaptureTime>2005-03-15T15:35:01EST</CaptureTime>
<MeasureId>hrSystemProcesses</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.host.hrSystem</MeasureSuppId1>
<Value>80</Value>
```

```
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for STORM in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-15T15:10:04EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
47.166.56.10,STORM

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTable.hrStorageEntry,Snapshot,5,2005-03-15T15:10:01EST
Label,Label,Label,Label,Label,Label,Label
hrStorageIndex,hrStorageType,hrStorageDescr,hrStorageAllocationUnits,hrStorageSize,h
rStorageUsed,hrStorageAllocationFailures
Value,Value,Value,Value,Value,Value,Value
14,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/5/cs,4096,924496,591
998,0
13,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/4/mtc,4096,260944,71
427,0
12,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/4/cs,4096,924496,505
263,0
```

```
11,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/3/mtc,4096,260944,66
723,0

10,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/3/cs,4096,924496,486
565,0

103,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageOther,Memory Buffers,256,53462,0,1026

102,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageVirtualMemory,Swap Space,1024,0,0,1025

101,.iso.org.dod.internet.mgmt.mib-2.host.hrStorage.hrStorageTypes.hrStorageRam,Real
Memory,1024,514140,381096,769

22,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/8/mtc,4096,260944,39
834,0

21,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/8/cs,4096,875344,639
076,0

9,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/2/mtc,4096,260944,41
535,0

20,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/7/mtc,4096,260944,37
872,0

8,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/2/cs,4096,924496,627
594,0

7,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/1/mtc,4096,260944,64
173,0

6,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/1/cs,4096,924496,484
559,0

5,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/0/mtc,4096,260944,41
693,0

4,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/0/cs,4096,924496,667
345,0

3,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/storm,4096,260944,298,0

2,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/boot,1024,101018,58993,0

1,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/,1024,59301,53462,0

19,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/7/cs,4096,875344,551
564,0
```

```
18,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/6/mtc,4096,260944,41
895,0

17,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/6/cs,4096,875344,600
004,0

16,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/usp,4096,514896,13870,0

15,.iso.org.dod.internet.mgmt.mib-
2.host.hrStorage.hrStorageTypes.hrStorageFixedDisk,/nfsserv/3pc/5/mtc,4096,260944,37
451,0

Table=End



SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

sysDescr,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-2.system,Linux
langley40 2.4.19-xfs #1 SMP Fri Nov 7 11:18:05 EST 2003 i686,Valid

snmpOutPkts,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,105897,Valid

snmpInBadVersions,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInBadCommunityNames,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,7,Valid

snmpInTotalReqVars,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,559127,Valid

snmpOutTraps,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,13412,Valid

snmpInBadCommunityUses,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInPkts,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-2.snmp,97059,Valid

snmpInTotalSetVars,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInASNParseErrs,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpSilentDrops,2005-03-15T15:10:00EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

hrSystemDate,2005-03-15T15:10:01EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,2005-3-15,20:10:1.0,+0:0,Valid

hrSystemUptime,2005-03-15T15:10:01EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,1640731,Valid

hrSystemProcesses,2005-03-15T15:10:01EST,.iso.org.dod.internet.mgmt.mib-
2.host.hrSystem,79,Valid

SingleValues=End
```

```
Entity=End

System=End

PMFile=End
```

GUI/CLUI Documentation for STORM

GUI Launching and User procedures

- NN10024-111 - STORM Basics

Related documents

- NN10110-511 - STORM Configuration
- NN10054-711 - STORM Performance Management
- NN10176-611 - STORM Administration and Security

Universal Audio Server (UAS)

This section contains IEMS Northbound log samples and device documentation references for the UAS.

UAS Fault Interface

Fault documentation for UAS :

- NN10073-911 UAS Fault Management

Fault Mapping for UAS

The following criteria can be used for looking up information on specific faults for UAS.

Fault Correlation for UAS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
UAS	logname and number	logname and number	logname and number	logname and number	NN10073-911 UAS Fault Management

Northbound Fault Formats for UAS

SCC2

The following is an example of a UAS log in SCC2 format:

```
*C59 UAS 301 0723 TBL  UAS Fault
        Location: UAS12_Test
        NotificationID: 2109441
        State: Raise
        Category: Processing Error
        Cause: Software error
        Time: Jan 22 15:41:28 2004
        Component Id: UAS;UASUnit=MATTA-2;Software=Call_Engine_1
        Specific Problem: 12289
        Description: CallEngine test alarm critical number 1
```

NTSTD

The following is an example of a UAS log in NTSTD format:

```
COMPACT506BT ***  UAS301 Jan22 20:59:00 1149 TBL  UAS Fault
        Location: UAS12_Test
        NotificationID: 2109441
        State: Raise
        Category: Processing Error
        Cause: Software error
        Time: Jan 22 15:41:28 2004
        Component Id: UAS;UASUnit=MATTA-2;Software=Call_Engine_1
        Specific Problem: 12289
        Description: CallEngine test alarm critical number 1
```

SNMP

The following is an example of a UAS log in SNMP format:

```
sysUpTime.0 => 3:21:08
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.19.50.48.48.52.45.49.45.50.50.44.51.58.53.57.58.48.46.52.44.28556
alarmActiveDateAndTime => 2004-1-22,3:59:0.4,
alarmActiveDescription => DeviceSpecificInfo=Unavailable;Location: UAS12_Test
NotificationID: 2109441
State: Raise
Category: Processing Error
Cause: Software error
Time: Jan 22 15:41:28 2004
Component Id: UAS;UASUnit=MATTA-2;Software=Call_Engine_1
Specific Problem: 12289
Description: CallEngine test alarm critical number 1
```

Syslog

The following is an example of a UAS log in Syslog format:

```
Jan 22 15:59:00 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=3086~~ UAS301 CRIT TBL UAS
Fault^M Location: UAS12_Test^M NotificationID: 2109441^M State:
Raise^M Category: Processing Error^M Cause: Software error^M Time:
Jan 22 15:41:28 2004^M Component Id: UAS;UASUnit=MATTA-
2;Software=Call_Engine_1^M Specific Problem: 12289^M Description:
CallEngine test alarm critical number 1
```

Performance

OM and PM Documentation references for UAS

- NTP NN10139-711 UAS Performance

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided
each of the Northbound formats provided

XML

The following is an example of performance data for UAS in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">

<FileCreationTime>2005-01-13T14:15:01EST</FileCreationTime>

<System>

<SystemId>NortelNetworks/IEMS</SystemId>

<Entity Type="UAS">

<EntityId>47.142.89.82</EntityId>

<Table MeasurementKind="Snapshot" IntervalDuration="5">

<TableId>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasResourceMan
agerObjects.norUasRequestStatsTable.norUasRequestStatsEntry</TableId>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<Labels>

<Label>norUasResourceName</Label>

<Label>norUasRequestCount</Label>

<Label>norUasRequestsFailed</Label>

</Labels>

<RowOfValues>

<RowValue>

<Value>EndpointIdPool5</Value>

</RowValue>

<RowValue>

<Value>0</Value>

</RowValue>

<RowValue>

<Value>0</Value>

</RowValue>

</RowOfValues>

<RowOfValues>

<RowValue>

<Value>EndpointIdPool4</Value>

</RowValue>

<RowValue>

<Value>0</Value>

</RowValue>

<RowValue>
```

```
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>EndpointIdPool3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>EndpointIdPool2</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>EndpointIdPool1</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
```

```
<Value>EndpointIdPool0</Value>
</RowValue>
<RowValue>
<Value>103</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasMgcpMessageRetransmissionFailures</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>3771</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasAckfail</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasProterror</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasAudioSegmentFailed</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
```

```
<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasComperror</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasProtocolSyntaxErrors</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:01EST</CaptureTime>

<MeasureId>norUasNumberOfPlayRecordErrors</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasIVRS
erviceObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasConfLackOfResourceRejections</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasConf
ServiceObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasConfTotal</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasConf
ServiceObjects</MeasureSuppId1>
```

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasConfPlays</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasConf
ServiceObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:01EST</CaptureTime>

<MeasureId>norUasNumberOfPlayRecords</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasIVRS
erviceObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasRestart</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasConndeleted</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasProtocolMessageValidationErrors</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasUdpReceiveErrors</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall EngineObjects</MeasureSuppId1>

<Value>10</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasNumDupsForOutstandingTransactions</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall EngineObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasEndpointsInUse</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall EngineObjects</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasTimeout</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall EngineObjects</MeasureSuppId1>

<Value>1256</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>

<MeasureId>norUasNumDupsForCompletedTransactions</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall EngineObjects</MeasureSuppId1>

```
<Value>3</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasUdpSendErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasCallControlMessageSendFailures</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>1257</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasMgcpMessageRetransmissions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>3771</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2005-01-13T14:15:00EST</CaptureTime>
<MeasureId>norUasAudioSegmentPlayed</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasCall
EngineObjects</MeasureSuppId1>
<Value>134</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of performance data for UAS in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-17T16:30:01EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
47.142.89.82,UAS

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasResourceManagerO
bjects.norUasRequestStatsTable.norUasRequestStatsEntry,Snapshot,5,2005-03-
17T16:30:00EST
Label,Label,Label
norUasResourceName,norUasRequestCount,norUasRequestsFailed
Value,Value,Value
EndpointIdPool5,0,0
EndpointIdPool4,7,0
EndpointIdPool3,21,0
EndpointIdPool2,0,0
EndpointIdPool1,62,0
EndpointIdPool0,116,0
Table=End


SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
norUasUdpSendErrors,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasNumDupsForCompletedTransactions,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,15,Valid
norUasCallControlMessageSendFailures,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,1,Valid
norUasMgcpMessageRetransmissions,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,4,Valid
norUasAudioSegmentPlayed,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,134,Valid
norUasTimeout,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasRestart,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasConndeleted,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
```

```
norUasProtocolMessageValidationErrors,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasUdpReceiveErrors,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,2,Valid
norUasNumDupsForOutstandingTransactions,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasEndpointsInUse,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasMgcpMessageRetransmissionFailures,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,3,Valid
norUasAckfail,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasProterror,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasAudioSegmentFailed,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasComperror,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasProtocolSyntaxErrors,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
allEngineObjects,0,Valid
norUasConfLackOfResourceRejections,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
onfServiceObjects,0,Valid
norUasConfTotal,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
onfServiceObjects,10,Valid
norUasConfPlays,2005-03-
17T16:30:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasC
onfServiceObjects,2,Valid
norUasNumberOfPlayRecords,2005-03-
17T16:30:01EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasI
VRServiceObjects,0,Valid
norUasNumberOfPlayRecordErrors,2005-03-
17T16:30:01EST,.iso.org.dod.internet.private.enterprises.nortel.voip.uas.norUasI
VRServiceObjects,0,Valid
SingleValues=End

Entity=End

System=End

PMFile=End
```

GUI/CLUI Documentation for UAS

GUI Launching and User procedures

- NN10010-111 - UAS Basics

Related documents

- NTP NN10095-511 - Universal Audio Server Basics
- NN10095-511 - Universal Audio Server Configuration Management
- NN10161-611 - Universal Audio Server Security and Administration

Universal Signaling Point (USP)

This section contains IEMS Northbound log samples and device documentation references for the USP.

USP Fault Interface

Fault documentation for USP :

- NN10071-911 - USP Fault Management
- NN10072-911 - USP-Compact Fault Management

Fault Mapping for USP

The following criteria can be used for looking up information on specific faults for USP.

Fault Correlation for USP

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
USP	Specific Problem: Log Group = <text> & Log Number = <number> Note: Log GroupID is not used	Specific Problem: Log Group = <text> & Log Number = <number> Note: Log GroupID is not used	Specific Problem: Log Group =<text> & Log Number=<number> Note: Log GroupID is not used	Specific Problem: Log Group =<text> & Log Number=<number> Note: Log GroupID is not used	NN10071-911 USP Fault Management

Northbound Fault Formats for USP

SCC2

The following is an example of a USP log in SCC2 format:

```
**10 USP 398 0022 FLT  USP Fault
        Location: 47.135.60.201
        Notification Id: 526
        State: Raised
        Category: processingError
        Cause: applicationSubsystemFailure(2)
        Time: Jan 20 07:10:29 2004
        Component Id: USP=autoimage;Shelf=0;Slot=15;ContextID=0x0
        Specific Problem: Log GroupID=13;Log Group=System Node Maintenance;Log N
        umber=3
        Description: Transition to DISABLED Operational State.
```

NTSTD

The following is an example of a USP log in NTSTD format:

```
COMPACT06BT  ** USP398 Jan20 12:10:29 0022 FLT  USP Fault
        Location: 47.135.60.201
        Notification Id: 526
        State: Raised
        Category: processingError
        Cause: applicationSubsystemFailure(2)
        Time: Jan 20 07:10:29 2004
        Component Id: USP=autoimage;Shelf=0;Slot=15;ContextID=0x0
        Specific Problem: Log GroupID=13;Log Group=System Node Maintenance;Log N
        umber=3
        Description: Transition to DISABLED Operational State.
```

SNMP

The following is an example of a USP log in SNMP format:

```
sysUpTime.0 => 2:58:15
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.48.44.55.58.49.48.58.50.57.46.48.44.36582
alarmActiveDateAndTime => 2004-1-20,7:10:29.0,
alarmActiveDescription =>
DeviceSpecificInfo=applicationSubsystemFailure(2);Transition to DISABLED Operational
State.
```

nnExtAlarmActiveEventType => 3

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => USP 398

nnExtAlarmActiveResourceDescription => IEMS=usp_germany-1321-Unit-0;USP=autoimage;Shelf=0;Slot=15;ContextID=0x0

nnExtAlarmActiveManualClear => 0

nnExtAlarmActiveSequenceNumber => 21

Syslog

The following is an example of a USP log in Syslog format:

```
Feb 22 01:50:39 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0088~~  USP398 MAJOR FLT
USP Fault^M       Location: 47.135.60.201^M       Notification Id: 526^M       State:
Raised^M        Category: processingError^M        Cause:
applicationSubsystemFailure(2)^M       Time: Jan 20 07:10:29 2004^M       Component
Id: USP=autoimage;Shelf=0;Slot=15;ContextID=0x0^M        Specific Problem: Log
GroupID=13;Log Group=System Node Maintenance;Log N^M      umber=3^M      Description:
Transition to DISABLED Operational State.
```

Performance

OM and PM Documentation references for USP

- NN10137-711 - USP Performance Management
- NN10138-711 - USP-Compact Performance Management
- USP_logs_oms - USP Logs and OMs

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided.
Note that for SN08, the OMs/PMs are provided in raw CSV format.

XML

The following is an example of performance data for USP in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-12-09T16:30:20EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity Type="USP">
<EntityId>47.135.60.71</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Linkset Utilization</TableId>
```

```
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Linkset Inactivity Duration</Label>
<Label>RST Received Count</Label>
<Label>RST Transmitted Count</Label>
<Label>TFA and TCA Received Count</Label>
<Label>TFA and TCA Transmitted Count</Label>
<Label>TFC Received Count</Label>
<Label>TFC Transmitted Count</Label>
<Label>TFP and TCP Received Count</Label>
<Label>TFP and TCP Transmitted Count</Label>
<Label>TFR and TCR Received Count</Label>
<Label>TFR and TCR Transmitted Count</Label>
<Label>UPU Received Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

```
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>ASP Path Traffic</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Discarded MSUs Count</Label>
<Label>Discarded MTP3b MSUs Count</Label>
<Label>Originated MSUs Count</Label>
<Label>Received MSUs Count</Label>
<Label>Sent MSUs Count</Label>
<Label>Terminated MSUs Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
```

```
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
```

```
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8376</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
```

```
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>SCCP System Totals</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Conn-Orient IP Dist Viol Count</Label>
<Label>Conn-Orient Msg Handled Count</Label>
<Label>Conn-Orient Msg Rtg Fail Count</Label>
<Label>LUDT Msg Rcvd Count</Label>
<Label>LUDT Msg Sent Count</Label>
<Label>LUDTS Msg Sent Count</Label>
```

```
<Label>MSUs Disc-Unrec SCCP Msg Count</Label>
<Label>Msg Incompatibility</Label>
<Label>Msg too large for segmentation</Label>
<Label>Out of sequence SCCP msg count</Label>
<Label>Reassembly Timer Expired</Label>
<Label>Reassembly buffer unavailable</Label>
<Label>Reassembly failed</Label>
<Label>Routing Failure - Unequip.User</Label>
<Label>SCCP Routing Failure Count</Label>
<Label>SSA Received Count</Label>
<Label>SSA Transmitted Count</Label>
<Label>SSP Received Count</Label>
<Label>SSP Transmitted Count</Label>
<Label>SST Received Count</Label>
<Label>SST Transmitted Count</Label>
<Label>Segmentation failed</Label>
<Label>Total messages handled</Label>
<Label>UDT Msg Rcvd Count</Label>
<Label>UDT Msg Sent Count</Label>
<Label>UDTS Msg Rcvd Count</Label>
<Label>UDTS Msg Sent Count</Label>
<Label>XUDT Msg Rcvd Count</Label>
<Label>XUDT Msg Sent Count</Label>
<Label>XUDTS Msg Rcvd Count</Label>
<Label>XUDTS Msg Sent Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>TUP Received Message Counts</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>B/TUP Error No AS for OPC/CIC</Label>
<Label>B/TUP Error No OPC/CIC Data</Label>
```

```
<Label>B/TUP Error No Path</Label>
<Label>B/TUP Error No Route</Label>
<Label>BTUP Call P Received Count</Label>
<Label>BTUP Maint Received Count</Label>
<Label>TUP Call P Received Count</Label>
<Label>TUP Maint Received Count</Label>
<Label>Wrong NE Received Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Link Faults and Performance</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Number of SUs received in error</Label>
<Label>Number of negative ack.received</Label>
<Label>Octets Retransmitted</Label>
<Label>SL alignment or proving failure</Label>
<Label>SL failure-Abnormal FIBR/BSNR</Label>
<Label>SL failure-All reasons</Label>
<Label>SL failure-Exc. delay of ack</Label>
<Label>SL failure-Exc. duration of con</Label>
<Label>SL failure-Excessive error rate</Label>
<Label>SL failure-Other reasons</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>System Node State</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Disabled, Locked Duration</Label>
<Label>Disabled, Unlocked Duration</Label>
<Label>Enabled, Locked Duration</Label>
<Label>Enabled, Unlocked Duration</Label>
<Label>Locked, Off-line Duration</Label>
<Label>Percentage Enabled</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>100</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>SCTP Management/Traffic Counts</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Association Aborted Count</Label>
<Label>Association Establish Attempts</Label>
<Label>Association Terminated Count</Label>
<Label>Chunk Retransmitted Count</Label>
<Label>Chunks Received Count</Label>
<Label>Chunks Transmitted Count</Label>
<Label>Established Association Count</Label>
<Label>Out of Blue SCTP Packet</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Log Server</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Critical Alarms Ack Count</Label>
<Label>Critical Alarms Cleared Count</Label>
<Label>Critical Alarms Received Count</Label>
<Label>Major Alarms Ack Count</Label>
<Label>Major Alarms Cleared Count</Label>
<Label>Major Alarms Received Count</Label>
<Label>Minor Alarms Ack Count</Label>
<Label>Minor Alarms Cleared Count</Label>
<Label>Minor Alarms Received Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>UDP</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Full Socket Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Gateway Screening Results</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Disallowed Cld Party Addr Count</Label>
<Label>Disallowed ISUP Count</Label>
```

```
<Label>Disallowed Trans Type Count</Label>
<Label>Invalid Affct Destination Count</Label>
<Label>Invalid Affct PC-SSN Count</Label>
<Label>Invalid Cng Party Addr Count</Label>
<Label>Invalid DPC Count</Label>
<Label>Invalid OPC Count</Label>
<Label>Invalid SIO Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Task Management</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Collection Period Duration</Label>
<Label>Idle Task Duration</Label>
<Label>Level 0 Priority Task Duration</Label>
<Label>Level 1 Priority Task Duration</Label>
<Label>Level 2 Priority Task Duration</Label>
<Label>Level 3 Priority Task Duration</Label>
<Label>Level 4 Priority Task Duration</Label>
<Label>Level 5 Priority Task Duration</Label>
<Label>Level 6 Priority Task Duration</Label>
<Label>Level 7 Priority Task Duration</Label>
<Label>Level 8 Priority Task Duration</Label>
<Label>Level 9 Priority Task Duration</Label>
<Label>OS System Tasks Duration</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>299580</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>32</Value>
</RowValue>
<RowValue>
<Value>12</Value>
</RowValue>
<RowValue>
<Value>44</Value>
</RowValue>
<RowValue>
<Value>87</Value>
</RowValue>
<RowValue>
<Value>4</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>93</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>143</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>299644</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>19</Value>
</RowValue>
<RowValue>
<Value>30</Value>
</RowValue>
<RowValue>
<Value>11</Value>
</RowValue>
<RowValue>
<Value>42</Value>
</RowValue>
<RowValue>
<Value>81</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>39</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>143</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>298200</Value>
</RowValue>
<RowValue>
<Value>23</Value>
```

```
</RowValue>
<RowValue>
<Value>140</Value>
</RowValue>
<RowValue>
<Value>256</Value>
</RowValue>
<RowValue>
<Value>95</Value>
</RowValue>
<RowValue>
<Value>381</Value>
</RowValue>
<RowValue>
<Value>320</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>46</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>522</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300010</Value>
</RowValue>
<RowValue>
<Value>213491</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>199</Value>
</RowValue>
<RowValue>
<Value>942</Value>
</RowValue>
<RowValue>
<Value>131</Value>
</RowValue>
<RowValue>
<Value>419</Value>
</RowValue>
<RowValue>
<Value>83882</Value>
</RowValue>
<RowValue>
<Value>35</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
```

```
<Value>53</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>820</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300000</Value>
</RowValue>
<RowValue>
<Value>293717</Value>
</RowValue>
<RowValue>
<Value>9</Value>
</RowValue>
<RowValue>
<Value>143</Value>
</RowValue>
<RowValue>
<Value>173</Value>
</RowValue>
<RowValue>
<Value>42</Value>
</RowValue>
<RowValue>
<Value>275</Value>
</RowValue>
<RowValue>
<Value>216</Value>
</RowValue>
<RowValue>
<Value>4563</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>241</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>616</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300000</Value>
</RowValue>
<RowValue>
<Value>268732</Value>
</RowValue>
<RowValue>
<Value>10</Value>
</RowValue>
<RowValue>
<Value>69</Value>
</RowValue>
<RowValue>
```

```
<Value>332</Value>
</RowValue>
<RowValue>
<Value>45</Value>
</RowValue>
<RowValue>
<Value>161</Value>
</RowValue>
<RowValue>
<Value>30313</Value>
</RowValue>
<RowValue>
<Value>15</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>28</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>290</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>299990</Value>
</RowValue>
<RowValue>
<Value>211715</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3405</Value>
</RowValue>
<RowValue>
<Value>18873</Value>
</RowValue>
<RowValue>
<Value>790</Value>
</RowValue>
<RowValue>
<Value>12939</Value>
</RowValue>
<RowValue>
<Value>1461</Value>
</RowValue>
<RowValue>
<Value>219</Value>
</RowValue>
<RowValue>
<Value>38315</Value>
</RowValue>
<RowValue>
<Value>68</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>12200</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300000</Value>
</RowValue>
<RowValue>
<Value>211866</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3381</Value>
</RowValue>
<RowValue>
<Value>18854</Value>
</RowValue>
<RowValue>
<Value>792</Value>
</RowValue>
<RowValue>
<Value>13024</Value>
</RowValue>
<RowValue>
<Value>1171</Value>
</RowValue>
<RowValue>
<Value>211</Value>
</RowValue>
<RowValue>
<Value>38497</Value>
</RowValue>
<RowValue>
<Value>68</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>12131</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300000</Value>
</RowValue>
<RowValue>
<Value>299319</Value>
</RowValue>
<RowValue>
<Value>7</Value>
</RowValue>
<RowValue>
<Value>48</Value>
</RowValue>
<RowValue>
<Value>89</Value>
</RowValue>
<RowValue>
<Value>34</Value>
</RowValue>
```

```
<RowValue>
<Value>137</Value>
</RowValue>
<RowValue>
<Value>128</Value>
</RowValue>
<RowValue>
<Value>11</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>26</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>196</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>299818</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>30</Value>
</RowValue>
<RowValue>
<Value>9</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>46</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>40</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>42</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
```

```
<RowValue>
<Value>300020</Value>
</RowValue>
<RowValue>
<Value>299819</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>29</Value>
</RowValue>
<RowValue>
<Value>9</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>46</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>40</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>42</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300030</Value>
</RowValue>
<RowValue>
<Value>299600</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>18</Value>
</RowValue>
<RowValue>
<Value>31</Value>
</RowValue>
<RowValue>
<Value>11</Value>
</RowValue>
<RowValue>
<Value>43</Value>
</RowValue>
<RowValue>
<Value>79</Value>
```

```
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>92</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>144</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Link Traffic</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Link utilization</Label>
<Label>MSUs Received Count</Label>
<Label>MSUs Requiring GTT Count</Label>
<Label>MSUs Transmitted Count</Label>
<Label>MTP3b Discard Count</Label>
<Label>Network Indicator Discard Count</Label>
<Label>OPC Screening Discard Count</Label>
<Label>Octets Received Count</Label>
<Label>Octets Requiring GTT Count</Label>
<Label>Octets Transmitted Count</Label>
<Label>Originated MSU Octets Count</Label>
<Label>Pri 0 MSU Inbd Discard Count</Label>
<Label>Pri 0 MSU Outbd Discard Count</Label>
<Label>Pri 1 MSU Inbd Discard Count</Label>
<Label>Pri 1 MSU Outbd Discard Count</Label>
<Label>Pri 2 MSU Inbd Discard Count</Label>
<Label>Pri 2 MSU Outbd Discard Count</Label>
<Label>Pri 3 MSU Inbd Discard Count</Label>
<Label>Pri 3 MSU Outbd Discard Count</Label>
<Label>Terminated MSU Octets Count</Label>
<Label>Through-Switched MSUs Count</Label>
<Label>Thru-Switched MSU Octets Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>70</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474484</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>70</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
```

```
<Value>8378</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474484</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>70</Value>
</RowValue>
<RowValue>
<Value>67021</Value>
</RowValue>
```

```
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474462</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>67021</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>70</Value>
```

```
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474484</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>70</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474484</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>70</Value>
</RowValue>
<RowValue>
<Value>67021</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474462</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>67021</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>70</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>8378</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474484</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>134048</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>70</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>8376</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1474484</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>134016</Value>
</RowValue>
<RowValue>
<Value>134016</Value>
</RowValue>
<RowValue>
<Value>67022</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>ISUP Received Message Counts</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>ACM Received Count</Label>
<Label>ALT Received Count</Label>
<Label>ANM Received Count</Label>
<Label>BLA Received Count</Label>
<Label>BLO Received Count</Label>
<Label>CCR Received Count</Label>
```

```
<Label>CFN Received Count</Label>
<Label>CGB Received Count</Label>
<Label>CGBA Received Count</Label>
<Label>CGU Received Count</Label>
<Label>CGUA Received Count</Label>
<Label>CMC Received Count</Label>
<Label>CMR Received Count</Label>
<Label>CMRJ Received Count</Label>
<Label>CON Received Count</Label>
<Label>COT Received Count</Label>
<Label>CPG Received Count</Label>
<Label>CQM Received Count</Label>
<Label>CQR Received Count</Label>
<Label>CRA Received Count</Label>
<Label>CRG Received Count</Label>
<Label>CRM Received Count</Label>
<Label>CSVR Received Count</Label>
<Label>CSVS Received Count</Label>
<Label>CVR Received Count</Label>
<Label>CVT Received Count</Label>
<Label>DRS Received Count</Label>
<Label>EXM Received Count</Label>
<Label>FAA Received Count</Label>
<Label>FAC Received Count</Label>
<Label>FAD Received Count</Label>
<Label>FAI Received Count</Label>
<Label>FAR Received Count</Label>
<Label>FOT Received Count</Label>
<Label>FRJ Received Count</Label>
<Label>GRA Received Count</Label>
<Label>GRS Received Count</Label>
<Label>IAM Received Count</Label>
<Label>IAMN1 Received Count</Label>
<Label>IDR Received Count</Label>
<Label>INF Received Count</Label>
<Label>INR Received Count</Label>
<Label>IRS Received Count</Label>
<Label>ISUP Error No AS for OPC/CIC</Label>
<Label>ISUP Error No OPC/CIC Data</Label>
<Label>ISUP Error No Path</Label>
<Label>ISUP Error No Route</Label>
<Label>ISUP Error Unknown Message</Label>
<Label>LOP Received Count</Label>
<Label>LPA Received Count</Label>
<Label>NRM Received Count</Label>
<Label>PAM Received Count</Label>
<Label>PRG Received Count</Label>
<Label>REL Received Count</Label>
<Label>RES Received Count</Label>
<Label>RLC Received Count</Label>
<Label>RPM Received Count</Label>
<Label>RSC Received Count</Label>
<Label>SAM Received Count</Label>
<Label>SGM Received Count</Label>
<Label>SUS Received Count</Label>
<Label>UBA Received Count</Label>
<Label>UBL Received Count</Label>
<Label>UCIC Received Count</Label>
<Label>UPA Received Count</Label>
<Label>UPT Received Count</Label>
<Label>USR Received Count</Label>
</Labels>
<RowOfValues>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
```

```
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>

</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Route Set Management</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>RouteSet Congested Count</Label>
<Label>Routeset Man-busied Count</Label>
<Label>Routeset Unavailability Count</Label>
<Label>Routeset Unavailability Dur.</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Link Management</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Changeover Procedure Count</Label>
```

```
<Label>Far End Mgmt Inhibit Count</Label>
<Label>Level 1 Congestion Count</Label>
<Label>Level 1 Congestion Duration</Label>
<Label>Level 2 Congestion Count</Label>
<Label>Level 2 Congestion Duration</Label>
<Label>Level 3 Congestion Count</Label>
<Label>Level 3 Congestion Duration</Label>
<Label>Link Available Duration</Label>
<Label>Link Deactivated Duration</Label>
<Label>Link Local Inhibit Duration</Label>
<Label>Link Remote Inhibit Duration</Label>
<Label>Near End Forced Unavailable Cou</Label>
<Label>RPO Count</Label>
<Label>RPO Cumulative Duration</Label>
<Label>Unavailable Duration</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value/>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>300</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>BICC Received Message Counts</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>BICC Call P Received Count</Label>
<Label>BICC Error No OPC Route</Label>
<Label>BICC Error No Path</Label>
```

```
<Label>BICC Error No Route</Label>
<Label>BICC Maint Received Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>ASP Path Management</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Path Down Time</Label>
<Label>Path Restore Time</Label>
<Label>Path Up Time</Label>
<Label>Path entered Down state</Label>
<Label>Path entered Restoring state</Label>
<Label>Path entered Up state</Label>
```

```
</Labels>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>300</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>Carrier</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Far End Line - Errored Seconds</Label>
<Label>Far End P - Sev Err Frm/AIS Sec</Label>
```

```
<Label>Far End P - Severely Err Secs</Label>
<Label>Far End P - Unavailable Seconds</Label>
<Label>Far End Path - Code Violations</Label>
<Label>Far End Path - Controlled Slips</Label>
<Label>Far End Path - Errored Seconds</Label>
<Label>Far End Path - Failure Count</Label>
<Label>Line - Code Violations</Label>
<Label>Line - Errored Seconds</Label>
<Label>Line - Loss of Signal Seconds</Label>
<Label>Line - Severely Errored Seconds</Label>
<Label>P - Severely Err Frame/AIS Secs</Label>
<Label>Path - AIS Seconds</Label>
<Label>Path - Code Violations</Label>
<Label>Path - Errored Seconds</Label>
<Label>Path - Failure Count</Label>
<Label>Path - Severely Errored Seconds</Label>
<Label>Path - Unavailable Seconds</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
```

```
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>ATM Driver Messaging</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Duplicate Messages Count</Label>
<Label>IP Message Count</Label>
<Label>Plane 1 CRC Error Count</Label>
<Label>Plane 1 Messages Count</Label>
<Label>Plane 2 CRC Error Count</Label>
<Label>Plane 2 Messages Count</Label>
<Label>Raw Cell Count</Label>
<Label>Raw Message Count</Label>
<Label>SSCOP Message Count</Label>
<Label>Sequence Number Reset Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>1725</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1725</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1725</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1091</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1730</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1730</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1730</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1096</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1087</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>24365</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>24365</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>24365</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>23731</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1997</Value>
</RowValue>
<RowValue>
<Value>869</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1997</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1997</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1128</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>24364</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>24364</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>24364</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>23730</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>3064</Value>
</RowValue>
<RowValue>
<Value>3064</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3064</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3064</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>3064</Value>
</RowValue>
<RowValue>
<Value>3064</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3064</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>3064</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1721</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1087</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>34</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1080</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>34</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1114</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1080</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>1729</Value>
</RowValue>
<RowValue>
<Value>634</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1729</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1729</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>1095</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>ASP Path Utilization</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>DAUD Received Count</Label>
<Label>DAVA Transmitted Count</Label>
<Label>DUNA Transmitted Count</Label>
<Label>DUPU Transmitted Count</Label>
<Label>SCON Transmitted Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
```

```
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
```

```
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>SCCP GTT</TableId>
<CaptureTime>2004-12-09T09:10:00EST</CaptureTime>
<Labels>
<Label>Alt Routing on Cong Count</Label>
<Label>GTT Performed Count</Label>
<Label>Hop Counter Violation Count</Label>
<Label>No Translation for Addr Count</Label>
<Label>Trans Type Not Found Count</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of performance data for USP in CSV format:

```
NOA;Task Management;LINK_NODE_3_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;23
NOA;Task Management;LINK_NODE_3_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;128
NOA;Task Management;LINK_NODE_3_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;348
NOA;Task Management;LINK_NODE_3_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;105
NOA;Task Management;LINK_NODE_3_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;377
NOA;Task Management;LINK_NODE_3_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;345
NOA;Task Management;LINK_NODE_3_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;33
NOA;Task Management;LINK_NODE_3_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
```

```
NOA;Task Management;LINK_NODE_3_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;149
NOA;Task Management;LINK_NODE_3_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;LINK_NODE_3_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;542
NOA;Task Management;LINK_NODE_3_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300000
NOA;Task Management;LINK_NODE_4_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;23
NOA;Task Management;LINK_NODE_4_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;129
NOA;Task Management;LINK_NODE_4_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;276
NOA;Task Management;LINK_NODE_4_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;105
NOA;Task Management;LINK_NODE_4_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;376
NOA;Task Management;LINK_NODE_4_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;298
NOA;Task Management;LINK_NODE_4_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;35
NOA;Task Management;LINK_NODE_4_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;LINK_NODE_4_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;148
NOA;Task Management;LINK_NODE_4_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;LINK_NODE_4_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;534
NOA;Task Management;LINK_NODE_4_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;CC_NODE_1_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;CC_NODE_1_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3404
NOA;Task Management;CC_NODE_1_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;18883
NOA;Task Management;CC_NODE_1_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;794
NOA;Task Management;CC_NODE_1_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;12846
NOA;Task Management;CC_NODE_1_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;1479
NOA;Task Management;CC_NODE_1_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;220
NOA;Task Management;CC_NODE_1_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;38371
NOA;Task Management;CC_NODE_1_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;70
NOA;Task Management;CC_NODE_1_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;CC_NODE_1_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;12199
NOA;Task Management;CC_NODE_1_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;LINK_NODE_5_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;23
NOA;Task Management;LINK_NODE_5_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;137
NOA;Task Management;LINK_NODE_5_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;402
NOA;Task Management;LINK_NODE_5_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;109
```

```
NOA;Task Management;LINK_NODE_5_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;380
NOA;Task Management;LINK_NODE_5_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;378
NOA;Task Management;LINK_NODE_5_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;34
NOA;Task Management;LINK_NODE_5_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;LINK_NODE_5_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;148
NOA;Task Management;LINK_NODE_5_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;LINK_NODE_5_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;540
NOA;Task Management;LINK_NODE_5_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;NODE_LINK_6_1;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;22
NOA;Task Management;NODE_LINK_6_1;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;148
NOA;Task Management;NODE_LINK_6_1;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;399
NOA;Task Management;NODE_LINK_6_1;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;109
NOA;Task Management;NODE_LINK_6_1;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;383
NOA;Task Management;NODE_LINK_6_1;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;382
NOA;Task Management;NODE_LINK_6_1;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;35
NOA;Task Management;NODE_LINK_6_1;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;NODE_LINK_6_1;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;148
NOA;Task Management;NODE_LINK_6_1;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;NODE_LINK_6_1;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;542
NOA;Task Management;NODE_LINK_6_1;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;IP_LINK_NODE_9;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;2
NOA;Task Management;IP_LINK_NODE_9;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;26
NOA;Task Management;IP_LINK_NODE_9;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;34
NOA;Task Management;IP_LINK_NODE_9;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;13
NOA;Task Management;IP_LINK_NODE_9;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;42
NOA;Task Management;IP_LINK_NODE_9;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;418
NOA;Task Management;IP_LINK_NODE_9;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;4
NOA;Task Management;IP_LINK_NODE_9;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;IP_LINK_NODE_9;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;41
NOA;Task Management;IP_LINK_NODE_9;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;IP_LINK_NODE_9;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;225
NOA;Task Management;IP_LINK_NODE_9;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300010
```

```
NOA;Task Management;IP_LINK_NODE_10;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;2
NOA;Task Management;IP_LINK_NODE_10;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;24
NOA;Task Management;IP_LINK_NODE_10;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;33
NOA;Task Management;IP_LINK_NODE_10;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;13
NOA;Task Management;IP_LINK_NODE_10;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;43
NOA;Task Management;IP_LINK_NODE_10;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;415
NOA;Task Management;IP_LINK_NODE_10;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;4
NOA;Task Management;IP_LINK_NODE_10;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;IP_LINK_NODE_10;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;42
NOA;Task Management;IP_LINK_NODE_10;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;IP_LINK_NODE_10;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;224
NOA;Task Management;IP_LINK_NODE_10;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300010
NOA;Task Management;RTC_NODE_15;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;RTC_NODE_15;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;45
NOA;Task Management;RTC_NODE_15;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;58
NOA;Task Management;RTC_NODE_15;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;13
NOA;Task Management;RTC_NODE_15;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;99
NOA;Task Management;RTC_NODE_15;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;130
NOA;Task Management;RTC_NODE_15;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;1399
NOA;Task Management;RTC_NODE_15;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;RTC_NODE_15;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;119
NOA;Task Management;RTC_NODE_15;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;RTC_NODE_15;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;131
NOA;Task Management;RTC_NODE_15;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299990
NOA;Task Management;CC_NODE_1_18;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;CC_NODE_1_18;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3410
NOA;Task Management;CC_NODE_1_18;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;19067
NOA;Task Management;CC_NODE_1_18;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;791
NOA;Task Management;CC_NODE_1_18;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;12798
NOA;Task Management;CC_NODE_1_18;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;1479
NOA;Task Management;CC_NODE_1_18;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;226
NOA;Task Management;CC_NODE_1_18;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;38371
```

```
NOA;Task Management;CC_NODE_1_18;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;67
NOA;Task Management;CC_NODE_1_18;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;CC_NODE_1_18;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;12207
NOA;Task Management;CC_NODE_1_18;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299980
NOA;System Node State;CC_NODE_1_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;LINK_NODE_3_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;LINK_NODE_4_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;LINK_NODE_5_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;NODE_LINK_6_1;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;IP_LINK_NODE_8;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;System Node State;IP_LINK_NODE_9;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;IP_LINK_NODE_10;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;IP_LINK_NODE_11;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;System Node State;RTC_NODE_12;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;RTC_NODE_15;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;System Node State;CC_NODE_1_18;Percentage Enabled;;03/24/2005
15:15:00;03/24/2005 15:20:00;100
NOA;Task Management;RTC_NODE_12;Level 0 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;3
NOA;Task Management;RTC_NODE_12;Level 1 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;47
NOA;Task Management;RTC_NODE_12;Level 2 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;67
NOA;Task Management;RTC_NODE_12;Level 3 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;13
NOA;Task Management;RTC_NODE_12;Level 4 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;118
NOA;Task Management;RTC_NODE_12;Level 5 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;149
NOA;Task Management;RTC_NODE_12;Level 6 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;1554
NOA;Task Management;RTC_NODE_12;Level 7 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;RTC_NODE_12;Level 8 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;166
NOA;Task Management;RTC_NODE_12;Level 9 Priority Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
NOA;Task Management;RTC_NODE_12;OS System Tasks Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;188
NOA;Task Management;RTC_NODE_12;Collection Period Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300000
ACC;System Node State;CC_NODE_1_18;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_18;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_18;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;CC_NODE_1_18;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;System Node State;CC_NODE_1_18;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Minor Alarms Cleared Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Major Alarms Cleared Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Critical Alarms Cleared Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Minor Alarms Ack Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Log Server;RTC_NODE_12;Major Alarms Ack Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Log Server;RTC_NODE_12;Critical Alarms Ack Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Minor Alarms Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Major Alarms Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Log Server;RTC_NODE_12;Critical Alarms Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2930
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1392
ACC;ATM Driver Messaging;RTC_NODE_12;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;4322
ACC;ATM Driver Messaging;RTC_NODE_12;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;4322
ACC;ATM Driver Messaging;RTC_NODE_12;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;4322
ACC;ATM Driver Messaging;RTC_NODE_12;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_12;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Association Terminated
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;MSUs Disc-Unrec SCCP Msg Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;Hop Counter Violation Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;Alt Routing on Cong Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;No Translation for Addr Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;SCCP GTT;USP:C7NETWRK1;Trans Type Not Found Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP GTT;USP:C7NETWRK1;GTT Performed Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Conn-Orient IP Dist Viol Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Conn-Orient Msg Rtg Fail Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Conn-Orient Msg Handled Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SCCP Routing Failure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Reassembly failed;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Segmentation failed;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Msg too large for segmentation;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Reassembly Timer Expired;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Reassembly buffer unavailable;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Out of sequence SCCP msg count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Msg Incompatibility;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;LUDTS Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;LUDT Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;LUDT Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;XUDTS Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;XUDT Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;XUDTS Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;XUDT Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;UDTS Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;UDT Msg Rcvd Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;UDTS Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;UDT Msg Sent Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SSA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SSA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SSP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;SSP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Association Aborted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Established Association
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;6
```

```
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Association Establish
Attempts;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Chunk Retransmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Chunks Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Chunks Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_10;Out of Blue SCTP
Packet;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;878
ACC;ATM Driver Messaging;IP_LINK_NODE_10;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;CC_NODE_1_18;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_18;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_18;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_18;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_18;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_18;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;RTC Sanity;CC_NODE_1_18; RTC12 Passive Audit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;RTC Sanity;CC_NODE_1_18; RTC15 Passive Audit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2022
ACC;ATM Driver Messaging;LINK_NODE_3_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2022
ACC;ATM Driver Messaging;LINK_NODE_3_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2022
ACC;ATM Driver Messaging;LINK_NODE_3_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;LINK_NODE_3_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1398
ACC;ATM Driver Messaging;LINK_NODE_3_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_3_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_3_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_3_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_3_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;LINK_NODE_3_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;System Node State;LINK_NODE_3_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1798
ACC;ATM Driver Messaging;LINK_NODE_4_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1798
ACC;ATM Driver Messaging;LINK_NODE_4_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1798
ACC;ATM Driver Messaging;LINK_NODE_4_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;LINK_NODE_4_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1174
ACC;ATM Driver Messaging;LINK_NODE_4_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_4_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_4_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_4_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_4_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;LINK_NODE_4_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_4_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_5_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_5_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_5_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;LINK_NODE_5_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;LINK_NODE_5_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2217
ACC;ATM Driver Messaging;LINK_NODE_5_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2217
ACC;ATM Driver Messaging;LINK_NODE_5_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2217
ACC;ATM Driver Messaging;LINK_NODE_5_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;LINK_NODE_5_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1593
ACC;ATM Driver Messaging;LINK_NODE_5_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;LINK_NODE_5_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ATM Driver Messaging;NODE_LINK_6_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2221
ACC;ATM Driver Messaging;NODE_LINK_6_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2221
ACC;ATM Driver Messaging;NODE_LINK_6_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2221
ACC;ATM Driver Messaging;NODE_LINK_6_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;NODE_LINK_6_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1597
ACC;ATM Driver Messaging;NODE_LINK_6_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;NODE_LINK_6_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;NODE_LINK_6_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;NODE_LINK_6_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;NODE_LINK_6_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;NODE_LINK_6_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;NODE_LINK_6_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_12;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;RTC_NODE_12;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_12;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;2300
ACC;ATM Driver Messaging;RTC_NODE_15;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1351
ACC;ATM Driver Messaging;RTC_NODE_15;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3651
ACC;ATM Driver Messaging;RTC_NODE_15;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3651
ACC;ATM Driver Messaging;RTC_NODE_15;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3651
ACC;ATM Driver Messaging;RTC_NODE_15;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;RTC_NODE_15;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_15;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_15;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;RTC_NODE_15;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_15;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_15;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;System Node State;IP_LINK_NODE_10;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_10;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_10;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;IP_LINK_NODE_10;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_10;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_10;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid SIO
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid DPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;LINK_NODE_3_1;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;297941
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
MAX;Link Traffic;LS:C7LKSET2 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Linkset Utilization;LS:STEPBOX01;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Linkset Utilization;LS:STPA_INTL;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Invalid OPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid SIO
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:0;Path entered Up
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:0;Path entered Up
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid DPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC13_PVG194A PID:1;Invalid OPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;DUPU Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;SCON Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;DUNA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:0;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:1;DAVA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Discarded MTP3b MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:0;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPC_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPC_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPC_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPC_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPFVME3_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPFVME3_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPFVME3_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPFVME3_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Near End Forced Unavailable Cou;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
```

```
ACC;Link Management;LS:RTPFVME3 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:RTPFVME3 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;B/TUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:RTPFVME3 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;USR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UPT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UBL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;UBA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;SUS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;SGM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;SAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;RSC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;RPM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;RLC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;RES Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;REL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;PRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;PAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;NRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;LPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;LOP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;IRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;INR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;INF Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;IDR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;IAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;GRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;GRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FOT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FRJ Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAI Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;FAA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;EXM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;DRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CVT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CVR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CQR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CQM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CPG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;COT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CON Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET3;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Linkset Utilization;LS:ITUCLKSET2;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ITUCLKSET2;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:0;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CMR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CMC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CGU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CGB Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CFN Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;CCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;BLO Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:RTPFVME3 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Octets Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;MSUs Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:RTPFVME3 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:RTPFVME3 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:RTPFVME3 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:RTPFVME3 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;DAUD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;AS Master;RTPSSP;Core Overload Duration;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;AS Master;RTPSSP;TUP Discard Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;AS Master;RTPSSP;BICC Discard Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;AS Master;RTPSSP;ISUP Discard Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;AS Master;RTPSSP;RANAP Discard Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;AS Master;RTPSSP;BSSAP Discard Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;DAUD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC15_PVG192A PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:CATTBOX01 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET2 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ITUCLKSET3 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;50
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC15_PVG192A PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:SIMTOOL_RTESET;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:SIMTOOL_RTESET;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:SIMTOOL_RTESET;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:SIMTOOL_RTESET;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC14_PVG190A PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET2;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET2;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET2;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET2;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:RTPFVME3 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path entered Down state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:0;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:0;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:RTPFVME3;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CATTBOX_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CATTBOX_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CATTBOX_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CATTBOX_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:CATTBOX01 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Utilization;ASP:GWC9_PVG192B PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPB_INTL;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STPA_INTL;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000002;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:ST000001;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:STEPBOX01;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET2;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:C7LKSET1;UPU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC9_PVG192B PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;DAUD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC2_PVG191_194 PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC2_PVG191_194 PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;DAUD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC1_PVG190_193 PID:0;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_11;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;IP_LINK_NODE_11;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_11;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_11;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_11;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_8;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;IP_LINK_NODE_8;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_8;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_8;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_8;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTPRTPB_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTPRTPB_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTPRTPB_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTPRTPB_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:CATTBOX01 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Route Set Management;RS:CRES16A_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES16A_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES16A_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES16A_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPS_INTL_RTP6;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPS_INTL_RTP6;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPS_INTL_RTP6;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPS_INTL_RTP6;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STEPBOX_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STEPBOX_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STEPBOX_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STEPBOX_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP6_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP6_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP6_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP6_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPB_INTL_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPB_INTL_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPB_INTL_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPB_INTL_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPA_INTL_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPA_INTL_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPA_INTL_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:STPA_INTL_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPI_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPI_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPI_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTPI_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES58A_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES58A_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES58A_RS;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:CRES58A_RS;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Route Set Management;RS:RTPSTORTP5_RS;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP5_RS;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP5_RS;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:RTPSTORTP5_RS;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPQRTESET1;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPQRTESET1;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPQRTESET1;Routeset Unavailability
Dur.;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPQRTESET1;Routeset Unavailability
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPB;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPB;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPB;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPB;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPA;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPA;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPA;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:BNRRTPSTPA;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET2;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET2;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET2;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET2;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET1;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET1;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET1;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:C7RTESET1;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;RTC_NODE_12;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;297690
ACC;Task Management;CC_NODE_1_18;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;211558
ACC;Task Management;RTC_NODE_15;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;297990
ACC;BICC Received Message Counts;LS:CATTBOX01 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;IP_LINK_NODE_10;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299204
```

```
ACC;ASP Path Traffic;ASP:GWC1_PVG190_193 PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;DUPU Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;SCON Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;IP_LINK_NODE_9;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;299199
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET2 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPB_INTL SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000002 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000002 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000002 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000002 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;NODE_LINK_6_1;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;297815
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:C7LKSET1 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STPA_INTL SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:STPB_INTL SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:CATTBOX01 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:ST000001 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;LINK_NODE_5_1;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;297830
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:STEPBOX01 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;LINK_NODE_4_1;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;298056
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:C7LKSET1 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:STPA_INTL SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:ST000001 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Total messages handled;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCCP System Totals;USP:C7NETWRK1;Routing Failure - Unequip.User;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
MAX;Link Traffic;LS:STEPBOX01 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:ST000002 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Near End Forced Unavailable Cou;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Near End Forced Unavailable Cou;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Management;LS:C7LKSET1 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;B/TUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET2 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;USR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UPT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UBL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;UBA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;SUS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;SGM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;SAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;RSC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;RPM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;RLC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;RES Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;REL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;PRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;PAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;NRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;LPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;LOP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;IRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;INR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;INF Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;IDR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;IAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;GRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;GRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;FOT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;FRJ Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;FAR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;FAI Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;FAD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;FAC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;FAA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;EXM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;DRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CVT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CVR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CQR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CQM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CPG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;COT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CON Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CMR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CMC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CGU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CGB Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CFN Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;CCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;BLO Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET2 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET2 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET2 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET2 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;B/TUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:C7LKSET1 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;USR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UPT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UBL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;UBA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;SUS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;SGM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;SAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;RSC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;RPM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;RLC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;RES Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;REL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;PRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;PAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;NRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;LPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;LOP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;IRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;INR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;INF Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;IDR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;IAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;GRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;GRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;FOT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;FRJ Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;FAR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;FAI Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;FAD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;FAC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;FAA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;EXM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;DRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CVT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CVR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CQR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CQM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CPG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;COT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CON Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CMR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CMC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CGU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CGB Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CFN Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;CCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;BLO Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:C7LKSET1 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:C7LKSET1 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Management;LS:C7LKSET1 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:C7LKSET1 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_12;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;RTC_NODE_12;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Association Terminated
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Association Aborted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Established Association
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;6
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Association Establish
Attempts;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Chunk Retransmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Chunks Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Chunks Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;SCTP Management/Traffic Counts;IP_LINK_NODE_9;Out of Blue SCTP
Packet;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;878
ACC;ATM Driver Messaging;IP_LINK_NODE_9;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;624
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;1502
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;IP_LINK_NODE_9;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_9;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_9;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_9;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;IP_LINK_NODE_9;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;IP_LINK_NODE_9;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STEPBOX01 SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;MSUs Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STEPBOX01 SLC:0;Octets Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;FAC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;FAD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;FAI Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;FAR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;FRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;FOT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;GRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;GRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;IAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;IDR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;INF Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;INR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STEPBOX01 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STEPBOX01 SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Traffic;LS:STPA_INTL SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPA_INTL SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000001 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPA_INTL SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;MSUs Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000001 SLC:0;Octets Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;BLO Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CFN Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CGB Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CGU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CMC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CMR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CON Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;COT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CPG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CQM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CQR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CVR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;CVT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;DRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;EXM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FAA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FAC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FAD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FAI Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FAR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FRJ Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;FOT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;GRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;GRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;IAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;IDR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;INF Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;INR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;IRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;LOP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;LPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;NRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;PAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;PRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;REL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;RES Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;RLC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;RPM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;RSC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;SAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;SGM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;SUS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UBA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UBL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;UPT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;USR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ISUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000001 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;FAC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;FAD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;FAI Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;FAR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;FRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;FOT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;GRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;GRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;IAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;IDR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;INF Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;INR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPA_INTL SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Traffic;LS:ST000002 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:STPB_INTL SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000001 SLC:0;B/TUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPA_INTL SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ST000002 SLC:0;Disallowed ISUP Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:STPB_INTL SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;MSUs Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ST000002 SLC:0;Octets Requiring GTT Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ACM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ALT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ANM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;BLA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;BLO Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CFN Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CGB Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CGU Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CMC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CMR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CON Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;COT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CPG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CQM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CQR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CVR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;CVT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;DRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;EXM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;FAA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;FAC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;FAD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;FAI Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;FAR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;FRJ Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;FOT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;GRA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;GRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;IAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;IDR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;INF Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;INR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;IRS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;LOP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;LPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;NRM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;PAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;PRG Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;REL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;RES Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;RLC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;RPM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;RSC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;SAM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;SGM Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;SUS Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UBA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UBL Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UPA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;UPT Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;USR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ST000002 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;FAC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;FAD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;FAI Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;FAR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;FRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;FOT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;GRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;GRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;IAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;IDR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;INF Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;INR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:STPB_INTL SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ST000002 SLC:0;B/TUP Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:STPB_INTL SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:ST000002 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Near End Forced Unavailable Cou;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000002 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Management;LS:STEPBOX01 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STEPBOX01 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:ST000001 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Near End Forced Unavailable Cou;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ST000001 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:STPB_INTL SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPB_INTL SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
```

```
ACC;Link Management;LS:STPA_INTL SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:STPA_INTL SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:STPA_INTL SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:CATTBOX01 SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:CATTBOX01 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;DUNA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:RTPSSSP PID:0;DAVA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Discarded MTP3b MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:RTPSSSP PID:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:CATTBOX01;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:AUTORTESET;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:AUTORTESET;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:AUTORTESET;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:AUTORTESET;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 3 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 2 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:AUTOLKSET SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:AUTOLKSET SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:AUTOLKSET SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;INR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;INF Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;IDR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;IAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;GRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;GRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;FOT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;FRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;FAR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;FAI Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;FAD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;FAC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:AUTOLKSET SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:AUTOLKSET SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 3 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 2 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:AUTOLKSET SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:AUTOLKSET SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 3 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 2 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 1 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 3 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 2 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 1 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:AUTOLKSET SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;Octets
Retransmitted;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;Number of negative
ack.received;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;Number of SUs received in
error;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL alignment or proving
failure;;03/24/2005 15:15:00;03/24/2005 15:20:00;24
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Other
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Exc. duration of
con;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Excessive error
rate;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Exc. delay of
ack;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-Abnormal
FIBR/BSNR;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_1;Locked, Off-line Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_1;Enabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;System Node State;CC_NODE_1_1;Enabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;System Node State;CC_NODE_1_1;Disabled, Locked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;System Node State;CC_NODE_1_1;Disabled, Unlocked Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Task Management;CC_NODE_1_1;Idle Task Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;211720
ACC;RTC Sanity;CC_NODE_1_1; RTC15 Passive Audit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;RTC Sanity;CC_NODE_1_1; RTC12 Passive Audit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;Sequence Number Reset Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;Raw Cell Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;Raw Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;SSCOP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;IP Message Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_1;Duplicate Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_1;Plane 2 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_1;Plane 1 Messages Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;3054
ACC;ATM Driver Messaging;CC_NODE_1_1;Plane 2 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ATM Driver Messaging;CC_NODE_1_1;Plane 1 CRC Error Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;UDP;CC_NODE_1_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;INR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;INF Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;IDR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;IAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;GRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;GRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;FOT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;FRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;FAR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;FAI Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;FAD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;FAC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:CATTBOX01 SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFC Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFC Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;RST Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;RST Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFA and TCA Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFA and TCA Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFR and TCR Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFR and TCR Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFP and TCP Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;TFP and TCP Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Linkset Utilization;LS:AUTOLKSET;Linkset Inactivity Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;UDP;CC_NODE_1_18;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;RTC_NODE_15;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;RTC_NODE_12;Full Socket Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;UDP;IP_LINK_NODE_10;Full Socket Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;UDP;IP_LINK_NODE_9;Full Socket Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;UDP;NODE_LINK_6_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;UDP;LINK_NODE_5_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;Link Faults and Performance;LS:AUTOLKSET SLC:0;SL failure-All
reasons;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;UDP;LINK_NODE_4_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;UDP;LINK_NODE_3_1;Full Socket Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET2 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPB_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPB_INTL SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPB_INTL SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPB_INTL SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPB_INTL SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPB_INTL SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000002 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000002 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000002 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000002 SLC:0;BICC Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000002 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000002 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET1 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET1 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET1 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET1 SLC:0;BICC Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET1 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:C7LKSET1 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPA_INTL SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPA_INTL SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPA_INTL SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPA_INTL SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPA_INTL SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STPA_INTL SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;BICC Received Message Counts;LS:ST000001 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000001 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000001 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000001 SLC:0;BICC Error No Path;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000001 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ST000001 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:STEPBOX01 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET2 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:ITUCLKSET2 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET2 SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC2_PVG191_194 PID:1;Path entered Up
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FAC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FAD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FAI Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FAR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;FOT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;GRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;GRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;IAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;IDR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;INF Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;INR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC9_PVG192B PID:1;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path entered Down state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:RTPSSSP PID:1;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC13_PVG194A PID:1;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC1_PVG190_193 PID:1;Path entered Up
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC15_PVG192A PID:1;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path Restore Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path Down Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path Up Time;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path entered Restoring
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path entered Down
state;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Management;ASP:GWC14_PVG190A PID:1;Path entered Up state;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid SIO
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid DPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC1_PVG190_193 PID:1;Invalid OPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid SIO
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid DPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC15_PVG192A PID:1;Invalid OPC
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;ASP:GWC14_PVG190A PID:1;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET2 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET2 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Management;LS:ITUCLKSET2 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC14_PVG190A PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;DUPU Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;SCON Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;DAUD Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;DUNA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Utilization;ASP:GWC13_PVG194A PID:1;DAVA Transmitted
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET3;Routeset Man-busied Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET3;RouteSet Congested Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET3;Routeset Unavailability Dur.;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Route Set Management;RS:ITURTESET3;Routeset Unavailability Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Discarded MTP3b MSUs
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Discarded MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Received MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Sent MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;ASP Path Traffic;ASP:GWC13_PVG194A PID:1;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;MSUs Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;MSUs Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Octets Transmitted Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Octets Received Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Pri 0 MSU Outbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Pri 0 MSU Inbd Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Originated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Terminated MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Through-Switched MSUs Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Originated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Terminated MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Thru-Switched MSU Octets Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;Network Indicator Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;OPC Screening Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Traffic;LS:ITUCLKSET3 SLC:0;MTP3b Discard Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
MAX;Link Traffic;LS:ITUCLKSET3 SLC:0;Link utilization;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Level 1 Congestion Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid OPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid DPC Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid SIO Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid Affct Destination
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid Cng Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Invalid Affct PC-SSN
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Disallowed Cld Party Addr
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Disallowed Trans Type
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Gateway Screening Results;LS:ITUCLKSET3 SLC:0;Disallowed ISUP
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ACM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ALT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ANM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;BLA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;BLO Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CCR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CFN Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CGB Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CGBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CGU Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CGUA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CMC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CMRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CMR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CON Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;COT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CPG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CQM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CQR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CSVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CSVS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CVR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;CVT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;DRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;EXM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;FAA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;FAC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;FAD Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;FAI Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;FAR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;FRJ Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;FOT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;GRA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;GRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;IAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;IAMN1 Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;IDR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;INF Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;INR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;IRS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;LOP Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;LPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;NRM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;PAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;PRG Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;REL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;RES Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;RLC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;RPM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
```

```
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;RSC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;SAM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;SGM Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;SUS Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;UBA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;UBL Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;UCIC Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;UPA Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;UPT Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;USR Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;ISUP Error Unknown
Message;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;ISUP Received Message Counts;LS:ITUCLKSET3 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;TUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;TUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;BTUP Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;BTUP Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;B/TUP Error No OPC/CIC
Data;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;B/TUP Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;B/TUP Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;B/TUP Error No AS for
OPC/CIC;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;TUP Received Message Counts;LS:ITUCLKSET3 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Call P Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Maint Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Error No
Path;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Error No
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;BICC Error No OPC
Route;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;BICC Received Message Counts;LS:ITUCLKSET3 SLC:0;Wrong NE Received
Count;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Link Deactivated Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
```

```
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Link Local Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Link Remote Inhibit Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Unavailable Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Level 1 Congestion Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Link Available Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;300
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Changeover Procedure Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Near End Forced Unavailable
Cou;;03/24/2005 15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;Far End Mgmt Inhibit Count;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;RPO Cumulative Duration;;03/24/2005
15:15:00;03/24/2005 15:20:00;0
ACC;Link Management;LS:ITUCLKSET3 SLC:0;RPO Count;;03/24/2005 15:15:00;03/24/2005
15:20:00;0
```

GUI/CLUI Documentation for USP

GUI Launching and User procedures

- NN10093-511 - USP Configuration Management
- NN10094-511 - USP-Compact Operational Configuration
- NN10159-611 - USP Security and Administration
- NN10160-611 - USP-Compact Security and Administration

Related documents

- NN10008-111 - USP Basics
- NN10045-461 - Upgrading the USP
- NN10009-111 - USP-Compact Basics

XACore

This section contains IEMS Northbound log samples and device documentation references for the XACore.

XACore Fault Interface

Fault documentation for XACore :

- 297-8991-510 - XA-Core Maintenance Manual
- NN10275-909 - Carrier VoIP Fault Management Logs Reference, volumes 1-6.
- NN10083-911 - Communication Server 2000 Fault Management

Fault Mapping for XACore

The following criteria can be used for looking up information on specific faults for XACore.

Note: All XA-Core Logs are treated as INFO Events by the IEMS and are associated to the CS2000 Manager when the CS2000 Manager is configured in IEMS.

Fault Correlation for XACore

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
XACore	log name and log number	log name and log number	log name and log number	log name and log number	297-8991-510 - XA-Core Maintenance Manual

Northbound Fault Formats for XACore

SCC2

The following is an example of a XACore log in SCC2 format:

```
* 47 XAC 305 0114 FLT  RTIF (Reset Terminal Interface)
        DESCRIPTION: State has changed from INSV to SYSB by FAULT action
        PORT: Type State Site FL Row Bay    Shf/Slt/Pk/Pt   EqPEC/Serial
              RTIF SYSB  HOST 01 A00 DPCC:00 00 15R U  1 NTLX08AA/  NNTM17205KR8
        REASON:  Device Fault: RTIF IPC Protocol Error.
        FAULT RECORD ID: 880166C7
```

NTSTD

The following is an example of a XACore log in NTSTD format:

```
COMPACT06BT   *  XAC305 Feb15 00:47:43 0114 FLT  RTIF (Reset Terminal Interface)
```

```
DESCRIPTION: State has changed from INSV to SYSB by FAULT action
PORT: Type State Site FL Row Bay    Shf/Slt/Pk/Pt   EqPEC/Serial
      RTIF SYSB  HOST 01 A00 DPCC:00 00 15R U  1 NTLX08AA/  NNTM17205KR8
REASON:  Device Fault: RTIF IPC Protocol Error.
FAULT RECORD ID: 880166C7
```

SNMP

The following is an example of a XACore log in SNMP format:

```
sysUpTime. => 0:28:39
snmpTrapOID. => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.54.45.50.52.44.51.58.53.51.58.52.49.46.48.44.5248
alarmActiveDateAndTime => 2004-6-24,3:53:41.0
alarmActiveDescription => DeviceSpecificInfo=localTransmissionError;time: 2004 06 24
15 53 41
event: set
compId: EM MANTEO LP 3 SONET 2
severity: minor
faultcode: 70115203
alarmType: communications
commentData: Far end has raised a Line Remote Failure Indication alarm (rxRfiAlarm).
Check the operational attributes of the far-end.

nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => PPEM300
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m3.us.nortel.com-MDM-Mgr;EM MANTEO
LP 3 SONET 2
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1375

sysUpTime. => 0:28:47
snmpTrapOID. => nnExtAlarmMinor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.54.45.50.52.44.51.58.53.51.58.52.56.46.48.44.5249
alarmActiveDateAndTime => 2004-6-24,3:53:48.0
```

```
alarmActiveDescription => time: 2004 06 24 15 53 48
event: set
compId: EM MANTEO LP 3 SONET 2
severity: minor
faultcode: 70115210
alarmType: communications
commentData: Far end line: Entering unavailable state (10 consecutive SESs).
Check the provisioning or the hardware on the local and far end.

nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 12
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => PPEM300
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m3.us.nortel.com-MDM-Mgr;EM MANTEO
LP 3 SONET 2
nnExtAlarmActiveManualClear => 1
nnExtAlarmActiveSequenceNumber => 1376
```

Syslog

The following is an example of a XACore log in Syslog format:

```
Feb 14 19:47:43 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=9773~~  XAC305 MINOR FLT
RTIF (Reset Terminal Interface)^M         node CM      ^M        DESCRIPTION: State
has changed from INSV to SYSB by FAULT action^M        PORT: Type State Site FL Row
Bay    Shf/Slt/Pk/Pt   EqPEC/Serial^M              RTIF SYSB  HOST 01 A00 DPCC:00 00
15R U  1 NTLX08AA/  NNTM17205KR8^M        REASON:  Device Fault: RTIF IPC Protocol
Error.  ^M        FAULT RECORD ID: 880166C7
```

Performance

OM and PM Documentation references for XACore

- 297-8991-810 - XA-Core Reference Manual
- NN10149-711 - Communications Server 2000 Performance Management
- NN10264-709 - Carrier VoIP Performance Management Operational Measurements Reference, volumes 1-4

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

Performance measurements for XACore are available from the CS2K Core Manager. See NN10149-711 - Communications Server 2000 Performance Management for more information.

XML

The following is an example of Performance data for XACore in XML format:

Note: *The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of Performance data for XACore in CSV format:

Note: *The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for XACore

The XACore provides both command-line and MAP-based interfaces accessed through the CS2000 Core Manager.

GUI/CLUI Launching and User procedures

- NN10018-111 - CS2000 Core Manager Basics

  see section “Accessing the Core”

Related documents

- NN10448-111 - Communication Server 2000 Basics
- NN10171-611 - Communication Server 2000 Security and Administration
- NN10324-509 - Carrier VoIP Operational Configuration: Data Schema Reference, volumes 1-2
- NN10324-509 - Carrier VoIP Performance Management Operational Measurements Reference, volumes 1-4
- 297-8021-808P2 - DMS-100 SERVORD Reference Manual
- 297-8991-810 - XA-Core Reference Manual

Platforms

Core Manager Platform

This section contains IEMS Northbound log samples and device documentation references for the Core Manager Platform.

Core Manager Platform Fault Interface

Fault documentation for Core Manager Platform :

- NN10408-900 ATM/IP Solution-level Fault Management
- NN10082-911 CS2000 Core Manager Fault Management
- NN10351-911 Core and Billing Manager 850 Fault Management

Fault Mapping for Core Manager Platform

The following criteria can be used for looking up information on specific faults for Core Manager Platform.

Note: All SDM Logs are treated as INFO Events by the IEMS and are associated to the Core Manager when the Core Manager is configured in IEMS.

Fault Correlation for Core Manager Platform

NB format -> Device/EM	SCC2	NTSTD	Document Reference
AIX Platform	logname and number	logname and number	NN10082-911 CS2000 Core Manager Fault Management
SPFS	logname and number	logname and number	NN10351-911 Core and Billing Manager 850 Fault Management

Northbound Fault Formats for Core Manager Platform

SCC2

The following is an example of a Core Manager Platform log in SCC2 format:

```
* 52 2 317 0162 TBL
          node SDM       SDM Base Maintenance
        DCE problem detected
```

```
        Reason: SEC Master Server 47.142.94.49 is down.
```

NTSTD

The following is an example of a SDM Platform log in NTSTD format:

```
COMPACT06BT   *  SDM 317 Feb15 00:52:49 0162 TBL
         node SDM      SDM Base Maintenance
        DCE problem detected
        Reason: SEC Master Server 47.142.94.49 is down.

SEC Master Server 47.142.94.49 is down.
```

Performance

OM and PM Documentation references for Core Manager Platform

- NN10148-700 CS2000 Core Manager Performance Management
- NN10361-711 Core and Billing Manager 850 Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for Core Manager Platform in XML format:

Note: *The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of performance data for Core Manager Platform in CSV format:

Note: *The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for Core Manager Platform

Core Manager Platform has a command line user interface that can be accessed via a secure shell.

GUI/CLUI Launching and User procedures

- NN10104-511 CS2000 Core Manager Configuration Management

Related documents

- NN10018-111 CS2000 Core Manager Basics
- NN10126-811 CS2000 Core Manager Accounting
- NN10170-611 CS2000 Core ManagerSecurity and Administration
- NN10355-111 Core and Billing Manager 850 Basics
- NN10363-811 Core and Billing Manager 850 Accounting
- NN10358-611 Core and Billing Manager 850 Security and Administration

Succession Server Platform Foundation Software (SSPFS)

This section contains IEMS Northbound log samples and device documentation references for the SSPFS platform.

SSPFS Fault Interface

Fault documentation for SSPFS

- NN10440-450 - Upgrading a Carrier VoIP Network

Fault Mapping for SSPFS

The following criteria can be used for looking up information on specific faults for SSPFS.

Fault Correlation for SSPFS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
SSPFS	logname and number	logname and number	logname and number	logname and number	NN10440-450 Upgrading a Carrier VoIP Network

Northbound Fault Formats for SSPFS

The SSPFS SNMP interface is not implemented yet.

SCC2

The following is an example of a SSPFS log in SCC2 format:

Not available at time of publication

NTSTD

The following is an example of a SSPFS log in NTSTD format:

Not available at time of publication

SNMP

The following is an example of a SSPFS log in SNMP format:

Not available at time of publication

Syslog

The following is an example of a SSPFS log in Syslog format:

Not available at time of publication

Performance

OM and PM Documentation references for SSPFS

The SSPFS platform does not generate and OMs or PMs, but it does collect such information from other network elements. For more information see:

- NN10276-500 - ATM/IP Configuration Management (Configuration of SNMP Poller)
- Upgrading a Carrier VoIP Network, NN10440-450.

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for SSPFS platform in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-12-14T13:20:20EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity Type="SSPFS">
<EntityId>47.142.106.220</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry</TableId>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<Labels>
<Label>ipAdEntAddr</Label>
<Label>ipAdEntIfIndex</Label>
<Label>ipAdEntNetMask</Label>
<Label>ipAdEntBcastAddr</Label>
<Label>ipAdEntReasmMaxSize</Label>
</Labels>
```

```
<RowOfValues>
<RowValue>
<Value>47.142.106.222</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>47.142.106.220</Value>
</RowValue>
<RowValue>
<Value>2</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>192.168.47.1</Value>
</RowValue>
<RowValue>
<Value>5</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>127.0.0.1</Value>
</RowValue>
<RowValue>
<Value>6</Value>
</RowValue>
<RowValue>
<Value>255.0.0.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
```

```
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>47.142.106.224</Value>
</RowValue>
<RowValue>
<Value>4</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>47.142.106.223</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
<RowValue>
<Value>255.255.255.0</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>65535</Value>
</RowValue>
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="5">
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInUnknownProtos</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipFragCreates</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>418461</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipOutRequests</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>19623971</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInDelivers</MeasureId>
```

```
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>21482658</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipOutNoRoutes</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipDefaultTTL</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>255</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipReasmReqds</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>137693</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInHdrErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipReasmFails</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipForwDatagrams</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipFragFails</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInDiscards</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipOutDiscards</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
```

```
<Value>4</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipForwarding</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>2</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipReasmTimeout</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>60</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInReceives</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>17207338</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipReasmOKs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>137693</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipRoutingDiscards</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipInAddrErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:00EST</CaptureTime>
<MeasureId>ipFragOKs</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.mgmt.mib-2.ip</MeasureSuppId1>
<Value>138590</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfInErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsSystemProcessTime</MeasureId>
```

```
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfCollisions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsDiskXfer1</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVSwapIn</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsDiskXfer3</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVIntr</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVPagesIn</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfOutPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsNiceModeTime</MeasureId>
```

```
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfOutErrors</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIdleModeTime</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVPagesOut</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsDiskXfer2</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsVSwapOut</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsDiskXfer4</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsIfInPackets</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-14T13:20:01EST</CaptureTime>
<MeasureId>rsUserProcessTime</MeasureId>
```

```
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf
</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
</PMFile>
```

CSV

The following is an example of performance data for SSPFS platform in CSV format:

```
PMFile=Begin

MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime

PM,commonFormat.xsd,2005-03-17T10:25:00EST


System=Begin

SystemId

NortelNetworks/IEMS


Entity=Begin

EntityId,Type

47.142.128.112,SSPFS


Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry,Snapshot,5,2005-03-
17T10:25:00EST

Label,Label,Label,Label,Label

ipAdEntAddr,ipAdEntIfIndex,ipAdEntNetMask,ipAdEntBcastAddr,ipAdEntReasmMaxSize

Value,Value,Value,Value,Value

47.142.128.112,1,255.255.255.128,1,65535

127.0.0.1,3,255.0.0.0,1,65535

47.142.128.115,2,255.255.255.128,1,65535

Table=End



SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5
```

```
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

ipInUnknownProtos,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipFragCreates,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipOutRequests,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-
2.ip,3525617,Valid

ipInDelivers,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-
2.ip,21811895,Valid

ipOutNoRoutes,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipDefaultTTL,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,255,Valid

ipReasmReqds,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipInHdrErrors,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipReasmFails,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipForwDatagrams,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipFragFails,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipInDiscards,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipOutDiscards,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipForwarding,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,2,Valid

ipReasmTimeout,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,60,Valid

ipInReceives,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-
2.ip,4673901,Valid

ipReasmOKs,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipRoutingDiscards,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipInAddrErrors,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

ipFragOKs,2005-03-17T10:25:00EST,.iso.org.dod.internet.mgmt.mib-2.ip,0,Valid

rsIfInErrors,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsSystemProcessTime,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsIfCollisions,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsDiskXfer1,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsVSwapIn,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsDiskXfer3,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsVIntr,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid
```

```
rsVPagesIn,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsIfOutPackets,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsNiceModeTime,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsIfOutErrors,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsIdleModeTime,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsVPagesOut,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsDiskXfer2,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsVSwapOut,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsDiskXfer4,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsIfInPackets,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

rsUserProcessTime,2005-03-
17T10:25:00EST,.iso.org.dod.internet.private.enterprises.sun.sunMib.sunHostPerf,0,Va
lid

SingleValues=End


Entity=End


System=End


PMFile=End
```

GUI/CLUI Documentation for SSPFS

GUI Launching and User procedures

- NN10276-500 - ATM/IP Configuration Management

  Note: Contains information on the SSPFS CLI interface

Related documents

- NN10281-600 - ATM/IP Administration and Security

Element Managers

CS2000 Core Manager

This section contains IEMS Northbound log samples and device documentation references for the CS2K Core Manager.

CS2K Core Manager Fault Interface

Fault documentation for CS2000 Core Manager :

- NN10275-909 - Carrier VoIP Fault Management Logs Reference
- NN10082-911 - CS 2000 Core Manager Fault Management

Fault Mapping for CS2000 Core Manager

The following criteria can be used for looking up information on specific faults for CS2000 Core Manager.

Fault Correlation for CS2000 Core Manager

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
CS2000 Core Manager	log name and number	log name and number	log name and number	log name and number	NN10275-909 Carrier VoIP Fault Management Logs Reference NN10082-911 CS 2000 Core Manager Fault Management

Northbound Fault Formats for CS2000 Core Manager

SCC2

The following is an example of a CS2000 Core Manager log in SCC2 format:

```
* 06 SDM 550 1506 INFO Node Status Change
        Node:   SDM 0
        Status:  ** ISTb      from  ** ISTb
        Reason: Application alarm set. SDM_ETA.eta
```

NTSTD

The following is an example of a CS2000 Core Manager log in NTSTD format:

```
COMPACT506BT   * SDM550 Feb15 03:07:00 1520 INFO Node Status Change
        Node:   SDM 0
       Status:     InSv      from   * ISTb
       Reason: Application alarm cleared. SDM_ETA.eta
```

SNMP

The following is an example of a CS2000 Core Manager log in SNMP format:

```
sysUpTime. => 1 day, 19:19:26
snmpTrapOID. => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr;
nnExtAlarmMessageDateAndTime => 2004-6-9,3:4:9.1
nnExtAlarmMessageDocumentationPointer => PM  610
nnExtAlarmMessageInfo =>  04 PM  610 3352 INFO ABI XPM C-side Link State Change

        Node: SMA2 0     Link: 0   Plane: 0   Port: 0

        From: SYSB   To: INSV

        Reason: Link opened by MG9K/ABI

sysUpTime.0 => 1 day, 19:19:27
snmpTrapOID.0 =>
alarmActiveResourceId => .0.0
alarmActiveDateAndTime => 2004-6-9,3:4:9.3
alarmActiveDescription => DeviceSpecificInfo=Unavailable;
Node:   SDM 0
Status:  ** ISTb      from  ** ISTb
Reason: Application alarm set. SDM_ETA.eta
```

Syslog

The following is an example of a CS2000 Core Manager log in Syslog format:

```
Feb 14 22:06:01 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=1165~~  SDM550 MINOR INFO
Node Status Change^M         node CM      ^M        Node:   SDM 0^M        Status:  **
ISTb      from  ** ISTb     ^M        Reason: Application alarm set. SDM_ETA.eta
```

Performance

OM and PM Documentation references for CS2000 Core Manager

- NN10148-711 - CS 2000 Core Manager Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for CS2000 Core Manager in XML format:

Note: *Northbound performance interface not supported for this component.*

CSV

The following is an example of performance data for CS2000 Core Manager in CSV format:

Note: *Northbound performance interface not supported for this component.*

GUI/CLUI Documentation for CS2000 Core Manager

The CS2000 Core Manager provides both command-line and MAP-based interfaces.

GUI/CLUI Launching and User procedures

- NN10018-111 - CS2000 Core Manager Basics

Related documents

- NN10060-461 - Upgrading the CS 2000 Core Manager
- NN10082-911 - CS 2000 Core Manager Fault Management
- NN10104-511 - CS 2000 Core Manager Configuration Management
- NN10126-811 - CS 2000 Core Manager Accounting

- NN10170-611 - CS 2000 Core Manager Administration and Security

Centrex IP Call Manager (CICM Manager)

This section contains IEMS Northbound log samples and device documentation references for the CICM Manager.

CICM Fault Interface

Fault documentation for CICM Manager:

- NN10334-911 - IEMS Fault Management

Fault Mapping for CICM Manager

The following criteria can be used for looking up information on specific faults for CICM Manager.

Fault Correlation for CICM Manager

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
CICM Mgr	logname and number	logname and number	logname and number	logname and number	NN10334-911 - IEMS Fault Management

Northbound Fault Formats for CICM Manager

SCC2

The following is an example of a CICM Manager log in SCC2 format:

```
?
  44 IEMS399 0011 FLT  Communication Regained
        Location: 47.142.106.223
        NotificationID: 0
        State: Cleared
        Category: Communications
        Time: Jun 30 15:44:06 2004
        ComponentId: 47.165.168.74-CICM-Mgr_Card_B
        Description: IEMS regained communication with the managed device
```

```
?
*C44 IEMS398 0012 FLT  Communication Lost
        Location: 47.142.106.223
        NotificationID: 0
        State: Raised
        Category: Communications
        Cause: Communications subsystem failure
        Time: Jun 30 15:44:15 2004
        ComponentId: 47.165.168.74-CICM-Mgr_Card_B
        Specific Problem: Connection Lost
        Description: IEMS Unable to communicate with managed device
```

NTSTD

The following is an example of a CICM Manager log in NTSTD format:

```
test     IEMS399 JUN30 15:44:06 0011 FLT  Communication Regained
        Location: 47.142.106.223
        NotificationID: 0
        State: Cleared
        Category: Communications
        Time: Jun 30 15:44:06 2004
        ComponentId: 47.165.168.74-CICM-Mgr_Card_B
        Description: IEMS regained communication with the managed device


test *** IEMS398 JUN30 15:44:15 0012 FLT  Communication Lost
        Location: 47.142.106.223
        NotificationID: 0
        State: Raised
        Category: Communications
        Cause: Communications subsystem failure
        Time: Jun 30 15:44:15 2004
        ComponentId: 47.165.168.74-CICM-Mgr_Card_B
        Specific Problem: Connection Lost
        Description: IEMS Unable to communicate with managed device
```

SNMP

The following is an example of a CICM Manager log in SNMP format:

```
sysUpTime. => 19:40:37

snmpTrapOID. => nnExtAlarmMajor

alarmActiveResourceId =>

.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.
20.50.48

.48.52.45.54.45.50.57.44.49.48.58.50.57.58.48.46.52.44.11925

alarmActiveDateAndTime => 2004-6-29,10:29:0.4

alarmActiveDescription => DeviceSpecificInfo=softwareProgramError(48);Backup
Fail

nnExtAlarmActiveEventType => 4

nnExtAlarmActiveProbableCause => 1024

nnExtAlarmActiveAdditionalText => Scheduled/on-demand backup failed during
last iteration.

nnExtAlarmActiveDocumentationPointer => CICM341

nnExtAlarmActiveResourceDescription => IEMS=47.142.86.95-CICM-
Mgr_Card_A;CICM=CICMEM-000-A;NodeType=Platform

nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a CICM Manager log in Syslog format:

```
Jun 30 15:44:06 2004      ComponentId: 47.165.168.74-CICM-Mgr_Card_B      Description:
IEMS regained communication with the managed device

Jun 30 15:44:15 znc0s0tm IEMS: _V2_~I=~H=znc0s0tm~A=IEMS~S=6162~~ IEMS398 CRIT FLT
Communication Lost       Location: 47.142.106.223       NotificationID: 0       State:
Raised      Category: Communications      Cause: Communications subsystem failure
Time:

Jun 30 15:44:15 2004       ComponentId: 47.165.168.74-CICM-Mgr_Card_B       Specific
Problem: Connection Lost        Description: IEMS Unable to communicate with managed
device
```

Performance

OM and PM Documentation references for CICM Manager

- NN10327-711 - IEMS Performance Management

Northbound OM/PM Formats

Performance measurements for CICM Manager are available only from the CICM Manager interface. See NN10327-711 - IEMS Performance Management for more information.

XML

The following is an example of Performance data for CICM Manager in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
- <PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-06-23T13:36:04EST</FileCreationTime>
- <System>
<SystemId>NortelNetworks/IEMS</SystemId>
- <Entity Type="CICM Mgr">
<EntityId>47.165.168.120</EntityId>
- <Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry</TableId>
<CaptureTime>2004-06-23T13:35:01EST</CaptureTime>
- <Labels>
<Label>usrHistoryControlInterval</Label>
<Label>usrHistoryControlIndex</Label>
<Label>usrHistoryControlStatus</Label>
<Label>usrHistoryControlOwner</Label>
</Labels>
- <RowOfValues>
- <RowValue>
<Value>900</Value>
</RowValue>
- <RowValue>
<Value>5</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>CICM-120A</Value>
</RowValue>
</RowOfValues>
</Table>
- <Table MeasurementKind="Snapshot" IntervalDuration="5">
<TableId>.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry</TableId>
```

<CaptureTime>2004-06-23T13:35:58EST</CaptureTime>

- <Labels>

<Label>usrHistoryControlInterval</Label>

<Label>usrHistoryControlIndex</Label>

<Label>usrHistoryControlStatus</Label>

<Label>usrHistoryControlOwner</Label>

</Labels>

- <RowOfValues>

- <RowValue>

<Value>900</Value>

</RowValue>

- <RowValue>

<Value>5</Value>

</RowValue>

- <RowValue>

<Value>1</Value>

</RowValue>

- <RowValue>

<Value>CICM-120A</Value>

</RowValue>

</RowOfValues>

</Table>

- <Table MeasurementKind="**Snapshot**" IntervalDuration="**5**">

<TableId>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry</TableId>

<CaptureTime>2004-06-23T13:35:02EST</CaptureTime>

- <Labels>

<Label>nnPerfMetricValue</Label>

<Label>nnPerfMetricSources</Label>

<Label>nnPerfMetricDataType</Label>

<Label>nnPerfMetricGroup</Label>

<Label>nnPerfMetricName</Label>

<Label>nnPerfMetricRefIndex</Label>

</Labels>

- <RowOfValues>

- <RowValue>

<Value>0</Value>

</RowValue>

- <RowValue>

```
<Value>2</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>CICM</Value>
</RowValue>
- <RowValue>
<Value>ActiveConnections</Value>
</RowValue>
- <RowValue>
<Value>5</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>0</Value>
</RowValue>
- <RowValue>
<Value>2</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>CICM</Value>
</RowValue>
- <RowValue>
<Value>PercentageCpuUsed</Value>
</RowValue>
- <RowValue>
<Value>4</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>0</Value>
```

```
</RowValue>
- <RowValue>
<Value>2</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>CICM</Value>
</RowValue>
- <RowValue>
<Value>PercentageMemoryUsed</Value>
</RowValue>
- <RowValue>
<Value>3</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
- <RowValue>
<Value>0</Value>
</RowValue>
- <RowValue>
<Value>2</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>CICM</Value>
</RowValue>
- <RowValue>
<Value>NumberOfLogs</Value>
</RowValue>
- <RowValue>
<Value>2</Value>
</RowValue>
</RowOfValues>
- <RowOfValues>
```

```
- <RowValue>
<Value>0</Value>
</RowValue>
- <RowValue>
<Value>2</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
- <RowValue>
<Value>CICM</Value>
</RowValue>
- <RowValue>
<Value>ActiveSessions</Value>
</RowValue>
- <RowValue>
<Value>1</Value>
</RowValue>
</RowOfValues>
</Table>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for CICM Manager in CSV.

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-29T15:30:02EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
47.165.168.252,CICM Mgr
```

```
Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.mgmt.mib-
2.rmon.usrHistory.usrHistoryControlTable.usrHistoryControlEntry,Snapshot,5,2005-03-
29T15:30:00EST

Label,Label,Label,Label

usrHistoryControlIndex,usrHistoryControlInterval,usrHistoryControlOwner,usrHistoryCo
ntrolStatus

Value,Value,Value,Value

9,900,CICMEM-070-B,1

Table=End



Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelPerfRefMIB.
nnPerfMetricReferenceTable.nnPerfMetricReferenceEntry,Snapshot,5,2005-03-
29T15:30:01EST

Label,Label,Label,Label,Label,Label

nnPerfMetricRefIndex,nnPerfMetricName,nnPerfMetricGroup,nnPerfMetricDataType,nnPerfM
etricSources,nnPerfMetricValue

Value,Value,Value,Value,Value,Value

9,TransmittedBytesPerSecond,CICM,1,2,0

8,ReceivedBytesPerSecond,CICM,1,2,0

7,LoggedInUsers,CICM,1,2,0

6,HalfCallAttempts,CICM,1,2,0

5,ActiveConnections,CICM,1,2,0

4,PercentageCpuUsed,CICM,1,2,1

3,PercentageMemoryUsed,CICM,1,2,18

2,NumberOfLogs,CICM,1,2,0

1,ActiveSessions,CICM,1,2,0

Table=End


Entity=End


System=End


PMFile=End
```

GUI/CLUI Documentation for CICM Manager

GUI Launching and User procedures

Related documents

GWC Manager

This section contains IEMS Northbound log samples and device documentation references for the GWC Manager.

GWC Manager Fault Interface

Fault documentation for GWC Mgr :

- NN10408-900 - ATM/IP Solution-level Fault Management
- NN10202-911 - Gateway Controller Fault Management

Fault Mapping for GWC Mgr

The following criteria can be used for looking up information on specific faults for GWC Mgr.

Fault Correlation for GWC Mgr

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
GWC Mgr	logname and number	logname and number	logname and number	logname and number	NN10408-900 - ATM/IP Solution-level Fault Management

Northbound Fault Formats for GWC Mgr

SCC2

The following is an example of a GWC Mgr log in SCC2 format:

```
*C14 CMT 301 7248 TBL  CMT Fault
        Location: gwcem
        NotificationID: 700
        State: Raise
```

```
        Category: Processing Error
        Cause: Corrupt data
        Time: Jan 23 15:14:38 2004
        Component Id: SESM=GWCEMalarm;GWCEM=Recovery;GWC=GWC-2-UNIT-0
        Specific Problem: FTP Problem
        Description: Problem detected in GWC Recovery Subsystem
```

NTSTD

The following is an example of a GWC Mgr log in NTSTD format:

```
COMPACT06BT ***  CMT301 Jan23 20:14:38 7248 TBL  CMT Fault
        Location: gwcem
        NotificationID: 700
        State: Raise
        Category: Processing Error
        Cause: Corrupt data
        Time: Jan 23 15:14:38 2004
        Component Id: SESM=GWCEMalarm;GWCEM=Recovery;GWC=GWC-2-UNIT-0
        Specific Problem: FTP Problem
        Description: Problem detected in GWC Recovery Subsystem
```

SNMP

The following is an example of a GWC Mgr log in SNMP format:

```
system.sysUpTime.0 => 23:10:15
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.
20.50.48
.48.52.45.49.45.50.51.44.51.58.49.52.58.51.56.46.48.44.42847
alarmActiveDateAndTime => 2004-1-23,3:14:38.0,
alarmActiveDescription => DeviceSpecificInfo=lANError;GWC is inaccessible
from GWCEM
nnExtAlarmActiveEventType => 2
nnExtAlarmActiveProbableCause => 1024
nnExtAlarmActiveAdditionalText => GWCEM fail to ping both GWC units of GWC-50
nnExtAlarmActiveDocumentationPointer => CMT301
```

```
nnExtAlarmActiveResourceDescription =>IEMS=rtp4cmt-GWC-
Mgr;SESM=GWCEMalarm;GWCEM=DeviceInAccessible;GWC=GWC-50-UNIT-0

nnExtAlarmActiveManualClear => 0

nnExtAlarmActiveSequenceNumber => 9027
```

Syslog

The following is an example of a GWC Mgr log in Syslog format:

```
Feb 23 15:15:56 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7305~~  CMT301 CRIT TBL  CMT
Fault^M       Location: gwcem^M       NotificationID: 700^M       State: Raise^M
Category: Processing Error^M       Cause: Corrupt data^M       Time: Jan 23 15:14:38
2004^M       Component Id: SESM=GWCEMalarm;GWCEM=Recovery;GWC=GWC-2-UNIT-0^M
Specific Problem: FTP Problem^M       Description: Problem detected in GWC Recovery
Subsystem^M
```

Performance

OM and PM Documentation references for GWC Mgr

GWC Mgr has no operational or performance measurements.

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for GWC Mgr in XML format:

Note: *Northbound performance interface not supported for this component.*

CSV

The following is an example of performance data for GWC Mgr in CSV format:

Note: *Northbound performance interface not supported for this component.*

GUI/CLUI Documentation for GWC Mgr

GUI Launching and User procedures

- NN10409-500 - ATM/IP Solution-level Configuration Management

- NN10402-600 - ATM/IP Solution-level Administration and Security
- NN10408-900 - ATM/IP Solution-level Fault Management

Related documents

Integrated Element Management System (IEMS)

This section contains IEMS Northbound log samples and device documentation references for the IEMS.

IEMS Fault Interface

Fault documentation for IEMS :

- NN10275-909v3: Carrier VoIP Fault Management Logs Reference Vol. 3
- NN10334-911: IEMS Fault Management

Fault Mapping for IEMS

The following criteria can be used for looking up information on specific faults for IEMS.

Fault Correlation for IEMS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
IEMS	Log name and log number (Log Names: EMSS, IEMS, EMJS)	Log name and log number (Log Names: EMSS, IEMS, EMJS)	Log name and log number (Log Names: EMSS, IEMS, EMJS)	Log name and log number (Log Names: EMSS, IEMS, EMJS)	See references listed above.

Northbound Fault Formats for IEMS

SCC2

The following is an example of a IEMS log in SCC2 format:

Sample Raise:

*C55 IEMS398 0006 FLT Communication Lost
Location: 47.142.94.68
NotificationID: 0
State: Raised
Category: Communications
Cause: Communications subsystem failure

Time: Dec 13 13:55:15 2004
ComponentId: znc0s0jh-SSPFS-Unit-0
Specific Problem: Connection Lost
Description: IEMS Unable to communicate with managed device

Sample Clear:

55 IEMS399 0007 FLT Communication Regained
Location: 47.142.94.68
NotificationID: 0
State: Cleared
Category: Communications
Time: Dec 13 13:55:22 2004
ComponentId: znc0s0jh-SSPFS-Unit-0
Description: IEMS regained communication with the managed device

NTStd

The following is an example of a IEMS log in NTStd format:

Sample Raise:

office_name *** IEMS398 DEC13 13:55:15 0006 FLT Communication Lost
Location: 47.142.94.68
NotificationID: 0
State: Raised
Category: Communications
Cause: Communications subsystem failure
Time: Dec 13 13:55:15 2004
ComponentId: znc0s0jh-SSPFS-Unit-0
Specific Problem: Connection Lost
Description: IEMS Unable to communicate with managed device

Sample Clear:

office_name IEMS399 DEC13 13:55:22 0007 FLT Communication Regained
Location: 47.142.94.68
NotificationID: 0
State: Cleared
Category: Communications
Time: Dec 13 13:55:22 2004
ComponentId: znc0s0jh-SSPFS-Unit-0
Description: IEMS regained communication with the managed device

SNMP

The following is an example of a IEMS log in SNMP format:

Sample Raise:

system.sysUpTime.0 => 7:01:55
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.49.50.45.49.51.44.50.58.52.58.56.46.51.44.649
alarmActiveDateAndTime => 2004-12-13,2:4:8.3,
alarmActiveDescription => IEMS Unable to communicate with managed device
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 6
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => IEMS398
nnExtAlarmActiveResourceDescription => IEMS=IEMS-Mgr;znc0s0jh-SSPFS-Unit-0
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 7

Sample Clear:

system.sysUpTime.0 => 7:01:55
snmpTrapOID.0 => nnExtAlarmClear
alarmActiveResourceId =>
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48.48.52.45.49.50.45.49.51.44.50.58.52.5
8.50.50.46.48.44.649
alarmActiveDateAndTime => 2004-12-13,2:4:22.0,
alarmActiveDescription => DeviceSpecificInfo=;IEMS regained communication with the managed
device
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => IEMS399
nnExtAlarmActiveResourceDescription => IEMS=IEMS-Mgr;znc0s0jh-SSPFS-Unit-0
nnExtAlarmActiveSequenceNumber => 8

Syslog

The following is an example of a IEMS log in Syslog format:

Sample Raise:

Dec 13 13:55:15 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=4093~~ IEMS398 CRIT FLT Communication Lost^M Location: 47.142.94.68^M NotificationID: 0^M State: Raised^M Category: Communications^M Cause: Communications subsystem failure^M Time: Dec 13 13:55:15 2004^M ComponentId: znc0s0jh-SSPFS-Unit-0^M Specific Problem: Connection Lost^M Description: IEMS Unable to communicate with managed device

Sample Clear:

Dec 13 13:55:22 znc0s0jh IEMS: _V2_~I=~H=znc0s0jh~A=IEMS~S=4094~~ IEMS399 NONE FLT Communication Regained^M Location: 47.142.94.68^M NotificationID: 0^M State: Cleared^M Category: Communications^M Time: Dec 13 13:55:22 2004^M ComponentId: znc0s0jh-SSPFS-Unit-0^M Description: IEMS regained communication with the managed device

Performance

OM and PM Documentation references for IEMS

- NN10327-711 IEMS Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for IEMS in XML format:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<PMFile xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="commonFormat.xsd" MeasurementCategory="PM">
<FileCreationTime>2004-12-13T13:06:04EST</FileCreationTime>
<System>
<SystemId>NortelNetworks/IEMS</SystemId>
<Entity Type="IEMS">
<EntityId>47.142.94.68</EntityId>
<Table MeasurementKind="Snapshot" IntervalDuration="30">
<TableId>fiveMinCollectionJobTable</TableId>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<Labels>
<Label>fiveMinCollectionJobID</Label>
<Label>fiveMinCollectionJobName</Label>
<Label>fiveMinCollectionJobStartTime</Label>
<Label>fiveMinCollectionJobExecutionTime</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>storm_collect</Value>
</RowValue>
<RowValue>
<Value>1102961130856</Value>
</RowValue>
```

```
<RowValue>
<Value>4586</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind=”Snapshot” IntervalDuration=”30”>
<TableId>thirtyMinCollectionJobTable</TableId>
<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>
<Labels>
<Label>thirtyMinCollectionJobID</Label>
<Label>thirtyMinCollectionJobName</Label>
<Label>thirtyMinCollectionJobStartTime</Label>
<Label>thirtyMinCollectionJobExecutionTime</Label>
</Labels>
<RowOfValues>
<RowValue>
<Value>1</Value>
</RowValue>
<RowValue>
<Value>iems_collect</Value>
</RowValue>
<RowValue>
<Value>1102961120556</Value>
</RowValue>
<RowValue>
<Value>2621</Value>
</RowValue>
</RowOfValues>
</Table>
<Table MeasurementKind=”Snapshot” IntervalDuration=”30”>
<TableId>tableSpaceTable</TableId>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<Labels>
<Label>tableSpaceName</Label>
<Label>usedTableSpaceInBytes</Label>
<Label>usedTableSpaceInPercent</Label>
</Labels>
<RowOfValues>
```

```
<RowValue>
<Value>IEMS_TS</Value>
</RowValue>
<RowValue>
<Value>18808832</Value>
</RowValue>
<RowValue>
<Value>3</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>IEMS_EVENT_TS</Value>
</RowValue>
<RowValue>
<Value>5963776</Value>
</RowValue>
<RowValue>
<Value>1</Value>
</RowValue>
</RowOfValues>
<RowOfValues>
<RowValue>
<Value>IEMS_PERF_TS</Value>
</RowValue>
<RowValue>
<Value>1835008</Value>
</RowValue>
<RowValue>
<Value>0</Value>
</RowValue>
</RowOfValues>
</Table>
<SingleValues MeasurementKind="Snapshot" IntervalDuration="30">
<SingleValue>
<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>
<MeasureId>systemRestartCount</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.system</MeasureSuppId1>
```

<Value>3</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>numOfActiveClients</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.client</MeasureSuppId1>

<Value>3</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>numOfEventsFromUnknownCustlogDevices</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>eventQueueSize</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>numOfEventsFromUnknownSNMPDevices</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>avgEventThroughputRate</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>numOfEventsFromUnknownDevices</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:50EST</CaptureTime>

<MeasureId>maxEventThroughputRate</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfDiscardedEvents</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfEvents</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>

<Value>6060</Value>

<Reliability>Valid</Reliability>

</SingleValue>

```
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfEventsAdded</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event</MeasureSuppId1>
<Value>5</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfAlarmsCleared</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSuppId1>
<Value>2</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfMajorAlarms</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSuppId1>
<Value>27</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfWarningAlarms</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSuppId1>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>
<MeasureId>numOfCriticalAlarms</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSuppId1>
```

<Value>48</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfAlarmsAdded</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfMinorAlarms</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSuppId1>

<Value>7</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfActiveAlarms</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms</MeasureSuppId1>

<Value>82</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfDBCleanUpPolicyExecutions</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.database</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfAttributesCollected</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSuppId1>

<Value>4146</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfReportsJobsProvisioned</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:53EST</CaptureTime>

<MeasureId>numOfTransferJobsProvisioned</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOfCollectionJobsProvisioned</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOfAttributesCollectedOverThisInterval</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSuppId1>

<Value>3342</Value>

<Reliability>Valid</Reliability>

```
</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOfFailedReportJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance</MeasureSupp
Id1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf24HrSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf30MinSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>

<Value>1</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf12HrSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCo
llectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf15MinSuccessfulJobs</MeasureId>
```

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf60MinSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf5MinSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCollectionJobs</MeasureSuppId1>

<Value>1</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf15MinPartialSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf60MinPartialSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSuccessfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

```
<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf5MinPartialSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf24HrPartialSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf30MinPartialSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf12HrPartialSuccessfulJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucce
ssfulCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf24HrFailedCollectionJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollec
tionJobs</MeasureSuppId1>
```

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf30MinFailedCollectionJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf12HrFailedCollectionJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf15MinFailedCollectionJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf60MinFailedCollectionJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:54EST</CaptureTime>

<MeasureId>numOf5MinFailedCollectionJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollectionJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOf24HrFailedTransferJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOf30MinFailedTransferJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOf12HrFailedTransferJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOf15MinFailedTransferJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransferJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

```
</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOf60MinFailedTransferJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransf
erJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOf5MinFailedTransferJobs</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransf
erJobs</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfManagedObjects</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>

<Value>47</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfDevicesInUnManagedState</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>

<Value>3</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfAddedManagedObjects</MeasureId>
```

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfDevicesInUnKnownState</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1>

<Value>8</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfUnKnownDeviceStateTransistions</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfdeletedManagedObjects</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

<SingleValue>

<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>

<MeasureId>numOfThrottledDeviceStateTransistions</MeasureId>

<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.nortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1>

<Value>0</Value>

<Reliability>Valid</Reliability>

</SingleValue>

```
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfDevicesInThrottledState</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfSystemUnManagedDeviceStateTransistions</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
<SingleValue>
<CaptureTime>2004-12-13T13:05:55EST</CaptureTime>
<MeasureId>numOfDevicesInSystemUnManagedState</MeasureId>
<MeasureSuppId1>.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.n
ortelNetworkManagementInterfaceMIBs.operationalMeasurements.topology</MeasureSuppId1
>
<Value>0</Value>
<Reliability>Valid</Reliability>
</SingleValue>
</SingleValues>
</Entity>
</System>
</PMFile>
```

CSV

The following is an example of Performance data for IEMS in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-17T13:00:02EST

System=Begin
```

```
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
47.142.128.115,IEMS

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
fiveMinCollectionJobTable,Snapshot,5,2005-03-17T13:00:02EST
Label,Label,Label,Label
fiveMinCollectionJobID,fiveMinCollectionJobName,fiveMinCollectionJobStartTime,fiveMi
nCollectionJobExecutionTime
Value,Value,Value,Value
1,IEMS5minCollection,1111082100898,2233
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
tableSpaceTable,Snapshot,5,2005-03-17T13:00:01EST
Label,Label,Label
tableSpaceName,usedTableSpaceInBytes,usedTableSpaceInPercent
Value,Value,Value
IEMS_TS,45875200,44
IEMS_EVENT_TS,134610944,16
IEMS_PERF_TS,13238272,2
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
fiveMinTransferJobTable,Snapshot,5,2005-03-17T13:00:02EST
Label,Label,Label,Label
fiveMinTransferJobID,fiveMinTransferJobName,fiveMinTransferJobStartTime,fiveMinTrans
ferJobExecutionTime
Value,Value,Value,Value
1,IEMS5minTransfer,1111082103882,453
Table=End
```

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
deviceEventRateTable,Snapshot,5,2005-03-17T13:00:01EST
Label,Label,Label,Label
deviceID,deviceName,eventRate,eventRateDetails
Value,Value,Value,Value
3,rtpo-mg9kem.us.nortel.com-MG9K-Mgr_7.0,0,106 events received in 298170
milliseconds.
2,wnc0s0pe.us.nortel.com-MG9K-Mgr_9.0,0,14 events received in 298170 milliseconds.
1,SYSLOG,0,6 events received in 298170 milliseconds.
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
fiveMinReportJobTable,Snapshot,5,2005-03-17T13:00:02EST
Label,Label,Label,Label
fiveMinReportJobID,fiveMinReportJobName,fiveMinReportJobStartTime,fiveMinReportJobEx
ecutionTime
Value,Value,Value,Value
1,IEMS5minReport,1111082100898,733
Table=End


SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
systemRestartCount,2005-03-
17T13:00:00EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.system,2,Valid
numOfActiveClients,2005-03-
17T13:00:00EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.client,6,Valid
numOfEventsFromUnknownCustlogDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,6,Valid
eventQueueSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid
```

```
numOfEventsFromUnknownSNMPDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

avgEventThroughputRate,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEventsFromUnknownDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,6,Valid

maxEventThroughputRate,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,2,Valid

numOfDiscardedEvents,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEvents,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,150735,Valid

numOfEventsAdded,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,137,Valid

numOfAlarmsCleared,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,73,Valid

numOfMajorAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,263,Valid

numOfWarningAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,75,Valid

numOfCriticalAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,36,Valid

numOfAlarmsAdded,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,47,Valid

numOfMinorAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,74,Valid

numOfActiveAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,448,Valid

numOfDBCleanUpPolicyExecutions,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.database,1,Valid

applicationHeapSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.memory,101923064,Valid

maxApplicationHeapSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.memory,139169296,Valid
```

```
numOfAttributesCollected,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,19411,Valid

numOfReportsJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfTransferJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfCollectionJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfAttributesCollectedOverThisInterval,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,176,Valid

numOfFailedReportJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOf24HrSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf30MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf12HrSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf15MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf60MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf5MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,1,Valid

numOf15MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf60MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf5MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
```

```
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf24HrPartialSuccessfulJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf30MinPartialSuccessfulJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf12HrPartialSuccessfulJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf24HrFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf30MinFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf12HrFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf15MinFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf60MinFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf5MinFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf24HrFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf30MinFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf12HrFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf15MinFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
```

```
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf60MinFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf5MinFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOfManagedObjects,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,345,Valid

numOfDevicesInUnManagedState,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,4,Valid

numOfAddedManagedObjects,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInUnKnownState,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,9,Valid

numOfUnKnownDeviceStateTransistions,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfdeletedManagedObjects,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfThrottledDeviceStateTransistions,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInThrottledState,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfSystemUnManagedDeviceStateTransistions,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInSystemUnManagedState,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

SingleValues=End
```

GUI/CLUI Documentation for IEMS

GUI Launching and User procedures

- NN10329-111 - IEMS Basics

Related documents

- NN10334-911: IEMS Fault Management
- NN10330-511: IEMS Configuration Management
- NN10327-711: IEMS Performance Management
- NN10336-611: IEMS Security and Administration

MG9000 Manager

This section contains IEMS Northbound log samples and device documentation references for the MG9000 Mgr.

MG9000 Mgr Fault Interface

Fault documentation for MG9000 Mgr :

- NN10074-911 MG9000 Fault Management
- NN10408-900 ATM/IP Solution-level Fault Management
- NN10275-909 Carrier VoIP Fault Management Logs Reference

Fault Mapping for MG9000 Mgr

The following criteria can be used for looking up information on specific faults for MG9000 Mgr.

Fault Correlation for MG9000 Mgr

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MG9000 Mgr	logname and number	logname and number	logname and number	logname and number	NN10074-911 MG9000 Fault Management

Northbound Fault Formats for MG9000 Mgr

SCC2

The following is an example of a MG9000 Mgr log in SCC2 format:

```
49 MGEM302 4260 TBL  MG9K InvalidEMIPAddress
```

```
        Location: MG9k EM Comm Network
        Notification Id: 17180020453
        State: Cleared
        Category: communications
        Cause: Communications Subsystem Failure
              Invalid EM IP Address - An invalid EM IP address has been set on the GW
        Component Id: MG9k EM Comm Network
        specificProblem: Invalid EM IP Address - An invalid EM IP address has be
        en set on the GW
        Description: An invalid EM IP address has been set on the GW
```

NTSTD

The following is an example of a MG9000 Mgr log in NTSTD format:

```
RTPU07BR     MGEM302 Jan20 06:49:09 4260 TBL  MG9K InvalidEMIPAddress
        Location: MG9k EM Comm Network
        Notification Id: 17180020453
        State: Cleared
        Category: communications
        Cause: Communications Subsystem Failure
              Invalid EM IP Address - An invalid EM IP address has been set on the GW
        Component Id: MG9k EM Comm Network
        specificProblem: Invalid EM IP Address - An invalid EM IP address has be
        en set on the GW
        Description: An invalid EM IP address has been set on the GW
```

SNMP

The following is an example of a MG9000 Mgr log in SNMP format:

```
system.sysUpTime.0 => 20:33:14
iso.org.dod.internet.snmpV2.snmpModules.snmpMIB.snmpMIBObjects.snmpTrap.snmpTrapOID.
0 => nnExtAlarmClear
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48
.48.52.45.49.45.50.48.44.49.58.52.57.58.57.46.51.44.37279
alarmActiveDateAndTime => 2004-1-20,1:49:9.3,
alarmActiveDescription => Communications Subsystem Failure
Invalid EM IP Address - An invalid EM IP address has been set on the GW
```

```
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 6
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => MGEM302
nnExtAlarmActiveResourceDescription => IEMS=cco4;MG9k EM Comm Network
nnExtAlarmActiveSequenceNumber => 7768
```

Syslog

The following is an example of a MG9000 Mgr log in Syslog format:

```
Feb 23 12:38:54 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=4317~~ MGEM302 NONE TBL
MG9K InvalidEMIPAddress^M       Location: MG9k EM Comm Network^M       Notification
Id: 17180020453^M      State: Cleared^M      Category: communications^M      Cause:
Communications Subsystem Failure^M          Invalid EM IP Address - An invalid EM IP
address has been set on the GW^M        Component Id: MG9k EM Comm Network^M
specificProblem: Invalid EM IP Address - An invalid EM IP address has be^M       en
set on the GW^M        Description: An invalid EM IP address has been set on the GW
```

Performance

OM and PM Documentation references for MG9000 Mgr

- NN10140-711 MG9000 Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided.

XML

The following is an example of performance data for MG9000 Mgr in XML format:

```
PMFile=Begin
MeasurementCategorynoNamespaceSchemaLocationFileCreationTime
PM commonFormat.xsd2004-11-18T15:45:53EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityIdType
47.142.110.210MG9K Mgr
```

```
SubEntity=Begin
SubEntityId
CC04
SubEntity=End
                                                    ""
SubEntity=Begin
SubEntityId
CC03
SubEntity=End
                                                    ""
SubEntity=Begin
SubEntityId
CC02
SubEntity=End
                                                    ""
SubEntity=Begin
SubEntityId
Sefik_CCO1
SubEntity=End
                                                    ""
SubEntity=Begin
SubEntityId
cco6

Table=Begin
TableIdMeasurementKindIntervalDurationCaptureTime
nnPmUtilOmIntervTableSnapshot52004-11-18T15:45:00EST
LabelLabelLabelLabelLabelLabelLabelLabelLabel
SourcennPmUtilIntervChanAvgnnPmUtilIntervChanPeaknnPmUtilIntervCpuAvg
nnPmUtilIntervCpuPeaknnPmUtilIntervFlashAvgnnPmUtilIntervFlashPeak
nnPmUtilIntervRamAvgnnPmUtilIntervRamPeak
ValueValueValueValueValueValueValueValueValue
Frame006.Shelf2.Slot1500000000
Frame006.Shelf2.Slot1400000000
Frame006.Shelf3.Slot1300000000
Frame006.Shelf2.Slot1300000000
Frame006.Shelf3.Slot1200000000
Frame006.Shelf2.Slot1200000000
```

```
Frame006.Shelf2.Slot1100000000
Frame006.Shelf2.Slot1000000000
Table=End
```

GUI/CLUI Documentation for MG9000 Mgr

GUI Launching and User procedures

- NN10096-511 MG9000 Configuration Management

Related documents

- NN10162-611 MG9000 Administration and Security
- NN10048-461 Upgrading the MG9000
- NN10409-500 ATM/IP Solution-level Configuration Management
- NN10408-900 ATM/IP Solution-level Fault Management

Multi-Service Data Manager (MDM)

This section contains IEMS Northbound log samples and device documentation references for the MDM.

Information in this section also applies to the following Media Gateways : MSS 7400, 15000, 20000. All these devices are closely related and are covered by the same set of customer documentation.

MDM Fault Interface

Fault documentation for MDM:

- 241-6001-011 - MDM Fault Management Tools
- NN10092-911 - MSS 15000, MG 15000 & MDM Fault Overview
- NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
- NN10600-520 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
- 241-6001-500 - MDM Alarms Reference Guide

Fault Mapping for MDM

The following criteria can be used for looking up information on specific faults for MDM.

MDM and Media Gateway devices (6400, 7480, 15000, 20000) use fault code to identify different alarms. Fault codes are eight digits or letters and are grouped by type (first four digits of fault code). Documentation for each fault code group is provided in the following table.

Fault Documentation for MDM

Fault Code Group	Document Reference
0000	NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
1100	NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
70xx	NN10600-500 - Nortel Networks Multiservice Switch 7400/15000/20000 Alarms Reference
0999	241-6001-500 - MDM Alarms Reference Guide
301x	241-6001-500 - MDM Alarms Reference Guide
50xx	241-6001-500 - MDM Alarms Reference Guide
600x	241-6001-500 - MDM Alarms Reference Guide
A0xx	241-6001-500 - MDM Alarms Reference Guide
B000	241-6001-500 - MDM Alarms Reference Guide
CDxx	241-6001-500 - MDM Alarms Reference Guide

The faults that are fed northbound from the IEMS use log name and number for distinction. The mapping between log name/number and fault code can be found in the Succession Solution document.

- NN10092-911 - MSS 15000, MG 15000 & MDM Fault Overview

Fault Correlation for MDM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Multi-Service Data manager (MDM)	log name and number	log name and number	log name and number	log name and number	NN10092-911 MSS 15000, MG 15000 & MDM Fault Overview

Northbound Fault Formats for MDM

SCC2

The following is an example of a MDM log in SCC2 format:

```
*C22 MDM 303 7891 TBL
        time: 2004 01 25 09 22 32
        event: set
        compId: EM PP14
        severity: critical
        faultcode: 09990001
        alarmType: equipment
        commentData: FMDR_SURV@rtpimdm has lost connection to EM PP14. Please in
        vestigate.
```

NTSTD

The following is an example of a MDM log in NTSTD format:

```
RTPU07BU ***  MDM303 Jan25 14:22:32 7345 TBL
        time: 2004 01 25 09 22 32
        event: set
        compId: EM PP14
        severity: critical
        faultcode: 09990001
        alarmType: equipment
        commentData: FMDR_SURV@rtpimdm has lost connection to EM PP14. Please in
        vestigate.
```

SNMP

The following is an example of a MDM log in SNMP format:

```
system.sysUpTime.0 => 3 days, 0:41:03

snmpTrapOID.0 => nnExtAlarmCritical

alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.53.44.57.58.50.50.58.51.50.46.48.44.13270

alarmActiveDateAndTime => 2004-1-21,6:41:14.0,

alarmActiveDescription => DeviceSpecificInfo=equipmentFailure;FMDR_SURV@rtpimdm has
lost connection to EM PP14. Please investigate.


nnExtAlarmActiveEventType => 4

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => MDM 303

nnExtAlarmActiveResourceDescription => IEMS=47.142.116.75-MDM-Mgr_PP14;EM PP14

nnExtAlarmActiveManualClear => 1

nnExtAlarmActiveSequenceNumber => 17433
```

Syslog

The following is an example of a MDM log in Syslog format:

```
Feb 27 11:16:54 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0402~~ MDM303 CRIT TBL ^M
time: 2004 01 27 11 15 32^M       event: set^M       compId: EM PP14^M       severity:
critical^M       faultcode: 09990001^M       alarmType: equipment^M       commentData:
FMDR_SURV@rtpimdm has lost connection to EM PP14. Please in^M       vestigate.
```

Performance

OM and PM Documentation references for MDM

- 241-6001-031 - Multiservice Data Manager Performance Management Tools
- 241-6001-032 - Multiservice Data Manager Performance Data Reference

Northbound OM/PM Formats

Performance measurements for MDM are available only from the MDM directly. For more information on MDM, MSS 7000, and MSS 15000 OMs, see 241-6001-806 - MDM MDP Data Formats Reference Guide

XML

The following is an example of Performance data for MDM in XML format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-17T13:00:02EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
47.142.128.115,IEMS

Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
fiveMinCollectionJobTable,Snapshot,5,2005-03-17T13:00:02EST
Label,Label,Label,Label
fiveMinCollectionJobID,fiveMinCollectionJobName,fiveMinCollectionJobStartTime,fiveMi
nCollectionJobExecutionTime
Value,Value,Value,Value
1,IEMS5minCollection,1111082100898,2233
Table=End


Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime
tableSpaceTable,Snapshot,5,2005-03-17T13:00:01EST
Label,Label,Label
tableSpaceName,usedTableSpaceInBytes,usedTableSpaceInPercent
Value,Value,Value
IEMS_TS,45875200,44
IEMS_EVENT_TS,134610944,16
IEMS_PERF_TS,13238272,2
Table=End


Table=Begin
```

```
TableId,MeasurementKind,IntervalDuration,CaptureTime

fiveMinTransferJobTable,Snapshot,5,2005-03-17T13:00:02EST

Label,Label,Label,Label

fiveMinTransferJobID,fiveMinTransferJobName,fiveMinTransferJobStartTime,fiveMinTrans
ferJobExecutionTime

Value,Value,Value,Value

1,IEMS5minTransfer,1111082103882,453

Table=End



Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

deviceEventRateTable,Snapshot,5,2005-03-17T13:00:01EST

Label,Label,Label,Label

deviceID,deviceName,eventRate,eventRateDetails

Value,Value,Value,Value

3,rtpo-mg9kem.us.nortel.com-MG9K-Mgr_7.0,0,106 events received in 298170
milliseconds.

2,wnc0s0pe.us.nortel.com-MG9K-Mgr_9.0,0,14 events received in 298170 milliseconds.

1,SYSLOG,0,6 events received in 298170 milliseconds.

Table=End



Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

fiveMinReportJobTable,Snapshot,5,2005-03-17T13:00:02EST

Label,Label,Label,Label

fiveMinReportJobID,fiveMinReportJobName,fiveMinReportJobStartTime,fiveMinReportJobEx
ecutionTime

Value,Value,Value,Value

1,IEMS5minReport,1111082100898,733

Table=End



SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
```

```
systemRestartCount,2005-03-
17T13:00:00EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.system,2,Valid

numOfActiveClients,2005-03-
17T13:00:00EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.client,6,Valid

numOfEventsFromUnknownCustlogDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,6,Valid

eventQueueSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEventsFromUnknownSNMPDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

avgEventThroughputRate,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEventsFromUnknownDevices,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,6,Valid

maxEventThroughputRate,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,2,Valid

numOfDiscardedEvents,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,0,Valid

numOfEvents,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,150735,Valid

numOfEventsAdded,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.event,137,Valid

numOfAlarmsCleared,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,73,Valid

numOfMajorAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,263,Valid

numOfWarningAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,75,Valid

numOfCriticalAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,36,Valid

numOfAlarmsAdded,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,47,Valid

numOfMinorAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,74,Valid
```

```
numOfActiveAlarms,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.fault.alarms,448,Valid

numOfDBCleanUpPolicyExecutions,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.database,1,Valid

applicationHeapSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.memory,101923064,Valid

maxApplicationHeapSize,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.memory,139169296,Valid

numOfAttributesCollected,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,19411,Valid

numOfReportsJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfTransferJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfCollectionJobsProvisioned,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOfAttributesCollectedOverThisInterval,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,176,Valid

numOfFailedReportJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance,0,Valid

numOf24HrSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf30MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf12HrSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf15MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf60MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,0,Valid

numOf5MinSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
```

```
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.successfulCol
lectionJobs,1,Valid

numOf15MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf60MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf5MinPartialSuccessfulJobs,2005-03-
17T13:00:01EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf24HrPartialSuccessfulJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf30MinPartialSuccessfulJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf12HrPartialSuccessfulJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.partialSucces
sfulCollectionJobs,0,Valid

numOf24HrFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf30MinFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf12HrFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf15MinFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf60MinFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf5MinFailedCollectionJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedCollect
ionJobs,0,Valid

numOf24HrFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
```

```
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf30MinFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf12HrFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf15MinFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf60MinFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOf5MinFailedTransferJobs,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.performance.failedTransfe
rJobs,0,Valid

numOfManagedObjects,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,345,Valid

numOfDevicesInUnManagedState,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,4,Valid

numOfAddedManagedObjects,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInUnKnownState,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,9,Valid

numOfUnKnownDeviceStateTransistions,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfdeletedManagedObjects,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfThrottledDeviceStateTransistions,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInThrottledState,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfSystemUnManagedDeviceStateTransistions,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid

numOfDevicesInSystemUnManagedState,2005-03-
17T13:00:02EST,.iso.org.dod.internet.private.enterprises.nortel.nortelGenericMIBs.no
rtelNetworkManagementInterfaceMIBs.operationalMeasurements.topology,0,Valid
```

```
SingleValues=End
```

CSV

The following is an example of Performance data for MDM in CSV format:

```
PMFile=Begin

MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime

PM,commonFormat.xsd,2005-05-25T10:37:17EST


System=Begin

SystemId

NortelNetworks/IEMS


Entity=Begin

EntityId,Type

pcary55w.ca.nortel.com-MDM-Mgr_P15KL,Preside MDM


Table=Begin

TableId,MeasurementKind,IntervalDuration,CaptureTime

MSH10,Snapshot,5,2005-05-25T10:35:00EST

Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,
Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,
Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,
Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,
Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,
Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,
Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,
Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,Label,
Label,Label,Label,Label,Label,Label

CARDUTILAVG,CRITICALCLEARALARMS,CRITICALSETALARMS,INARPPACKETSLOCAL,INBYTES,INCBRCLP
0+1,INCBRFAIL,INCBRSETUP,INCLP0+1,INCLP0+1DIS,INFAIL100,INFAIL104,INFAIL111,INFAIL17
,INFAIL18,INFAIL21,INFAIL27,INFAIL28,INFAIL3,INFAIL35,INFAIL36,INFAIL37,INFAIL41,INF
AIL45,INFAIL47,INFAIL49,INFAIL57,INFAIL58,INFAIL63,INFAIL65,INFAIL73,INFAIL78,INFAIL
88,INFAIL96,INFAIL99,INFWDEXCEPTIONS,INICMPPACKETSLOCAL,INLOCALEXCEPTIONS,INNRTVBRCL
P0+1,INNRTVBRFAIL,INNRTVBRSETUP,INOSPFPACKETSLOCAL,INOTHERPACKETSLOCAL,INPACKETS,INP
ACKETSDIS,INRTVBRCLP0+1,INRTVBRFAIL,INRTVBRSETUP,INSETUP,INTCPPACKETSLOCAL,INUBRCLP0
+1,INUBRFAIL,INUBRSETUP,INUDPPACKETSLOCAL,IPLINKCAP,LINKCAP,LINKID,LMBUTIL,MAJORCLEA
RALARMS,MAJORSETALARMS,MAXTEMP,MINORCLEARALARMS,MINORSETALARMS,OUTARPPACKETSLOCAL,OU
TBYTES,OUTCBRCLP0+1,OUTCBRCLP0+1DIS,OUTCBRFAIL,OUTCBRSETUP,OUTCLP0+1,OUTCLP0+1DIS,OU
TFAIL100,OUTFAIL104,OUTFAIL111,OUTFAIL17,OUTFAIL18,OUTFAIL21,OUTFAIL27,OUTFAIL28,OUT
FAIL3,OUTFAIL35,OUTFAIL36,OUTFAIL37,OUTFAIL41,OUTFAIL45,OUTFAIL47,OUTFAIL49,OUTFAIL5
7,OUTFAIL58,OUTFAIL63,OUTFAIL65,OUTFAIL73,OUTFAIL78,OUTFAIL88,OUTFAIL96,OUTFAIL99,OU
TICMPPACKETSLOCAL,OUTNRTVBRCLP0+1,OUTNRTVBRCLP0+1DIS,OUTNRTVBRFAIL,OUTNRTVBRSETUP,OU
TOSPFPACKETSLOCAL,OUTOTHERPACKETSLOCAL,OUTPACKETS,OUTPACKETSDIS,OUTRTVBRCLP0+1,OUTRT
VBRCLP0+1DIS,OUTRTVBRFAIL,OUTRTVBRSETUP,OUTSETUP,OUTTCPPACKETSLOCAL,OUTUBRCLP0+1,OUT
UBRCLP0+1DIS,OUTUBRFAIL,OUTUBRSETUP,OUTUDPPACKETSLOCAL,REMOTEATMIFLABEL,SIGNALLINGCH
ANNELSTATUS

Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,
Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,
Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,
```

```
Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,
Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,
Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,
Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,
Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,Value,
Value,Value,Value,Value,Value,Value

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/5,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,,,0,865005,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,0,0,,,0,0,9838,0,,,,0,,,0,18719971,,E
M/P15KL LAPS/801
STS/0,,,,,,,0,7574550,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,,,,0,0,55404,0,,,,,0,,,,0,
,

4,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/4,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

4,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/3,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/2,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/1,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/0,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
ATMIF/300,,,,,,,,,0,0,0,0,278,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0
,0,0,0,,,,,278,0,0,0,0,,0,0,0,0,,GEN/CS2K_MSH10_HIOP14RL1_AMDI13R,0

,,,,,0,0,0,11227,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,711,0,0,,,,,
10516,0,0,0,,0,0,0,,,353207,EM/P15KL
ATMIF/203,,,,,,,,,0,0,0,0,13510,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,487,0,0,0,,,,,13023,0,0,0,0,,0,0,0,0,,EM/P15KE ATMIF/404,1

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
ATMIF/202,,,,,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,0
,0,0,,,,,0,0,0,0,0,,0,0,0,0,,GEN/MG4K_MSH10_7,0

,,,,,13334,0,594,25405,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,
,,,,12071,0,0,594,,0,0,0,,,353207,EM/P15KL
ATMIF/201,,,,,,,,,13349,0,0,190,24426,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,,0,0,0,0,,,,,11077,0,0,0,190,,0,0,0,0,,GEN/MG4K_MSH10_6,1

,,,,,0,0,0,19105,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,19
105,0,0,0,,0,0,0,,,353207,EM/P15KL
ATMIF/200,,,,,,,,,0,0,0,0,20174,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,0,0,0,0,,,,,20174,0,0,0,0,,0,0,0,0,,GEN/CS2K_MSH10_HIOP5RL1_AMDI6R,0

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
ATMIF/1303,,,,,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,
0,0,0,,,,,0,0,0,0,0,,0,0,0,0,,GEN/UAS_MSH10_DOMAIN_B_PORT_2,0

,,,49,86134,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,18,762,,,,75,300,1139,0,,,,,310,,,,10,12
50000,,EM/P15KL LP/0
OAMENET/0,,,,,,,0,95594,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,18,,,,,0,0,260,0,,,,,,230,,,,
,10,,

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
```

```
ATMIF/1302,,,,,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,
0,0,0,,,,,0,0,0,0,0,,0,0,0,0,,GEN/UAS_MSH10_DOMAIN_A_PORT_2,0

,,,,,0,0,0,3641,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,3521,0,0,,,,,
120,0,0,0,,0,0,0,,,353207,EM/P15KL
ATMIF/1301,,,,,,,,,0,0,0,0,4490,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,4370,0,0,0,,,,,120,0,0,0,0,,0,0,0,0,,GEN/SAM21_MSH10_SC_SLOT_7,1

,,,0,7580550,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,0,30,,,,30,0,55494,0,,,,,0,,,,0,1871997
1,,EM/P15KL LP/8 SONET/2
STS/0,,,,,,,0,865005,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,,,,,0,0,9838,0,,,,,,0,,,,,0,,

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
ATMIF/1203,,,,,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,
0,0,0,,,,,0,0,0,0,0,,0,0,0,0,,GEN/UAS_MSH10_DOMAIN_B_PORT_1,0

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
ATMIF/1202,,,,,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,
0,0,0,,,,,0,0,0,0,0,,0,0,0,0,,GEN/UAS_MSH10_DOMAIN_A_PORT_1,0

,,,,,0,0,0,160,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,40,0,0,,,,,120
,0,0,0,,0,0,0,,,353207,EM/P15KL
ATMIF/1201,,,,,,,,,0,0,0,0,160,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,
40,0,0,0,,,,,120,0,0,0,0,,0,0,0,0,,GEN/SAM21_MSH10_SC_SLOT_7,1

,,,,,0,0,0,3768,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,3650,0,0,,,,,
118,0,0,0,,0,0,0,,,353207,EM/P15KL
ATMIF/1200,,,,,,,,,0,0,0,0,3145,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
,3027,0,0,0,,,,,118,0,0,0,0,,0,0,0,0,,GEN/MG9K_MSH10_RM9K_DCC_SLOT_10,1

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
ATMIF/900,,,,,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,0
,0,0,,,,,0,0,0,0,0,,0,0,0,0,,Line gateway B,0

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/13,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/12,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,,,,,0,,,170852,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,,,,,,,0,,,,,170852,,,,,353207,EM/P15
KL
ATMIF/802,,,,,,,,,0,0,,,26467,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,0,0,,,,,,,0,0,,,,,26467,0,
,,,8600A,

,,,,,0,0,0,26168,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,
0,0,0,,26168,0,0,,,353207,EM/P15KL
ATMIF/801,,,,,,,,,0,0,0,0,170418,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,,0,0,0,0,,,,,0,0,0,0,0,,170418,0,0,0,,GEN/MG9K_IP9K,0

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
ATMIF/800,,,,,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,0
,0,0,,,,,0,0,0,0,0,,0,0,0,0,,line gateway A,0

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
FABRICCARD/Y,,,,29,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,0,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL
SHELF,,0,0,,0,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
FABRICCARD/X,,,,25,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
```

```
,,,,,10845,0,495,12852,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,
,,,,3416,0,0,495,,0,0,0,,,1412830,EM/P15KL
ATMIF/600,,,,,,,,,10863,0,0,93,12380,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,,0,0,0,0,,,,,2936,0,0,0,93,,0,0,0,0,,EM/P15KH ATMIF/1200,1

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/9,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,,,,,19565,0,102,22064,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,
,,,,2499,0,0,102,,0,0,0,,,353207,EM/P15KL
ATMIF/403,,,,,,,,,19570,0,0,82,21774,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0
,0,0,,0,0,0,0,,,,,2204,0,0,0,82,,0,0,0,0,,EM/P15KH ATMIF/203,1

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/8,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,0,0,0,
0,,0,0,0,,,353207,EM/P15KL
ATMIF/402,,,,,,,,,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,0
,0,0,,,,,0,0,0,0,0,,0,0,0,0,,GEN/MG4K_MSH10_5_TEMP_ON_NODE_H,0

2,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/7,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,,,,,0,0,0,40,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,40,0,
0,0,,0,0,0,,,353207,EM/P15KL
ATMIF/401,,,,,,,,,0,0,0,0,40,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,0,
0,0,0,,,,,40,0,0,0,0,,0,0,0,0,,GEN/DPTSPM_MSH10_1,1

3,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,EM/P15KL SHELF
CARD/6,0,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

,,,,,1209,0,0,1688,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,,,,0,0,0,,,,,
479,0,0,0,,0,0,0,,,353207,EM/P15KL
ATMIF/400,,,,,,,,,1184,0,0,826,2312,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,,0,0,0,0,,,,,1128,0,0,0,826,,0,0,0,0,,GEN/IWSPM_MSH10_2,1
```


BDF

The MDM provides a Bulk Data Format option for PM data as well as the CSV file format. The BDF format and reference information can be found in the Preside MDM MDP Data Formats Reference Guide.

GUI/CLUI Documentation for MDM

GUI Launching and User procedures

The following documents provide specific details about the various user interfaces provided by the MDM.

- 241-6001-801 - MDM Overview
- 241-6001-011 - MDM Fault Management Tools
- 241-6001-013 - MDM Remote Network Communication System User Guide
- 241-6001-015 - MDM Network Model Administration

- 241-6001-022 - MDM Network Reporting System
- 241-6001-023 - MDM Configuration Management Tools
- 241-6001-031 - MDM Performance Management

Related documents

Numerous documents are available on MDM installation, configuration, and planning. All the documents in the **241-6001-xxx** series are related to the MDM and its operations.

- NN10028-111 - MSS 15000, MG 15000 & MDM - Basics (PT-AAL1/UA-AAL1/UA-IP)
- NN10070-461 - Upgrading Multiservice Switch 15000 (PT-AAL1/UA-AAL1)
- NN10092-911 - MSS 15000, MG 15000 & MDM Fault Overview (PT-AAL1/UA-AAL1/UA-IP)
- NN10114-511 - MSS 15000, MG 15000 & MDM Configuration Overview (PT-AAL1/UA-AAL1/UA-IP/PT-AAL2)
- NN10158-711 - MSS 15000, MG 15000 & MDM Performance (PT-AAL1/UA-AAL1/UA-IP)
- NN10180-611 - MSS 15000, MG 15000 & MDM Security and Administration (PT-AAL1/UA-AAL1/UA-IP)
- NN10185-461 - Upgrading MDM
- NN10198-912 - MSS 15000, MG 15000 & MDM Troubleshooting (PT-AAL1/UA-AAL1/UA-IP)
- NN10225-512 - MSS 15000, MG 15000 & MDM Configuration Attribute Summary (PT-AAL1/UA-AAL1/UA-IP/PT-AAL2)

SAM21 Element Manager

This section contains IEMS Northbound log samples and device documentation references for the SAM21 EM.

SAM21 EM Fault Interface

Fault documentation for SAM21 EM :

The SAM 21 Manager reports faults for the SAM 21 Shelf Controller. Please refer to the SAM 21 SC documents below for details about SAM 21 faults.

- NN10089-911 - SAM21 Shelf Controller Fault Management

Fault Mapping for SAM21 EM

The following criteria can be used for looking up information on specific faults for SAM21 EM.

Fault Correlation for SAM21 EM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
SAM21 Mgr	logname and number	logname and number	logname and number	logname and number	NN10089-911 SAM21 Shelf Controller Fault Management

Northbound Fault Formats for SAM21 EM

SCC2

The following is an example of a SAM21 EM log in SCC2 format:

```
**37 SCU 350 0009 FLT  Alarm Raised
        Location: SAM21 1:CSAM01-01:sled 3
        Time:     Wed Jan 14 13:55:52 EST 2004
        Reason:   Temperature in Sled 3 is high
```

NTSTD

The following is an example of a SAM21 EM log in NTSTD format:

```
COMPACT06BT  **  SCU350 Jan15 00:37:17 0009 FLT  Alarm Raised
        Location: SAM21 1:CSAM01-01:sled 3
        Time:     Wed Jan 14 13:55:52 EST 2004
        Reason:   Temperature in Sled 3 is high
```

SNMP

The following is an example of a SAM21 EM log in SNMP format:

```
sysUpTime.0 => 9:14:20
snmpTrapOID.0 => nnExtAlarmMajor
```

```
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.51.44.51.58.49.52.58.51.56.46.48.44.42847

alarmActiveDateAndTime => 2004-1-23,3:14:38.0,

alarmActiveDescription => DeviceSpecificInfo=;Location: SAM21 1:CSAM01-01:sled 3

Time:     Wed Jan 14 13:57:48 EST 2004

Reason:   Temperature in Sled 3 is high


nnExtAlarmActiveEventType => 5

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => SCU 350

nnExtAlarmActiveResourceDescription => IEMS=wnc0y0kz.us.nortel.com-SAM21-Mgr;

nnExtAlarmActiveManualClear => 2

nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a SAM21 EM log in Syslog format:

```
Feb 12 18:30:19 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7929~~  SCU350 MAJOR FLT
Alarm Raised^M       Location: SAM21 1:CSAM01-01:sled 3^M       Time:     Mon Jan 12
12:49:06 EST 2004^M        Reason:   Temperature in Sled 3 is high
```

Performance

OM and PM Documentation references for SAM21 EM

SAM21 EM has no operational or performance measurements.

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of performance data for SAM21 EM in XML format:

> ***Note:*** *Northbound performance interface not supported for this component.*

CSV

The following is an example of performance data for SAM21 EM in CSV format:

```
PMFile=Begin
MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime
PM,commonFormat.xsd,2005-03-16T10:55:01EST

System=Begin
SystemId
NortelNetworks/IEMS

Entity=Begin
EntityId,Type
172.16.144.134,SAM21

SingleValues=Begin
MeasurementKind,IntervalDuration
Snapshot,5
MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability
totalBytesRxed,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,14792,Valid
rxedTimeoutCount,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,0,Valid
bytesSentPerSec,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,24,Valid
cellDropCount,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,0,Valid
oversizedPDUCount,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,0,Valid
bytesRxedPerSec,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,24,Valid
totalBytesSent,2005-03-
16T10:55:00EST,.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceCont
rol.scu.scuMessaging.ipoaMIB,16765,Valid
SingleValues=End

Entity=End

System=End
```

PMFile=End

GUI/CLUI Documentation for SAM21 EM

GUI Launching and User procedures

- NN10409-500 - ATM/IP Solution-level Configuration Management
- NN10402-600 - ATM/IP Solution-level Administration and Security
- NN10111-511 - SAM21 Shelf Controller Configuration Management

Related documents

- NN10025-111 - SAM21 Shelf Controller Basics
- NN10408-900 - ATM/IP Solution-level Fault Management
- NN10155-711 - SAM21 Shelf Controller Performance Management
- NN10177-611 - SAM21 Shelf Controller Administration and Security

Applications

Audio Provisioning Server (APS)

This section contains IEMS Northbound log samples and device documentation references for the APS.

APS Fault Interface

Fault documentation for APS :

- NN10328-911 - MS 2000 Series Fault Management

Fault Mapping for APS

The following criteria can be used for looking up information on specific faults for APS.

Fault Correlation for APS

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
APS	SpecificProblem	SpecificProblem	SpecificProblem	SpecificProblem	NN10328-911 MS 2000 Series Fault Management

Northbound Fault Formats for APS

SCC2

The following is an example of a APS log in SCC2 format:

```
*C02 APS 398 2759 TBL  APS Fault
        Location: rtp2aps
        Notification Id: 28673
        State: Raise
        Category: communications
        Cause: softwareError
        Time: Jan 27 07:02:30 2004
        Component Id: APS;APSUnit=nc0rtp170;Software=Audio_Management_0
        Specific Problem: 28673
        Description: DB is not available, or the user cannot get a connection to
        the DB
```

NTSTD

The following is an example of a APS log in NTSTD format:

```
RTPU07BR ***  APS398 Jan27 12:02:30 2207 TBL  APS Fault
        Location: rtp2aps
        Notification Id: 28673
        State: Raise
        Category: communications
        Cause: softwareError
        Time: Jan 27 07:02:30 2004
        Component Id: APS;APSUnit=nc0rtp170;Software=Audio_Management_0
        Specific Problem: 28673
        Description: DB is not available, or the user cannot get a connection to
```

```
the DB
```

SNMP

The following is an example of a APS log in SNMP format:

```
sysUpTime.0 => 2 days, 18:44:37

snmpTrapOID.0 => nnExtAlarmCritical

alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.18.50.48
.48.52.45.49.45.50.55.44.5

5.58.49.58.54.46.48.44.11202

alarmActiveDateAndTime => 2004-1-27,7:1:6.0

alarmActiveDescription => DeviceSpecificInfo=;DB is not available, or the user cannot
get a connection to

nnExtAlarmActiveEventType => 5

nnExtAlarmActiveProbableCause => 118

nnExtAlarmActiveAdditionalText =>

nnExtAlarmActiveDocumentationPointer => APS 398

nnExtAlarmActiveResourceDescription => IEMS=znc0s0j6-SSPFS-Unit-
0;APS;APSUnit=nc0rtp170;Software=Audio_Management_0

nnExtAlarmActiveManualClear => 4

nnExtAlarmActiveSequenceNumber => 13458
```

Syslog

The following is an example of a APS log in Syslog format:

```
Feb 27 07:02:24 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=6645~~  APS398 CRIT TBL  APS
Fault^M      Location: rtp2aps^M      NotificationID: 28673^M      State: Raise^M
Category: Communications^M       Cause: Software error^M       Time: Jan 27 07:02:30
2004^M       Component Id: APS;APSUnit=nc0rtp170;Software=Audio_Management_0^M
Specific Problem: 28673^M       Description: DB is not available, or the user cannot
get a connection to^M         the DB^M
```

Performance

OM and PM Documentation references for APS

- NN10331-711 - MS 2000 Series Performance Management

Northbound OM/PM Formats

XML

The following is an example of performance data for APS in XML format:

> ***Note:*** *Northbound performance interface not supported for this component.*

CSV

The following is an example of performance data for APS in CSV format:

```
PMFile=Begin

MeasurementCategory,noNamespaceSchemaLocation,FileCreationTime

PM,commonFormat.xsd,2005-03-24T14:55:02EST


System=Begin

SystemId

NortelNetworks/IEMS


Entity=Begin

EntityId,Type

172.17.40.230,MS2000


SingleValues=Begin

MeasurementKind,IntervalDuration

Snapshot,5

MeasureId,CaptureTime,MeasureSuppId1,Value,Reliability

sysDescr,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.system,Product:
IPmedia 2000;SW Version: 4.60B.003,Valid

snmpOutPkts,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.snmp,159,Valid

snmpInBadVersions,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInBadCommunityNames,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInTotalReqVars,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,323,Valid

snmpOutTraps,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.snmp,6,Valid

snmpInBadCommunityUses,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

snmpInPkts,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.snmp,154,Valid

snmpInTotalSetVars,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid
```

```
snmpInASNParseErrs,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-
2.snmp,0,Valid

tcpOutSegs,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.tcp,42,Valid

tcpInSegs,2005-03-24T14:55:01EST,.iso.org.dod.internet.mgmt.mib-2.tcp,7148,Valid

udpOutDatagrams,2005-03-24T14:55:02EST,.iso.org.dod.internet.mgmt.mib-
2.udp,3974,Valid

udpInDatagrams,2005-03-24T14:55:02EST,.iso.org.dod.internet.mgmt.mib-2.udp,238,Valid

snmpSilentDrops,2005-03-24T14:55:02EST,.iso.org.dod.internet.mgmt.mib-2.snmp,0,Valid

acPerfCpMessageSendErrors,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpNumDupsForCompletedTransactions,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageMaxRetransmissionsExceeded,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,421,Valid

acPerfCpMessageReceiveErrors,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessageRetransmissions,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,2954,Valid

acPerfCpNumDupsForOutstandingTransactions,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpMessagesFromUntrustedSources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfCpProtocolSyntaxErrors,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfCp,0,Valid

acPerfRtpRcvrLostPackets,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfRtp,0,Valid

acPerfRtpFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfRtp,0,Valid

acPerfIvrPlayCollectRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayCollectFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid
```

```
acPerfIvrPlayFailedDueToProvMismatch,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrContDigitCollectRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrPlayCollectFailedDueToProvMismatch,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfIvrContDigitCollectFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfIvr,0,Valid

acPerfBctFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfBct,0,Valid

acPerfBctRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfBct,0,Valid

acPerfConfRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfConfPortsUsed,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfConfAddFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfConfFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfConf,0,Valid

acPerfTtFailedDueToLackOfResources,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfTt,0,Valid

acPerfTtRequests,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaServices.acPerfTt,0,Valid

acPerfSystemPacketEndpointsInUse,2005-03-
24T14:55:02EST,.iso.org.dod.internet.private.enterprises.audioCodes.acPerformances.a
cPerfMediaGateway.acPerfSystem,0,Valid

SingleValues=End


Entity=End


System=End


PMFile=End
```

GUI/CLUI Documentation for APS

GUI Launching and User procedures

- NN10340-511 - MS 2000 Series Configuration Management

Related documents

Line Maintenance Manager (LMM)

This section contains IEMS Northbound log samples and device documentation references for LMM.

LMM Fault Interface

Fault documentation for LMM :

There are no faults or logs associated with this application.

Fault Mapping for LMM

There are no faults or logs associated with this application.

Performance

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for LMM

GUI Launching and User procedures

Related documents

Network Patch Manager (NPM)

This section contains IEMS Northbound log samples and device documentation references for the Network Patch Manager (NPM).

NPM Fault Interface

Fault documentation for NPM :

- NN10408-900 - ATM/IP Solution-level Fault Management

Fault Mapping for NPM

The following criteria can be used for looking up information on specific faults for NPM.

Fault Correlation for NPM

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
NPM	logname and number	logname and number	logname and number	logname and number	NN10408-900 - ATM/IP Solution-level Fault Management

Northbound Fault Formats for NPM

SCC2

The following is an example of an NPM log in SCC2 format:

```
  38 NPM 360 6012 INFO Alarm Raised
        Alarm ACT_NOT_APP has been raised.
        Alarm Description: Activatable patches not applied.
```

NTSTD

The following is an example of an NPM log in NTSTD format:

```
RTPU07BU      NPM360 Jan27 15:38:44 5466 INFO Alarm Raised
        Alarm ACT_NOT_APP has been raised.
        Alarm Description: Activatable patches not applied.
```

SNMP

The following is an example of an NPM log in SNMP format:

```
system.sysUpTime.0 => 2 days, 22:22:15
snmpTrapOID.0 => nnExtAlarmMessage
```

```
nnExtAlarmMessageResource => .0.0

nnExtAlarmMessageResourceDescription => IEMS=znc0s0j6-SSPFS-Unit-0;

nnExtAlarmMessageDateAndTime => 2004-1-27,10:38:44.0

nnExtAlarmMessageDocumentationPointer => NPM 360

nnExtAlarmMessageInfo =>   38 NPM 360 6012 INFO Alarm Raised                  Alarm
ACT_NOT_APP has been raised.


        Alarm Description: Activatable patches not applied.
```

Syslog

The following is an example of an NPM log in Syslog format:

```
Feb 27 10:40:03 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0201~~  NPM360 NONE INFO
Alarm Raised^M        Alarm ACT_NOT_APP has been raised.^M        Alarm Description:
Activatable patches not applied.
```

Performance

OM and PM Documentation references for NPM

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for NPM

GUI Launching and User procedures

- NN10409-500 - ATM/IP Solution-level Configuration Management

Related documents

- NN10402-600 - ATM/IP Solution-level Administration and Security
- NN10440-450 - Upgrading theCarrier VoIP Network

OSSGate

This section contains IEMS Northbound log samples and device documentation references for the OSSGate.

OSSGate Fault Interface

Fault documentation for OSSGate :

There are no faults or logs associated with this application.

Fault Mapping for OSSGate

There are no faults or logs associated with this application.

Performance

OM and PM Documentation references for OSSGate

There are no OMs or PMs associated with this application.

Northbound OM/PM Formats

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for OSSGate

GUI Launching and User procedures

- NE10004-512 OSSGate User's Guide

Related documents

- 297-9051-8081 SERVORD Reference Manual Vol 1 of 2
- 297-9051-8082 SERVORD Reference Manual Vol 2 of 2

QoS Collector Application (QCA)

This section contains IEMS Northbound log samples and device documentation references for the QCA.

QCA Fault Interface

Fault documentation for QCA :

The QoS Collector reports faults as part of the CS2K Management Tools suite. The documents below contain information about QoS Collector faults.

- NN10083-911 - Communication Server 2000 Fault Management

Fault Mapping for QCA

The following criteria can be used for looking up information on specific faults for QCA.

Fault Correlation for QCA

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
QCA	logname and number	logname and number	logname and number	logname and number	NN10083-911 Communication Server 2000 Fault Management

Northbound Fault Formats for QCA

SCC2

The following is an example of a QCA log in SCC2 format:

```
*C34 QCA 310 0052 TBL  wnc0y0kz
        Location: wnc0y0kz
        NotificationID : 49
        State : Raise
        Category : Processing Error
        Cause : storageCapacityProblem
        Time : Jan 22 16:34:19 2004
        Component Id: /data/qca
        Specific Problem: checkDiskSpace() has shown that there is less than
        104857600 bytes available on the local disk.
        Description : More Disk space is required  immediately.
```

NTSTD

The following is an example of a QCA log in NTSTD format:

```
COMPACT06BT ***  QCA 310 Jan22 21:34:19 0052 TBL  wnc0y0kz
        Location: wnc0y0kz
        NotificationID : 49
        State : Raise
        Category : Processing Error
        Cause : storageCapacityProblem
        Time : Jan 22 16:34:19 2004
        Component Id: /data/qca
        Specific Problem: checkDiskSpace() has shown that there is less than
```

```
104857600 bytes available on the local disk.
Description : More Disk space is required  immediately.
```

SNMP

The following is an example of a QCA log in SNMP format for a raise alarm:

```
system.sysUpTime.0 => 0:28:36
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.2
8.50.48.48.53.45.48.57.45.48.55.44.49.57.58.53.55.58.51.56.46.48.44.45.48.52
.58.48.48.140819
alarmActiveDateAndTime => 2004-1-22,4:34:20.0,
alarmActiveDescription => If 10 (or more) records with unsupported version are
received consecutively, Major fault log is generated and the connection is
closed
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 166
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => QCA 301
nnExtAlarmActiveResourceDescription => IEMS=rtp4cmt-QOS
nnExtAlarmActiveManualClear => 4
nnExtAlarmActiveSequenceNumber => 3
```

The following is an example of a QCA log in SNMP format for a clear alarm:

```
system.sysUpTime.0 => 0:28:36
snmpTrapOID.0 =>
alarmActiveResourceId =>
1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.2
8.50.48.48.53.45.48.57.45.48.55.44.49.57.58.53.55.58.51.56.46.48.44.45.48.52
.58.48.48.140819
alarmActiveDateAndTime => 2004-1-22,4:34:20.0,
alarmActiveDescription => If 10 (or more) records with unsupported version are
received consecutively, Major fault log is generated and the connection is
closed
nnExtAlarmActiveEventType => 1
nnExtAlarmActiveProbableCause => 1024
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => QCA 399
nnExtAlarmActiveResourceDescription => IEMS=rtp4cmt-QOS
nnExtAlarmActiveManualClear => 4
```

```
nnExtAlarmActiveSequenceNumber => 3
```

Syslog

The following is an example of a QCA log in Syslog format:

```
Feb 22 16:34:19 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0062~~  QCA310 CRIT TBL
wnc0y0kz^M        Location: wnc0y0kz^M        NotificationID : 49^M        State :
Raise^M      Category : Processing Error^M      Cause : storageCapacityProblem^M
Time : Jan 22 16:26:49 2004^M       Component Id: /data/qca^M       Specific Problem:
checkDiskSpace() has shown that there is less than^M       104857600 bytes available
on the local disk.^M        Description : More Disk space is required  immediately.^M
```

Performance

OM and PM Documentation references for QCA

- There are no OMs or PMs associated with QCA.

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for QCAin XML format:

Note: *Northbound performance interface not supported for this component.*

CSV

The following is an example of Performance data for QCA in CSV format:

Note: *Northbound performance interface not supported for this component.*

GUI/CLUI Documentation for QCA

GUI Launching and User procedures

- NN10409-500 - ATM/IP Solution-level Configuration Management

Related documents

Trunk Maintenance Manager (TMM)

This section contains IEMS Northbound log samples and device documentation references for TMM.

TMM Fault Interface

Fault documentation for TMM :

There are no faults or logs associated with this application.

Fault Mapping for TMM

There are no faults or logs associated with this application.

Performance

OM and PM Documentation references for TMM

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for TMM

GUI Launching and User procedures

- NN10409-500 - ATM/IP Solution-level Configuration Management

Related documents

Non-Topology Elements

This section contains references to applications that do not appear in the IEMS topology, but still report faults to the Northbound log streams.

Data Audit System

This section contains IEMS Northbound log samples and device documentation references for the Data Audit System.

Data Audit System Fault Interface

Fault documentation for Data Audit System :

- NN10408-900 - ATM/IP Solution-level Fault Management

Fault Mapping for Data Audit System

The following criteria can be used for looking up information on specific faults for Data Audit System.

Fault Correlation for Data Audit System

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
Data Audit System	logname and number	logname and number	logname and number	logname and number	NN10408-900 - ATM/IP Solution-level Fault Management

Northbound Fault Formats for Data Audit System

SCC2

The following is an example of a Data Audit System log in SCC2 format:

```
*C43 CMT 300 5341 TBL CMT Fault
        Location: Audit
        NotificationID: 1001
        State: Raise
        Category: Processing Error
        Cause: Corrupt data
        Time: Jan 23 13:43:37 2004
        Component Id: SESM=AuditSystem;Audit=CS2K Data Integrity Audit
        Specific Problem: Data mismatches detected
        Description: The SESM audit: CS2K Data Integrity Audit, has 59 unresolve
        d problems. To view and correct the problems, open the audit problem rep
        ort from the Audit System found under the SESM Maintenance menu item.
```

NTSTD

The following is an example of a Data Audit System log in NTSTD format:

```
COMPACT06BT ***  CMT300 Jan23 18:43:37 5341 TBL CMT Fault
        Location: Audit
        NotificationID: 1001
        State: Raise
        Category: Processing Error
        Cause: Corrupt data
        Time: Jan 23 13:43:37 2004
        Component Id: SESM=AuditSystem;Audit=CS2K Data Integrity Audit
        Specific Problem: Data mismatches detected
        Description: The SESM audit: CS2K Data Integrity Audit, has 59 unresolve
        d problems. To view and correct the problems, open the audit problem rep
        ort from the Audit System found under the SESM Maintenance menu item.
```

SNMP

The following is an example of a Data Audit System log in SNMP format:

```
system.sysUpTime.0 => 21:39:13
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.51.44.49.58.52.51.58.51.55.46.48.44.42485
alarmActiveDateAndTime => 2004-1-23,1:43:37.0,
alarmActiveDescription => DeviceSpecificInfo=;Event from Unknown Syslog Device
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => CMT 300
nnExtAlarmActiveResourceDescription => IEMS=znc0s0j6;SESM=AuditSystem;Audit=CS2K Data
Integrity Audit
nnExtAlarmActiveManualClear => 0
nnExtAlarmActiveSequenceNumber => 8390
```

Syslog

The following is an example of a Data Audit System log in Syslog format:

```
Feb 23 13:44:54 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=5398~~ CMT300 CRIT TBL CMT
Fault^M Location: Audit^M NotificationID: 1001^M State: Raise^M Category: Processing
Error^M Cause: Corrupt data^M Time: Jan 23 13:43:37 2004^M Component Id:
SESM=AuditSystem;Audit=CS2K Data Integrity Audit^M Specific Problem: Data mismatches
detected^M Description: The SESM audit: CS2K Data Integrity Audit, has 59 unresolve^M
d problems. To view and correct the problems, open the audit problem rep^M ort from
the Audit System found under the SESM Maintenance menu item.^M
```

Performance

OM and PM Documentation references for Data Audit System

There are no OMs or PMs associated with this application.

Northbound OM/PM Formats

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for Data Audit System

GUI Launching and User procedures

- NN10320-100 - ATM Solutions Basics
- NN10300-100 - IP Solutions Basics
- NN10276-500 - ATM/IP Configuration Management
- NN10325-900 - ATM/IP Fault Management

Related documents

IW-SPM IP

This section contains IEMS Northbound log samples and device documentation references for the IW-SPM IP.

IW-SPM IP Fault Interface

Fault documentation for IW-SPM IP :

- NN10078-911 - IW SPM IP Fault Management
- NN10275-909 - Carrier VoIP Fault Management Logs Reference

Fault Mapping for IW-SPM IP

The following criteria can be used for looking up information on specific faults for IW-SPM IP.

Fault Correlation for IW-SPM IP

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
IW-SPM IP	Logname and number	Logname and number	Logname and number	Logname and number	NN10078-911 IW SPM IP Fault Management

Northbound Fault Formats for IW-SPM IP

SCC2

The following is an example of a IW-SPM IP log in SCC2 format:

```
**17 SPM 313 4488 TBL  Fault
        SPM   0 CEM   0 : A                      Time: 12:16:13.890
        Source: None           State: Insv       Type: None
        Reason:     Loadname mismatch.
        Diagnostic: Autonomous fault detection
        Comp:MCM         RegAddr:0           Exp:0           Act:0
```

NTSTD

The following is an example of a IW-SPM IP log in NTSTD format:

```
RTPU07BU  **  SPM313 Feb28 00:06:14 9091 TBL  Fault
        SPM   0 CEM   1 : A                      Time: 19:05:14.820
        Source: None           State: Insv       Type: None
        Reason:     SYNC OOSpec: prim. ref. NA.
        Diagnostic: Autonomous fault detection
        Comp:TIC         RegAddr:0           Exp:0           Act:0
```

SNMP

The following is an example of a IW-SPM IP log in SNMP format:

```
system.sysUpTime.0 => 3 days, 6:54:40
snmpTrapOID.0 => nnExtAlarmMajor
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.50.45.50.55.44.55.58.49.50.58.50.55.46.54.44.14023
alarmActiveDateAndTime => 2004-2-27,7:12:27.6
alarmActiveDescription => DeviceSpecificInfo=Unavailable;SPM  0 CEM  0 : A
Time: 19:11:31.010
Source: None           State: Insv       Type: None
Reason:     SYNC OOSpec: prim. ref. NA.
Diagnostic: Autonomous fault detection
Comp:TIC         RegAddr:0           Exp:0           Act:0
```

```
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => SPM 313
nnExtAlarmActiveResourceDescription => IEMS=wnc0y0m0.us.nortel.com-CS2K-Mgr;
nnExtAlarmActiveManualClear => 3
nnExtAlarmActiveSequenceNumber => 18489
```

Syslog

The following is an example of a IW-SPM IP log in Syslog format:

```
Feb 28 12:11:09 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=7983~~  SPM313 MAJOR TBL
Fault^M       SPM   0 CEM   1 : I                    Time: 12:10:11.080^M       Source:
None           State: Insv       Type: None  ^M        Reason:     No frame pulse from
DS-512 #0    ^M      Diagnostic: Autonomous fault detection      ^M      Comp:TIC
RegAddr:0            Exp:0           Act:0
```

Performance

OM and PM Documentation references for IW-SPM IP

- NN10144-711 - IW SPM IP Performance Management

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for IW-SPM IP in XML format:

Note: *The IEMS northbound performance interface does not support this device.*

CSV

The following is an example of Performance data for IW-SPM IP in CSV format:

Note: *The IEMS northbound performance interface does not support this device.*

GUI/CLUI Documentation for IW-SPM IP

GUI Launching and User procedures

- NN10015-111 - IW SPM IP Basics

Related documents

- NN10056-461 - Upgrading the IW SPM IP
- NN10100-511 - IW SPM IP Configuration Management
- NN10166-611 - IW SPM IP Administration and Security

MG9000 Manager Mid-Tier

This section contains IEMS Northbound log samples and device documentation references for the MG9000 Mgr Mid-Tier.

MG9000 Mgr Mid-Tier Fault Interface

Fault documentation for MG9000 Mgr Mid-Tier :

All MG9000 Mgr Mid-Tier faults are delivered via MG9000 Mgr. See document(s)

- NN10074-911 MG9000 Fault Management
- NN10408-900 ATM/IP Solution-level Fault Management
- NN10275-909 Carrier VoIP Fault Management Logs Reference

Fault Mapping for MG9000 Mgr Mid-Tier

The following criteria can be used for looking up information on specific faults for MG9000 Mgr Mid-Tier.

Fault Correlation for MG9000 Mgr Mid-Tier

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
MG9K Mid-Tier	log name and number	log name and number	log name and number	log name and number	NN10074-911 MG9000 Fault Management

Northbound Fault Formats for MG9000 Mgr Mid-Tier

SCC2

The following is an example of a MG9000 Mgr Mid-Tier log in SCC2 format:

```
  52 MGEM703 0193 INFO Shutdown_Event
        Status: Shutting MG 9K Midtier Server down ...
```

NTSTD

The following is an example of a MG9000 Mgr Mid-Tier log in NTSTD format:

```
RTPU07BT     MGEM703 Feb02 20:52:08 0197 INFO Shutdown_Event
        Status: Shutting MG 9K Midtier Server down ...
```

SNMP

The following is an example of a MG9000 Mgr Mid-Tier log in SNMP format:

sysUpTime.0 => 1:30:14

snmpTrapOID.0 => nnExtAlarmMessage

nnExtAlarmMessageResource => .0.0

nnExtAlarmMessageResourceDescription => IEMS=wnc0y0nr.us.nortel.com-SSPFS-Unit-0;

nnExtAlarmMessageDateAndTime => 2004-2-2,3:52:8.0

nnExtAlarmMessageDocumentationPointer => MGEM703

nnExtAlarmMessageInfo => 52 MGEM703 0193 INFO Shutdown_Event Status: Shutting MG 9K Midtier Server down ...

Syslog

The following is an example of a MG9000 Mgr Mid-Tier log in Syslog format:

```
Mar  4 15:27:47 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=0682~~ MGEM703 NONE INFO
Shutdown_Event
Status: Shutting MG 9K Midtier Server down ...
```

Performance

OM and PM Documentation references for MG9000 Mgr Mid-Tier

There are no OMs or PMs associated with this component.

GUI/CLUI Documentation for MG9000 Mgr Mid-Tier

GUI Launching and User procedures

The MG9000 Mgr Mid-Tier is an application that runs on an SSPFS machine. See SSPFS platform for client launch details.

- NN10096-511 MG9000 Configuration Management

Related documents

- NN10048-461 Upgrading the MG9000
- NN10409-500 ATM/IP Solution-level Configuration Management
- NN10408-900 ATM/IP Solution-level Fault Management
- NN10162-611 MG9000 Administration and Security

OM Collector

OM Collector Fault Interface

This section contains IEMS Northbound log samples and device documentation references for the OM Collector.

Fault documentation for OM Collector :

- NN10074-911 MG9000 Fault Management

Fault Mapping for OM Collector

- NN10074-911 MG9000 Fault Management

The following criteria can be used for looking up information on specific faults for OM Collector.

Fault Correlation for OM Collector

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
OM Collector	logname and number	logname and number	logname and number	logname and number	NN10074-911 MG9000 Fault Management

Northbound Fault Formats for OM Collector

SCC2

The following is an example of a OM Collector log in SCC2 format:

```
  27 OMC 700 0470 INFO Startup_Event
        Status: OMCLTR_Process: OMCollector Process was started with PSID 17585
```

NTSTD

The following is an example of a OM Collector log in NTSTD format:

```
RTPU07BR      OMC700 Jan28 21:27:53 9923 INFO Startup_Event
         Status: OMCLTR_Process: OMCollector Process was started with PSID 17585
```

SNMP

The following is an example of a OM Collector log in SNMP format:

```
system.sysUpTime.0 => 4 days, 4:10:00
snmpTrapOID.0 => nnExtAlarmMessage
nnExtAlarmMessageResource => .0.0
nnExtAlarmMessageResourceDescription => IEMS=wnc0s0kq.us.nortel.com-SSPFS-Unit-0;
nnExtAlarmMessageDateAndTime => 2004-1-28,4:27:53.0
nnExtAlarmMessageDocumentationPointer => OMC 700
nnExtAlarmMessageInfo =>   27 OMC 700 0470 INFO Startup_Event
        Status: OMCLTR_Process: OMCollector Process was started with PSID 17585
```

Syslog

The following is an example of a OM Collector log in Syslog format:

```
Feb 28 16:27:48 wnc0s0pf IEMS: _V2_~I=~H=wnc0s0pf~A=IEMS~S=4656~~  OMC700 NONE INFO
Startup_Event^M        Status: OMCLTR_Process: OMCollector Process was started with
PSID 17585
```

Performance

OM and PM Documentation references for OM Collector

There are no OMs or PMs associated with this application. For MG9000 performance information see:

- NN10140-711 MG9000 Performance Management

Northbound OM/PM Formats

There are no OMs or PMs associated with this application.

GUI/CLUI Documentation for OM Collector

GUI Launching and User procedures

- NN10140-711 MG9000 Performance Management
- NN10096-511 MG9000 Configuration Management

Related documents

- NN10409-500 ATM/IP Solution-level Configuration Management

V5.2 Data Audit

This section contains IEMS Northbound log samples and device documentation references for the V5.2 Data Audit.

V5.2 Data Audit Fault Interface

Fault documentation for V5.2 Data Audit :

The V5.2 Data Integrity Audit Module of V5.2 Data Audit will raise CMT300 faults, and it will be covered in **DataAudit**'s Fault Management.

The Data Audit system will generate CMT300 logs when problems are found during any of its audits. The component ID of the log can be used to identify the specific audit that encountered a problem.

- NN10275-909 - Carrier VoIP Fault Management Logs Reference
- NN10408-900 - ATM/IP Solution-level Fault Management

Fault Mapping for V5.2 Data Audit

The following criteria can be used for looking up information on specific faults for V5.2 Data Audit.

Fault Correlation for V5.2 Data Audit

NB format -> Device/EM	SCC2	NTSTD	SNMP	Syslog	Document Reference
V5.2 Data Audit	log name and log number. Seen as component ID in generic CMT300 Audit log. example: componentid = SESM=AuditSystem;Audit=V5.2 Data Integrity Audit	log name and log number. Seen as component ID in generic CMT300 Audit log. example: componentid = SESM=AuditSystem;Audit=V5.2 Data Integrity Audit	log name and log number. Seen as component ID in generic CMT300 Audit log. example: componentid = SESM=AuditSystem;Audit=V5.2 Data Integrity Audit	log name and log number. Seen as component ID in generic CMT300 Audit log. example: componentid = SESM=AuditSystem;Audit=V5.2 Data Integrity Audit	NN10275-909 Carrier VoIP Fault Management Logs Reference

Northbound Fault Formats for V5.2 Data Audit

SCC2

The following is an example of a V5.2 Data Audit log in SCC2 format:

```
*C12 CMT 300 0002 TBL  CMT Fault
        Location: Audit
        NotificationID: 1002
        State: Raise
        Category: Processing Error
        Cause: Corrupt data
        Time: Feb 14 23:12:48 2004
        Component Id: SESM=AuditSystem;Audit=V5.2 Data Integrity Audit
        Specific Problem: Data mismatches detected
        Description: The SESM audit: V5.2 Data Integrity Audit, has 5 unresolved
        problems. To view and correct the problems, open the audit problem repo
        rt from the Audit System found under the SESM Maintenance menu item.
```

NTSTD

The following is an example of a V5.2 Data Audit log in NTSTD format:

```
COMPACT06BT ***  CMT300 Feb15 07:12:48 0002 TBL  CMT Fault
```

```
Location: Audit
NotificationID: 1002
State: Raise
Category: Processing Error
Cause: Corrupt data
Time: Feb 14 23:12:48 2004
Component Id: SESM=AuditSystem;Audit=V5.2 Data Integrity Audit
Specific Problem: Data mismatches detected
Description: The SESM audit: V5.2 Data Integrity Audit, has 5 unresolved
problems. To view and correct the problems, open the audit problem repo
rt from the Audit System found under the SESM Maintenance menu item.
```

SNMP

The following is an example of a V5.2 Data Audit log in SNMP format:

```
system.sysUpTime.0 => 3:05:01
snmpTrapOID.0 => nnExtAlarmCritical
alarmActiveResourceId =>
.1.3.6.1.2.1.111.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.20.50.48
.48.52.45.49.45.50.49.44.54.58.52.49.58.49.52.46.48.44.8995
alarmActiveDateAndTime => 2004-1-21,6:41:14.0,
alarmActiveDescription => DeviceSpecificInfo=;Event from Unknown Syslog Device
nnExtAlarmActiveEventType => 5
nnExtAlarmActiveProbableCause => 118
nnExtAlarmActiveAdditionalText =>
nnExtAlarmActiveDocumentationPointer => CMT 300
nnExtAlarmActiveResourceDescription => IEMS=zsups228;SESM=AuditSystem;Audit=V5.2 Data
Integrity Audit
nnExtAlarmActiveManualClear => 2
nnExtAlarmActiveSequenceNumber => 1
```

Syslog

The following is an example of a V5.2 Data Audit log in Syslog format:

```
Feb 14 23:12:50 zsups228 IEMS: _V2_~I=~H=zsups228~A=IEMS~S=0008~~ CMT300 CRIT TBL CMT
Fault^M Location: Audit^M NotificationID: 1002^M State: Raise^M
Category: Processing Error^M Cause: Corrupt data^M Time: Feb 14 23:12:48
2004^M Component Id: SESM=AuditSystem;Audit=V5.2 Data Integrity Audit^M
Specific Problem: Data mismatches detected^M Description: The SESM audit: V5.2
Data Integrity Audit, has 5 unresolved^M problems. To view and correct the
```

```
problems, open the audit problem repo^M        rt from the Audit System found under
the SESM Maintenance menu item.^M
```

Performance

OM and PM Documentation references for V5.2 Data Audit

- There are no performance measurements for V5.2 Data Audit V5.2 Data Audit

Northbound OM/PM Formats

This section provides example output of Performance Measurement data in each of the Northbound formats provided

XML

The following is an example of Performance data for V5.2 Data Audit in XML format:

Note: *Northbound performance interface not supported for this component.*

CSV

The following is an example of Performance data for V5.2 Data Audit in CSV format:

Note: *Northbound performance interface not supported for this component.*

GUI/CLUI Documentation for V5.2 Data Audit

GUI Launching and User procedures

Related documents

- NN10083-911 - CS2000 Fault Management
- NN10402-600 - ATM/IP Solution-level Administration and Security
- NN10409-500 - ATM/IP Solution-level Configuration Management
- NIS V208-1 - V5.2 Interface Specification for CS2000

References

Fault Specifications

[1] Syslog Protocol (RFC 3164): http://www.ietf.org/rfc/rfc3164.txt

[2] Alarm MIB (draft): http://www.ietf.org/html.charters/disman-charter.html

[3] Notification Log MIB (RFC 3014): http://www.ietf.org/rfc/rfc3014.txt?number=3014

OAM&P Security

[4] NN10402-600 - ATM/IP Solution-level Administration and Security

Network Engineering

[5] <SN08 SEB number> - IAC Engineering Guidelines

[6] <SN08 SEB number> - IAW Engineering Guidelines

[7] <SN08 SEB number> - UAIP Engineering Guidelines

[8] <SN08 SEB number> - PT-IP Engineering Guidelines

[9] <SN08 SEB number> - VoATM Engineering Guidelines

[10] <SN08 SEB number> - TRIMODAL Engineering Guidelines

Industry Standards

PAM

[11] Introduction to PAM: http://docs.sun.com/db/doc/805-7229/6j6q8svdi?q=pam.conf&a=view

[12] PAM RFC from OpenGroup: http://www.opengroup.org/tech/rfc/mirror-rfc/rfc86.0.txt

[13] pam.conf (Solaris 8): http://docs.sun.com/db/doc/806-0633/6j9vn6q5t?q=pam.conf&a=view

NSSwitch

[14] Solaris Name Services: http://docs.sun.com/db/doc/806-1387/6jam6926b?q=nsswitch&a=view

[15] nsswitch.conf (Solaris 8): http://docs.sun.com/db/doc/806-0633/6j9vn6q5m?q=nsswitch&a=view

Secure Shell (SSH)

[16] Secure Shell (secsh) Internet Drafts: http://www.ietf.org/html.charters/secsh-charter.html

[17] OpenSSH: http://www.openssh.org

SNMP V3/USM

[18] An Architecture for Describing SNMP Management Frameworks (RFC3411): http://www.ietf.org/rfc/rfc3411.txt?number=3411

[19] User-based Security Model (RFC3414): http://www.ietf.org/rfc/rfc3414.txt?number=3414

[20] View-based Access Control Model (RFC3415): http://www.ietf.org/rfc/rfc3415.txt?number=3415

HTTPS

[21] The SSL Protocol V3.0: http://wp.netscape.com/eng/ssl3/ssl-toc.html

[22] Transport Layer Security (TLS) Extensions (RFC2246): http://www.ietf.org/rfc/rfc3546.txt

[23] HTTP over TLS (RFC 2818): http://www.ietf.org/rfc/rfc2818.txt

[24] OpenSSL: http://www.openssl.org

IEMS Appendix 1: Northbound OSS Configurations

Depending on customer requirements, a single-source OSS interface can be provided from the IEMS server. As an alternate configuration, to support customer transition, some NE specific OSS interfaces can be provided via SDM in parallel with the interfaces provided by IEMS.

For some existing Nortel Networks ATM customers with no new equipment (such as VTOA-AAL1 solutions with only MG4K, PP15K-MSS and XA-Core), the SDM can provide the complete set external interface to third party OSSs. This configuration is only supported for solutions frozen in the SN06 hardware configuration.

In normal configuration, the IEMS is configured to forward all of its collected faults to the OSS through its aggregated interface. The aggregated interface can supply the feed in NTSTD, SCC2, Syslog or SNMP (v2 or v3) format.

The alternate SDM feed can optionally, in addition to the IEMS feed, provide fault streams equivalent to the SN06 steams for the following devices. Use of the optional SDM feed is not required:

- GWC - via GWC Mgr (SESM) on SSPFS via custlog to SDM
- SAM21 - via SAM21 Mgr on SSFPS via custlog to SDM
- UAS - via UAS Mgr (SESM) on SSPFS via custlog to SDM
- PVG (MG7K, MG15K) - via MDM to passport log streamer to SDM
- Passport 15K MSS - via MDM to passport log streamer to SDM

Note: All of the streams above also go into IEMS for proper IEMS GUI and security operation. OSSs will still connect to IEMS for any of the other equipment in the portfolio. IEMS can block OSS delivery of the alternate feeds northbound if the same OSS is also connected to the SDM to prevent duplication.

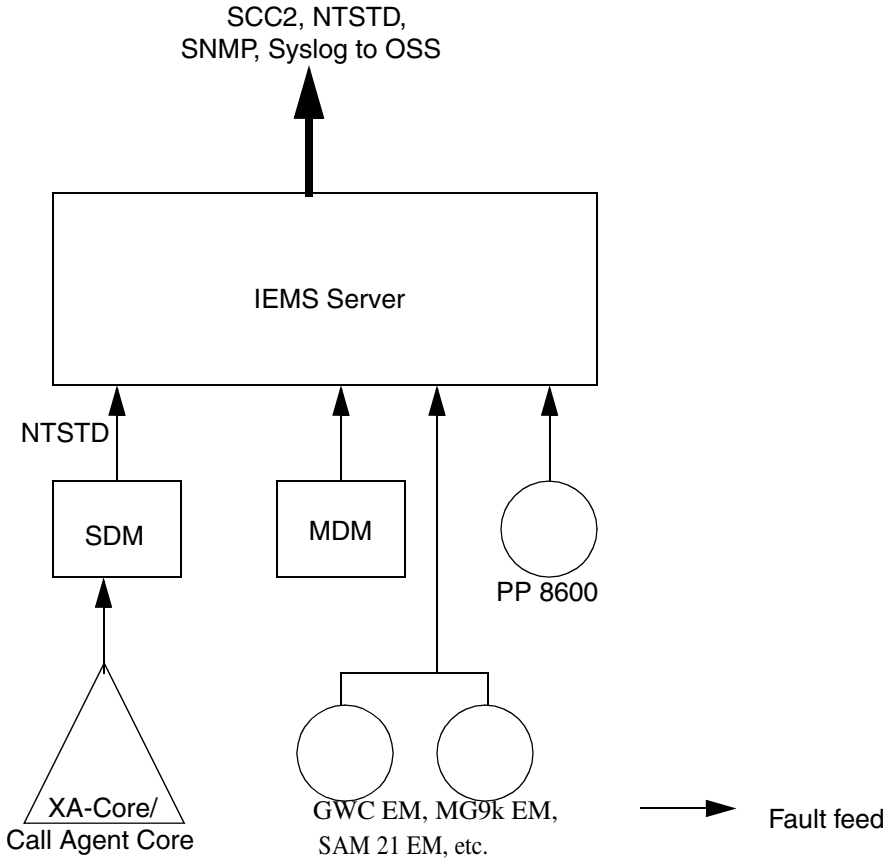
These are in addition to fault streams which can originate from SDM and are supported in all configurations, including TDM only and VTOA-AAL1 solutions:

- CM (XA-Core or Compact) - via SDM
- SDM platform and applications - via SDM

All other fault streams are only supported via IEMS as of SN07. (including but not limited to STORM, CICM, SSPFS Platforms, MS20x0, NGSS

(SSTrunks), SSLines, RTP MP (BCP 7100), MAS, PP8600, MCS System Manager).

Fault flow with IEMS as Northbound interface (typical)



Note: The SDM SCC2 and NTSTD logroute streams must be configured for SCC2_old or NTstd_old. This is a change from SN06.2

This figure shows the fault flows in an office where the IEMS will be the northbound interface. In this configuration, all the devices that have been implemented in IEMS forward their fault information to IEMS. The SDM will only be responsible for forwarding core faults to the IEMS.

Note: The SDM logroute stream must be configured from tcpin.

IEMS Appendix 2: Nortel Alarm Extension MIB

```
-- Draft Version

NORTEL-ALARM-EXT-MIB

DEFINITIONS ::= BEGIN

   IMPORTS
       nortelGenericMIBs FROM NORTEL-GENERIC-MIB
       alarmActiveEntry, alarmActiveResourceId, alarmActiveDescription,
       ResourceId, alarmActiveDateAndTime
                                    FROM ALARM-MIB
       IANAItuEventType, IANAItuProbableCause
                                    FROM IANA-ITU-ALARM-TC
       AdminState, OperState, UsageState,
       AlarmStatus, StandbyStatus    FROM ENTITY-STATE-MIB
      nlmLogName, nlmLogIndex      FROM NOTIFICATION-LOG-MIB
       NOTIFICATION-GROUP            FROM SNMPv2-CONF
       DateAndTime, DisplayString    FROM SNMPv2-TC
       SnmpAdminString               FROM SNMP-FRAMEWORK-MIB
       MODULE-IDENTITY, OBJECT-IDENTITY,
       OBJECT-TYPE, NOTIFICATION-TYPE,
       Unsigned32
                                    FROM SNMPv2-SMI;


   nnExtAlarmMIB  MODULE-IDENTITY
       LAST-UPDATED "200401270000Z"
       ORGANIZATION "Nortel Networks"
       CONTACT-INFO
              "     Nortel Networks
                    8200 Dixie Road
                    Brampton, Ontario L6T 5P6
                    Canada

                    1-800-4Nortel
```

```
                    www.nortelnetworks.com "
       DESCRIPTION
              "This module contains objects that extend the IETF Alarm MIB, including
notifications."

       -- Revision history

       REVISION "200401270000Z"
       DESCRIPTION
                " Initial version"

       ::= { nortelGenericMIBs 6 }

  nnExtAlarmObjects  OBJECT IDENTIFIER ::= { nnExtAlarmMIB 1 }
  nnExtAlarmConformance  OBJECT IDENTIFIER ::= { nnExtAlarmMIB 2 }
  nnExtAlarmCompliances  OBJECT IDENTIFIER ::= { nnExtAlarmConformance 1 }
  nnExtAlarmGroups  OBJECT IDENTIFIER ::= { nnExtAlarmConformance 2 }


  -- Textual Convetions

  NnAvailabilityStatus  ::=  TEXTUAL-CONVENTION
       STATUS         current
       DESCRIPTION
            "Represents the availability status"
       SYNTAX INTEGER {
        notSupported (1),
      inTest (2),
      failed (3),
      powerOff (4),
      offLine (5),
      offDuty (6),
      dependency (7),
      degraded (8),
      notInstalled (9),
      logFull (10)
   }

  NnControlStatus  ::=  TEXTUAL-CONVENTION
```

```
      STATUS         current
      DESCRIPTION
           "Represents the control status"
      SYNTAX INTEGER {
       notSupported (1),
    subjectToTest (2),
    partOfServiceLocked (3),
    reservedForTest (4),
    suspended (5)
 }

NnProceduralStatus  ::=  TEXTUAL-CONVENTION
     STATUS         current
     DESCRIPTION
          "Represents the procedural status"
     SYNTAX INTEGER {
      notSupported (1),
     initializationRequired (2),
    notInitialized (3),
    initializing (4),
    reporting (5),
    terminating (6)
 }

NnUnknownStatus  ::=  TEXTUAL-CONVENTION
     STATUS         current
     DESCRIPTION
          "The unknown status attribute is used to indicate that
          the state of the resource represented by the managed object
          is unknown. When the unknown status attribute value is
          true, the value of the state attributes may not reflect
          the actual state of the resource."
 SYNTAX     INTEGER {
      false(1),
      true(2)
   }
```

```
-- Nortel Extended Active Alarm Table

 nnExtAlarmActiveTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF NnExtAlarmActiveEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table contains additional information about active alarms than
        what is found in the IETF Alarm MIB."
    ::= { nnExtAlarmObjects 1 }

nnExtAlarmActiveEntry OBJECT-TYPE
    SYNTAX      NnExtAlarmActiveEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An active alarm entry"
    AUGMENTS { alarmActiveEntry }
    ::= { nnExtAlarmActiveTable 1 }

 NnExtAlarmActiveEntry ::= SEQUENCE {
    nnExtAlarmActiveEventType                    IANAItuEventType,
    nnExtAlarmActiveProbableCause                IANAItuProbableCause,
    nnExtAlarmActiveAdditionalText               SnmpAdminString,
    nnExtAlarmActiveDocumentationPointer         SnmpAdminString,
    nnExtAlarmActiveResourceDescription          SnmpAdminString,
    nnExtAlarmActiveManualClear                  INTEGER,
    nnExtAlarmActiveSequenceNumber               Integer32
          }

   nnExtAlarmActiveEventType OBJECT-TYPE
    SYNTAX       IANAItuEventType
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
             "Represents the per active alarm instance event type values."
     REFERENCE
         "ITU Recommendation M.3100, 'Generic Network Information
```

```
                Model', 1995
             ITU Recommendation X.733, 'Information Technology - Open
                Systems Interconnection - System Management: Alarm
                Reporting Function', 1992
             ITU Recommendation X.736, 'Information Technology - Open
                Systems Interconnection - System Management: Security
                Alarm Reporting Function', 1992"
      ::= { nnExtAlarmActiveEntry 1 }

   nnExtAlarmActiveProbableCause OBJECT-TYPE
      SYNTAX      IANAItuProbableCause
      MAX-ACCESS  read-write
      STATUS       current

       DESCRIPTION
               "Per active alarm instance ITU probable cause values."
       REFERENCE
           "ITU Recommendation M.3100, 'Generic Network Information
                Model', 1995
             ITU Recommendation X.733, 'Information Technology - Open
                Systems Interconnection - System Management: Alarm
                Reporting Function', 1992
             ITU Recommendation X.736, 'Information Technology - Open
                Systems Interconnection - System Management: Security
                Alarm Reporting Function', 1992"
      ::= { nnExtAlarmActiveEntry 2 }


   nnExtAlarmActiveAdditionalText OBJECT-TYPE
      SYNTAX  SnmpAdminString
      MAX-ACCESS read-write
      STATUS     current
      DESCRIPTION
               "Represents the per active alarm instanace additional text
               field."
       REFERENCE
           "ITU Recommendation M.3100, 'Generic Network Information
                Model', 1995
```

```
            ITU Recommendation X.733, 'Information Technology - Open
               Systems Interconnection - System Management: Alarm
               Reporting Function', 1992"
      ::= { nnExtAlarmActiveEntry 3}

  nnExtAlarmActiveDocumentationPointer OBJECT-TYPE
      SYNTAX      SnmpAdminString
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
               "This object servces as a pointer to documentation related to this
               problem.

               If there is no specific document pointer for this alarm, this object
               is a null length string."
      ::= { nnExtAlarmActiveEntry 4 }

  nnExtAlarmActiveResourceDescription OBJECT-TYPE
      SYNTAX      SnmpAdminString
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
           "This is a textual description of the resource under
            under alarm.

            The format of the string is as follows:

NEtype=NEname;componentType=componentInstanceId;subcompType=subcompInstanceId;....

          With NE as the root, the entire containment with the list of Relative
          Distinguished Names (RDNs) is presented upto the
           point where the alarming component is clearly identified.
           Semicolon is the delimiter between a 'category=value' pair.
           The string can only contain alphanumeric characters and
           underscores. No commas, spaces, slashes, hyphens, or
           dollar signs are allowed
               "
      ::= { nnExtAlarmActiveEntry 5 }
```

```
nnExtAlarmActiveManualClear OBJECT-TYPE
    SYNTAX      INTEGER {
         other (1),
         forbidden (2),
         required (3),
         optional (4)
         }
    MAX-ACCESS  read-only
    STATUS       current
    DESCRIPTION
              "This object provides guidance to a mid-level manager
              on the handling of this alarm. A value of forbidden
              indicates that a mid-level manager MUST NOT allow
              this alarm to be manually cleared. A value of
              required indicates that this alarm has no corresponding
              clear so MUST always be manually cleared. A value of
              optional indicates that this alarm does have a corresponding
              clear, but that is MAY also be cleared manually. A value of
              other indicates that the manual clear status is either
              unknown or not one of the specified values."
     ::= { nnExtAlarmActiveEntry 6 }

nnExtAlarmActiveSequenceNumber OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS       current
    DESCRIPTION
              "The sequence number of this notification. This object
              MUST have a value of 0 for notifications without
              sequence numbers or solutions that don't support
              sequence numbers."
    DEFVAL { 0 }
     ::= { nnExtAlarmActiveEntry 7 }

-- Nortel Extended Alarm State Information

   nnExtAlarmStateTable OBJECT-TYPE
```

```
    SYNTAX      SEQUENCE OF NnExtAlarmStateEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "This table contains state information about active alarms than
        what is found in the IETF Alarm MIB."
    ::= { nnExtAlarmObjects 2 }

nnExtAlarmStateEntry OBJECT-TYPE
    SYNTAX      NnExtAlarmStateEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An active alarm state entry"
    AUGMENTS { alarmActiveEntry }
    ::= { nnExtAlarmStateTable 1 }

NnExtAlarmStateEntry ::= SEQUENCE {
 nnExtAlarmStateAdministrative   AdminState,
 nnExtAlarmStateOperational      OperState,
 nnExtAlarmStateUsage            UsageState,
 nnExtAlarmStateAlarm            AlarmStatus,
 nnExtAlarmStateAvailability     NnAvailabilityStatus,
 nnExtAlarmStateControl          NnControlStatus,
 nnExtAlarmStateProcedural       NnProceduralStatus,
 nnExtAlarmStateStandby          StandbyStatus,
 nnExtAlarmStateUnknown          NnUnknownStatus
}

 nnExtAlarmStateAdministrative OBJECT-TYPE
    SYNTAX      AdminState
    MAX-ACCESS  read-only
    STATUS       current
    DESCRIPTION
             ""
     ::= { nnExtAlarmStateEntry 1 }

  nnExtAlarmStateOperational OBJECT-TYPE
```

```
      SYNTAX      OperState
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
               ""
       ::= { nnExtAlarmStateEntry 2 }

   nnExtAlarmStateUsage OBJECT-TYPE
      SYNTAX      UsageState
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
               ""
       ::= { nnExtAlarmStateEntry 3 }

    nnExtAlarmStateAlarm OBJECT-TYPE
      SYNTAX      AlarmStatus
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
               ""
       ::= { nnExtAlarmStateEntry 4 }

   nnExtAlarmStateAvailability OBJECT-TYPE
      SYNTAX      NnAvailabilityStatus
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
               ""
       ::= { nnExtAlarmStateEntry 5 }

    nnExtAlarmStateControl OBJECT-TYPE
      SYNTAX      NnControlStatus
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
               ""
       ::= { nnExtAlarmStateEntry 6 }
```

```
   nnExtAlarmStateProcedural OBJECT-TYPE
      SYNTAX      NnProceduralStatus
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
                ""
       ::= { nnExtAlarmStateEntry 7 }

    nnExtAlarmStateStandby OBJECT-TYPE
      SYNTAX      StandbyStatus
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
                ""
       ::= { nnExtAlarmStateEntry 8 }

    nnExtAlarmStateUnknown OBJECT-TYPE
      SYNTAX      NnUnknownStatus
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
                ""
       ::= { nnExtAlarmStateEntry 9 }

  -- Table of Information related to Messages

     nnExtAlarmMessageTable OBJECT-TYPE
      SYNTAX      SEQUENCE OF NnExtAlarmMessageEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
          "A table of information on messages. Entries are
          added to this table when their corresponding
          notifications have been sent. Entires will be
          removed from this table as outlined in the
          Notification Log MIB [RFC3014]. Implementations
          that do not support the Notification Log MIB should
```

```
          provide behaviour for nlmLogName, nlmLogIndex and
          this table as if they did."
      ::= { nnExtAlarmObjects 3 }

  nnExtAlarmMessageEntry OBJECT-TYPE
      SYNTAX      NnExtAlarmMessageEntry
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
          "An alarm message entry."
      INDEX       { nlmLogName, nlmLogIndex }
      ::= { nnExtAlarmMessageTable 1 }

   NnExtAlarmMessageEntry ::= SEQUENCE {
       nnExtAlarmMessageResource             ResourceId,
       nnExtAlarmMessageResourceDescription  SnmpAdminString,
       nnExtAlarmMessageDateAndTime          DateAndTime,
       nnExtAlarmMessageDocumentationPointer SnmpAdminString,
       nnExtAlarmMessageInfo                 SnmpAdminString
    }

    nnExtAlarmMessageResource    OBJECT-TYPE
      SYNTAX      ResourceId
      MAX-ACCESS  read-only
      STATUS      current
      DESCRIPTION
         "This object identifies the resource that this message pertains to

         If there is no corresponding resource, then
         the value of this object MUST be 0.0."
      ::= { nnExtAlarmMessageEntry 1 }

     nnExtAlarmMessageResourceDescription OBJECT-TYPE
      SYNTAX      SnmpAdminString
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
           "This is a textual description of the resource this message
```

```
           pertains to.

            The format of the string is as follows:

NEtype=NEname;componentType=componentInstanceId;subcompType=subcompInstanceId;....

           With NE as the root, the entire containment with the list of Relative
           Distinguished Names (RDNs) is presented upto the
            point where the messaging component is clearly identified.
            Semicolon is the delimiter between a 'category=value' pair.
            The string can only contain alphanumeric characters and
            underscores. No commas, spaces, slashes, hyphens, or
            dollar signs are allowed
               "
       ::= { nnExtAlarmMessageEntry 2 }



   nnExtAlarmMessageDateAndTime OBJECT-TYPE
      SYNTAX      DateAndTime
      MAX-ACCESS  not-accessible
      STATUS      current
      DESCRIPTION
          "The local date and time when the message originated.

          Implementations MUST include the offset from UTC,
          if available.  Implementation in environments in which
          the UTC offset is not available is NOT RECOMMENDED."
      ::= { nnExtAlarmMessageEntry 3 }

    nnExtAlarmMessageDocumentationPointer OBJECT-TYPE
      SYNTAX      SnmpAdminString
      MAX-ACCESS  read-only
      STATUS       current
      DESCRIPTION
               "This object servces as a pointer to documentation related to this
               problem.

               If there is no specific document pointer for this alarm, this object
```

```
                is a null length string."
        ::= { nnExtAlarmMessageEntry 4 }

   nnExtAlarmMessageInfo OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A textual discription of the event that has occurred,
            suitable to display to an operator. "
    ::= { nnExtAlarmMessageEntry 5 }


  -- all notification OIDs would be prefixed with a zero OID to
  -- facilitate  snmp v1<->v2 conversion

  nnExtNotificationPrefix  OBJECT-IDENTITY
           STATUS         current
           DESCRIPTION
                  "This OID represents the prefix branch for all Nortel ITU
                   Alarm  Notifications.
                   The last but one sub identifier in the OID of
                   any Notification must have the value zero to facilitate
                   v2<-->v1 conversion."
           ::=  {nnExtAlarmObjects  0 }

 -- Alarm  Notifications

          nnExtAlarmClear NOTIFICATION-TYPE
                          OBJECTS { alarmActiveResourceId,
                                    alarmActiveDateAndTime,
                                    alarmActiveDescription,
                                    nnExtAlarmActiveEventType,
                                    nnExtAlarmActiveProbableCause,
                 nnExtAlarmActiveAdditionalText,
                                    nnExtAlarmActiveDocumentationPointer,
                                    nnExtAlarmActiveResourceDescription,
                                    nnExtAlarmActiveSequenceNumber
```

```
                        }
  STATUS  current
  DESCRIPTION
    "This notification indicates that one or more previously
     reported alarms have been cleared and the previously reported
     alarms are identified via the correlation id list field.
     The varbinds include alarm context via the ComponentId field
     and other additional useful information."


::= { nnExtNotificationPrefix 301 }


nnExtAlarmWarning NOTIFICATION-TYPE
                OBJECTS { alarmActiveResourceId,
                          alarmActiveDateAndTime,
                          alarmActiveDescription,
                          nnExtAlarmActiveEventType,
                          nnExtAlarmActiveProbableCause,
        nnExtAlarmActiveAdditionalText,
                          nnExtAlarmActiveDocumentationPointer,
                          nnExtAlarmActiveResourceDescription,
                          nnExtAlarmActiveManualClear,
                          nnExtAlarmActiveSequenceNumber
                        }
  STATUS  current
  DESCRIPTION
    "This notification indicates that an alarm of 'Warning' severity
     has been raised on a NE.
     The varbinds include alarm context via the ComponentId field
     and other additional useful information on the alarm condition."


::= { nnExtNotificationPrefix 302 }


nnExtAlarmMinor NOTIFICATION-TYPE
                OBJECTS { alarmActiveResourceId,
```

```
                            alarmActiveDateAndTime,
                            alarmActiveDescription,
                            nnExtAlarmActiveEventType,
                            nnExtAlarmActiveProbableCause,
          nnExtAlarmActiveAdditionalText,
                            nnExtAlarmActiveDocumentationPointer,
                            nnExtAlarmActiveResourceDescription,
                            nnExtAlarmActiveManualClear,
                            nnExtAlarmActiveSequenceNumber
                          }
    STATUS  current
    DESCRIPTION
      "This notification indicates that an alarm of 'Minor' severity
       has been raised on a NE.
       The varbinds include alarm context via the ComponentId field
       and other additional useful information on the alarm condition."


::= { nnExtNotificationPrefix 303 }



nnExtAlarmMajor NOTIFICATION-TYPE
                  OBJECTS { alarmActiveResourceId,
                            alarmActiveDateAndTime,
                            alarmActiveDescription,
                            nnExtAlarmActiveEventType,
                            nnExtAlarmActiveProbableCause,
          nnExtAlarmActiveAdditionalText,
                            nnExtAlarmActiveDocumentationPointer,
                            nnExtAlarmActiveResourceDescription,
                            nnExtAlarmActiveManualClear,
              nnExtAlarmActiveSequenceNumber
                          }
    STATUS  current
    DESCRIPTION
      "This notification indicates that an alarm of 'Major' severity
       has been raised on a NE.
```

```
      The varbinds include alarm context via the ComponentId field
      and other additional useful information on the alarm condition."


::= { nnExtNotificationPrefix 304 }


nnExtAlarmCritical NOTIFICATION-TYPE
                OBJECTS { alarmActiveResourceId,
                          alarmActiveDateAndTime,
                          alarmActiveDescription,
                          nnExtAlarmActiveEventType,
                          nnExtAlarmActiveProbableCause,
        nnExtAlarmActiveAdditionalText,
                          nnExtAlarmActiveDocumentationPointer,
                          nnExtAlarmActiveResourceDescription,
                          nnExtAlarmActiveManualClear,
            nnExtAlarmActiveSequenceNumber
                        }
  STATUS  current
  DESCRIPTION
    "This notification indicates that an alarm of 'Critical' severity
     has been raised on a NE.
     The varbinds include alarm context via the ComponentId field
     and other additional useful information on the alarm condition."


::= { nnExtNotificationPrefix 305 }

nnExtAlarmMessage NOTIFICATION-TYPE
                OBJECTS {
                        nnExtAlarmMessageResource,
                        nnExtAlarmMessageResourceDescription,
                        nnExtAlarmMessageDateAndTime,
                        nnExtAlarmMessageDocumentationPointer,
                        nnExtAlarmMessageInfo
                        }
  STATUS  current
```

```
            DESCRIPTION
              "An informational message. This notification does not
              correspond to an alarm so would not be stored in the
              active alarm table and it does not have a corresponing
              clear."
           ::= { nnExtNotificationPrefix 306 }

-- Notification group definitions


    nnExtAlarmNotificationsGroup NOTIFICATION-GROUP
           NOTIFICATIONS  {
                          nnExtAlarmClear,
                          nnExtAlarmWarning,
                          nnExtAlarmMinor,
                          nnExtAlarmMajor,
                          nnExtAlarmCritical
                          }
           STATUS   current
           DESCRIPTION
                " Nortel alarm notification group."
           ::= { nnExtAlarmGroups 1}

    nnExtAlarmGroup OBJECT-GROUP
           OBJECTS  {
                          nnExtAlarmActiveEventType,
                          nnExtAlarmActiveProbableCause,
                          nnExtAlarmActiveAdditionalText,
                          nnExtAlarmActiveDocumentationPointer,
                          nnExtAlarmActiveResourceDescription,
                          nnExtAlarmActiveManualClear,
                          nnExtAlarmActiveSequenceNumber
                          }
           STATUS   current
           DESCRIPTION
                " Nortel alarm  group."
           ::= { nnExtAlarmGroups 2}
```

```
     nnExtAlarmStateGroup OBJECT-GROUP
           OBJECTS {
           nnExtAlarmStateAdministrative,
          nnExtAlarmStateOperational,
          nnExtAlarmStateUsage,
          nnExtAlarmStateAlarm,
          nnExtAlarmStateAvailability,
          nnExtAlarmStateControl,
          nnExtAlarmStateProcedural,
          nnExtAlarmStateStandby,
           nnExtAlarmStateUnknown
       }
      STATUS   current
           DESCRIPTION
                " Nortel  alarm state group."
           ::= { nnExtAlarmGroups 3}

     nnExtAlarmMessageGroup OBJECT-GROUP
         OBJECTS {
         nnExtAlarmMessageResource,
         nnExtAlarmMessageInfo,
         nnExtAlarmMessageDocumentationPointer,
         nnExtAlarmMessageDateAndTime,
         nnExtAlarmMessage
         }
     STATUS   current
           DESCRIPTION
                " Nortel  alarm message group."
           ::= { nnExtAlarmGroups 4}

-- Compliance
 nnExtAlarmCompliance MODULE-COMPLIANCE
     STATUS current
     DESCRIPTION
          "The compliance statement for entities which implement
          the Nortel Alarm MIB."
     MODULE    -- this module
          MANDATORY-GROUPS {
```

```
                nnExtAlarmGroup
            }
    ::= { nnExtAlarmCompliances 1}
END
```

Chapter 3: IP, ATM, TDM solutions feature descriptions

(I)SN09 Feature Deltas

Product = CS 2000

A89007819--QoS Reporting: QoS Collector Application (QCA)

Functional Description

1: Applicable Solution(s)

PT-IP, IAW, IAC, Int'l PT-IP, Int'l IAW, Int'l IAC

1.1 Description

This document covers the QoS Collector Application functionality supported in SN09 time frame.

In Voice over IP/ATM networks, Quality of Service (QoS) can be adversely affected by the components in the network. Unlike TDM networks where the voice quality is consistent for all calls, VoIP/ATM networks can experience different voice quality on all calls.

The common parameters that make up voice quality are;

- Packets sent
- Packets received
- Packet loss
- Octets sent
- Octets received
- Inter-arrival latency

- Jitter

All gateways beginning SN06 VoIP solutions report these statistics via end-of-call reporting mechanisms specific to the protocol used for MGC - VMG communication.

It is the purpose of this activity is to design a method for reporting these QoS parameters on a per call basis for the purposes of;

- Network engineering
- Trend analysis
- Trouble-shooting network problems
- SLA validation

This is accomplished by implementing a reporting mechanism that will allow QoS reports (as IPDR records) to be delivered to a customer provided OSS for processing. In order to achieve SLA validation, QoS reports are correlated to appropriate billing records so that the QoS of billed calls can be determined.

QoS Reporting is applicable for more then just VoIP networks. It can be used in hybrid networks as well. From SN06 time frame to SN08 time frame QoS Reporting was limited to pure IP networks which consist only of GWC driven GWs.

Support for SPM peripherals and hybrid networks will be accomplished in a later release.

The proposed architecture for QoS Reporting beginning SN06 consists of the following components;

1. QoS Correlation ID and billing
2. QoS Reporting Application (on GWC)
3. Provisioning
4. QoS Report collection
5. QoS Report processing

This activity implements component 4. QoS Report collection, the QoS Collector Application (QCA).

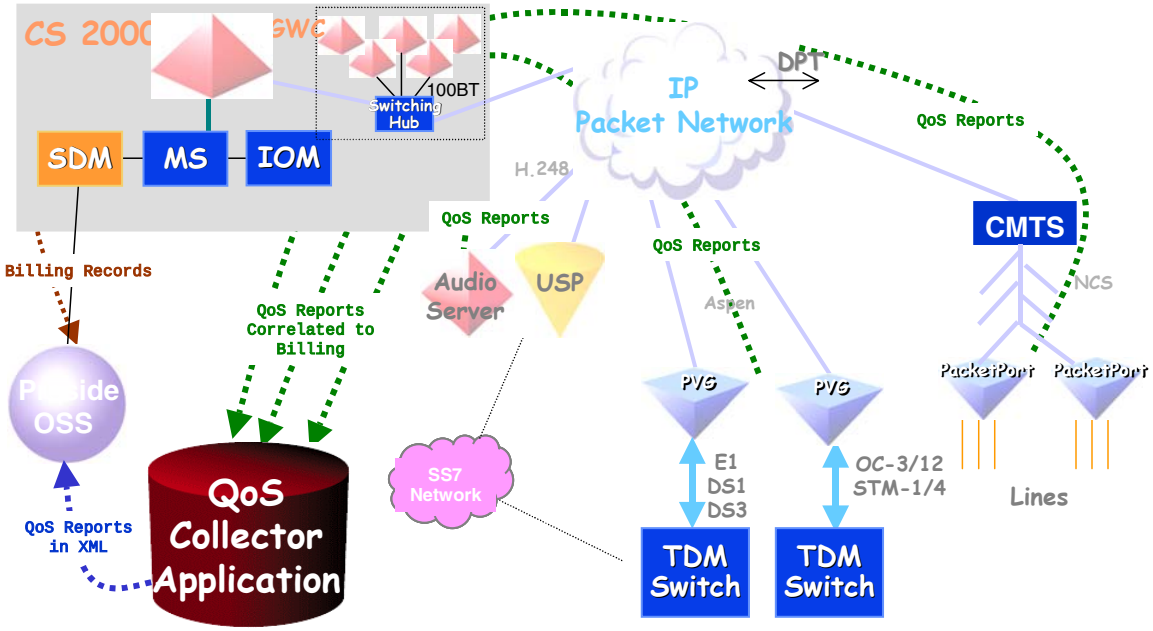
1.1.1 System behavior

All QoS (IPDR) records are stored on a QoS Collector Application (QCA) host. The QCA will receive binary QoS records from the GWCs,

converts these to QCA IPDR records and stores them in a file. The QCA IPDR records can be obtained by the OSS for processing.

The configuration of this proposal is shown in Figure 1, "QoS Reporting in a VoIP/ATM Network".

Figure 1 QoS Reporting in a VoIP/ATM Network



1.1.2 Configuration

The configuration details for the QoS Collector Application are provided by a properties files. The properties file is located at /opt/nortel/qca/properties/qca.properties and can be configured by the user.

The QCA properties are given in Table 1, “QCA properties,” on page 783 and an example QCA properties file is given in Figure 2, "Example of the QCA properties file".

Table 1 QCA properties

Name	Description	Units	Range	default
portNumber[3]	the port number the QCA accepts connections on	N/A	20000 to 20004	20000
MaxFileSize	maximum size of an output file	MBytes	1 to 100	1

Table 1 QCA properties

Name	Description	Units	Range	default
MaxFileTime	interval output file is open	minutes	1 to 240	15
RetainFileTime	how long the output files should be retained	days	1 to 30	5
recycleToD	the hour in the day the directories will be recycled	hour	0 to 23	0
fileExt	the output file extension	N/A	String	xml
nodeName	the node name to be used in the output files	N/A	String	QCA
closedFileCompression[1]	whether the file should be compressed when closed and moved to today	boolean	true or false	true
oldFileCompression[1,2]	whether the files should be compressed at the first directory recycle	boolean	true or false	true

Notes:

1. File compression may be required as there is limited disk space for QCA IPDR record storage.
2. If *closedFileCompression* is true the value of the *oldFileCompression* property is negated as the files will have already been compressed.
3. A range of port numbers is provided for flexibility. The main use is for upgrade purposes, where two QCA instance may be running on a single host. Multiple QCAs, and therefore port numbers, should not be used to segregate QCA traffic.

The qca.properties file is read when the QCA is started, therefore the QCA must be stopped and restarted for changes in the qca.properties to be picked up.

When the qca.proprties file is read the contents is validated. If any of the properties are not present or invalid, the default value is automatically used. A warning customer log is generated to indicate that the default value is being used.

An example customer log warning:

```
Oct 11 12:00:02 wmdhs0j8 main:0001 QCA201 WARNING init label:
RetainFileTime property in properties/qca.properties is out of
range. QCA is starting with default retain file time of 5 days
```

Figure 2 Example of the QCA properties file

```
# QCA Properties file
# The QCA will have to be restarted for changes in the properties
# file to be reflected in the application's operation

# The maximum size of a file, in MBytes, before it is closed
# Range is 1 to 100. Default is 1.
  MaxFileSize=1

# The maximum time, in minutes, a file can be open before
# it is closed
# Range is 1 to 240. Default is 15.
  MaxFileTime=15

# Hour of the day that the directory structure is recycled
# Range 0 (12:00 AM) to 23 (11:00 PM). Default is 0 (12:00 AM).
# Do NOT specify minutes.
  recycleToD=0

# port number to start application on.
# Range is 20000 to 20004. Default is 20000.
  portNumber=20000

# How long, in days, the files are kept before deleting
# VERY IMPORTANT: Depending on the call volume and the number of
# days for file retention it could be possible to exhaust all
# available disk space, therefore the value of this property
# should be considered in great depth.If QCA is started with
# the value of this property less than the number of today
# directories for a given port the older directories will be
# deleted.
# Range 1 to 30. Default is 5.
  RetainFileTime=5

# File Extension used in the QCA output file name.
# Default is xml.
  fileExt=xml

# Node name to be used in the QCA output file name.
# Default is QCA.
  nodeName=QCA

# true or false value indicating whether the output file
# should be compressed when closed. Default is true.
  closedFileCompression=true

# true or false value indicating whether the file should be
# compressed at the first directory recycle
# Note: If closedFileCompression is true the value of the
# oldFileCompression property is negated as the files will have
```

1.1.3 Starting QCA

The `qca_server` script is used to start the QCA. The user should log in as root to execute this script.

When the `qca_server` script is run the following warning is displayed:

```
Attempting to register QCA as Qca with PMFADM.
```

If a QCA instance has not already been started with `qca_server` the following message is displayed:

```
Registration as Qca was ok. QCA started.
```

If a QCA instance has already been started with `qca_server` the following message is displayed:

```
pmfadm: Request "Qca" already queued
Could not register QCA as Qca with PMFADM, this suggests a QCA
instance is already running.
```

When the QCA is started the following steps are performed:

- the QCA is registered with PMFADM (processes monitor facility administration).

  This is a Solaris utility that monitors register processes and restarts the process if no longer running.

- configuration details (qca.properties file) are read

  If any of the properties information is not present or is invalid the default value is used and a customer log is generated to indicate this. It is at this point the user can stop the QCA if using default values is not acceptable.

- the QCA attempts to open a server socket on the specified port.

  If the specified port is in use the QCA can not be started.

- a file management process is started

  If the QCA output directory is not available when the QCA is started the directories are created.

  If a file exists in the active output directory, this indicates that QCA did not stop gracefully, the QCA will attempt to complete the file and move it to the today directory.

- the QCA waits for connections from clients (GWCs and SPMs) on the port number specified in the qca.properties.

1.1.4 Stopping QCA

The `stop_qca` script is used to stop the QCA. The user should log in as root to execute this script.

When the `stop_qca` script is run the following warning is displayed:

```
Are you sure you want to stop the QCA? Have you checked the port
number in qca.properties? [ no or yes ]
```

If the port number in qca.properties has been checked and is correctly specified for the QCA to be stopped, this should be validated against the QCA datafill in PTM, then **yes** should be entered, otherwise **no** should be entered and the port number checked.

If a QCA instance was started by `qca_server` the following message will be displayed:

```
Attempting to unregister QCA as Qca from PMFADM.
Attempting to stop local QCA on port : 20001
QCA stopped successfully.
```

If a QCA was not was started by `qca_server` the following message will be displayed:

```
Attempting to unregister QCA as Qca from PMFADM.
pmfadm: "Qca" No such <nametag> registered

QCA not registered with PMFADM as Qca, so stop_qca aborted.
```

If the above message is seen the `query_qca` script should be used to determine if a QCA instance is running on the host.

When the QCA is stopped the following steps are performed, in order:

- the QCA is unregistered with PMFADM
- the QCA stops accepting connections from clients
- the connection to the client(s) is closed
- the IPDR / XML structure in the output file is closed
- the output file is closed and moved to the today directory

> ***Note:*** to avoid alarms being generated by all the GWCs sending QoS records to the QCA when the QCA is stopped the QCA details must be removed from PTM first. Please refer to activity 89007781 - QoS Reporting: Provisioning for QoS Reporting provisioning details.

1.1.5 Client (GWC) connection to QCA

When the QoS reporting mechanism is started on a client (GWC) it will connect to the QCA as specified in PTM, e.g. IP Address and port.

When a connection is established the QCA waits to received data from the client (GWC).

1.1.6 Client (GWC) Connection heart beat

The TCP/IP connection between the client and QCA will be automatically closed if it is not used for more than 2 hours. To ensure the connection is not closed in this circumstance, the client will send a 'heart beat' message after 2 hours of inactivity.

The QCA simply receives the client 'heart beat', and does not generate a QCA IPDR record.

1.1.7 QCA File Management

The active output file is in the active directory. When a file is closed it is moved to the today directory.

1.1.7.1 Initialization

When the QCA is started the following file management steps are performed:

- the output directories are created if they do not already exist.
- any files in the active output directory are validated, ensuring that the last IPDR is complete and that the file structure is closed. Once the file is complete it is moved to the today output directory.
- all 'today' directories older than the file retention period are deleted. This can occur if the qca.properties is change such that file retention period is reduced.
- a new file is created using the naming convention given below. If the file name already exists the new file will have the number 0 added before the file extension, if this exists, the number 1 will be used, then 2 and so on.

1.1.7.2 Output directory

The directory used for the current QCA output is:

/data/qca/"port number"/output/active

Note: In SN07, QCA registers with the 'servman'[1] on the SSPFS machine. Depending on your selection of `RetainFileTime` property in qca.properties file and your calculation of Disk consumption depending on Call traffic at your CO, proper disk partition size of /data/qca should be

1. servman is the application service manager on the SSPFS platform starting SN06.2. servman manages registration and deregistration of all client applications running on the SSPFS machine whether it is simplex or clustered.

requested during SSPFS installation. For calculation on how much disk space should be allocated, refer to section 2.2.7.5.

Where “port number” is the port number that is specified in qca.properties and that the QCA accepts connections on. This allows the output of two QCAs running on the same host to be distinguished.

1.1.7.3 File names

The QCA will use the following file naming convention:

<Node Type>.<Node Name>.<ReportName>.Year.Mon.Date_HR.MN_<TZ>.<File Ext>

For example:

QCA.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml

Where each of the elements is described as:

<NodeType> - A Nortel defined string identifying the product origination. Always “QCA”.

<Node Name> - This name should MATCH the name of the node that is used in faults, in configuration (FQDN), in accounting and in GUIs. This value is configurable as property nodeName in qca.properties.

<Report Name> - The name of the script/filter/report that is used to create this file. There may be 1 or more report names in operation for a given NE simultaneously. Each report type must be identified in the filename. Always “QoS”

<Year.Mon.Date_HR.MN_> - This field when present in the active directory refers to the time when the file was opened or created in the active directory . The same field when present in today directories refers to the time the file was closed i.e the time when the files are closed and recycled to the today directories.

<TZ> - This is the Time Zone of the NE the Performance data is being collected from. This can be an off set from UMT or GMT.

<File Ext> - The file extension specified in qca.properties or the default xml.

1.1.7.4 Output file rotation (closure)

QCA file management provides file rotation (closure) based on file size and time the file has been open, on a ‘which ever comes first’ basis. Theses values are MaxFileSize and MaxFileTime, respectively, in qca.properties.

1.1.7.5 Output file compression

Due to the size of each QCA IPDR record (maximum about 840 bytes) the required disk space to store several days of QCA output files could be very large.

The required disk space storage requirement calculation is a follows:

Assuming:

- BHCA = 550K
- Calls per day = 10 x BHCA = 5.5 M
- QoS records per day = 2 x Calls per day = 11 M
- Record size = 840-bytes
- Compression ratio = 88% (achieved in testing)

Per day disk space required = 11 M x 840 = 8.6 GBytes

When using compression = 8.6 GBytes * 0.12 = 1 GByte

It can be seen that file compression offers a major saving is disk space requirements. And with out compression the disk space in the /data/qca partition would be quickly exhausted.

The file compression is controlled by two properties, closedFileCompression and oldFileCompression.

closedFileCompression controls whether the active file should be compressed when it is closed and moved to the today directory.

oldFileCompression controls whether the retained files should be compressed when the output directories are recycled. When oldFileCompression is enabled, the files in the today-n directories will be checked, and compressed if required, every time directory recycling occurs.

1.1.7.6 Output file retention

The file management of the QCA follows that implemented for the SN05 feature SNMP Performance Measurement Poller (59039902). The output directory structures will contain a *number* of directories, for the current active file, today's closed files and the last *number-1* days closed files.

The clean-up mechanism is described by two parameters:

‘retain file duration’ (RetainFileTime) - how long (in days) should the files be retained on the local disk.

‘recycle time of day’ (recycleToD) - the hour of the day that the today directories are recycled.

Both are parameters specified in the qca.properties file read when the QCA is started.

At a predefined time (recycleToD in qca.properties, default is 12:00 AM), the output directories will be recycled.

The today-n directories are not created when the QCA is started but when the output files are recycled.

When the today directory reaches the maximum file retention period the information is discarded.

E.g.Output file structure if *number* were 30:

/data/qca/”port number”/output/active

/data/qca/”port number”/output/today

/data/qca/”port number”/output/today-1

/data/qca/”port number”/output/today-2

.

/data/qca/”port number”/output/today-28

/data/qca/”port number”/output/today-29

> ***Note:*** if the QCA is stopped and restarted with a new ‘retain file duration’, that is less than the previous ‘retain file duration’ the QCA operated with, any existing today directories older than the new ‘retain file duration’ will be deleted.

The value for the ‘retain file duration’ should be considered carefully as the operation of the QCA and other applications may be impacted if there is no free disk space because it is used to store QCA output files.

In arriving at a value for the ‘retain file duration’ the following should be considered:

- the BHCA and total number of calls per day.
- total disk space available for file retention
- whether file compression is used.

A similar calculation to that in section 2.2.7.5 ‘Output file compression’ should be used to determine the require ‘per day’ disk space requirements and there fore the ‘retain file duration’, e.g.:

‘retain file duration’ = available disk space in MBytes
required MBytes/day

Suppose the /data/QCA partition size is 8GBytes. Using the assumptions in section 2.2.7.5 ‘Output file compression’ and the above calculation the maximum ‘retain file duration’ value is:

8000 MBytes = 8days
1000 MBytes

However, you may request a higher partition size of /data/qca during SSPFS installation as per the calculation shown in section 2.2.7.5.

1.1.7.7 Retaining modified qca.properties over an Upgrade

NOTE: Applicable only if values of parameters in qca.properties have been modified (different than default), and the same are required to be maintained over QCA upgrade.

When QCA is installed, qca.properties at /opt/nortel/qca/properties contains default values of various parameters (For example portNumber = 20000, and retainFileTime = 5). If customers are using other than default values of parameters in qca.properties file, and are planning for upgrade of QCA, following procedure needs to be followed to retain these customized values after upgrade, without having to stop/re-start QCA:

1. Before proceeding with upgrade, change the qca.properties on the inactive side of the cluster as required. (for example, portNumber = 20001, retainFileTime = 5)

2. State of QCA on the inactive side of the cluster: NOT RUNNING

3. Perform the upgrade. (The procedure will involve swacting of the cluster).

4. After the upgrade is complete, the newly active unit of the cluster will have the qca.properties of the previous inactive unit. This way we can expect the modified qca.properties to be maintained over an upgrade, without having to stop/re-start QCA.

5. If the above procedure is not followed, default values of parameters will remain in qca.properties.

For example, consider the present qca.properties have the values for portNumber and retainFileTime to be 20001 and 1 respectively. (It is 20000 and 5 repectively by default). If this qca.properties is to be maintained over an upgrade, the qca.properties of the inactive unit of the cluster has to be updated with these values, before performing the upgrade.

Problem scenario (Before Upgrade):

Active unit	Inactive unit (qca.properties not modified)
(SN08)	(SN09)
portNumber: 20001	portNumber: 20000
RetainFileTime=1	RetainFileTime=5
State: QCA running	QCA Not running

Problem scenario (After Upgrade):

Active unit	Inactive unit
(SN09)	(SN08)
portNumber: 20000	portNumber: 20001
RetainFileTime=5	RetainFileTime=1
State: QCA Running	QCA Not running

As seen in above problem scenario, qca.properties will not be maintained over an upgrade if qca.properties not modified in the inactive unit of the cluster.

Solution (Before Upgrade):

Active unit	Inactive unit (qca.properties modified)

(SN08)	(SN09)
portNumber: 20001	portNumber: 20001
RetainFileTime=1	RetainFileTime=1
State: QCA running	QCA Not running

Solution (After Upgrade):

Active unit	Inactive unit
---	---
(SN09)	(SN08)
portNumber: 20001	portNumber: 20001
RetainFileTime=1	RetainFileTime=1
State: QCA Running	QCA Not running

(No records lost)

As seen above, updating qca.properties of inactive unit of the cluster will result in maintaining modified qca.properties over an upgrade.

1.1.7.8 Reporting disk space issues

As the QCA operates, disk space in /data/qca is used for the active file and to retain closed files. If the disk space in /data/qca becomes exhausted this would effect the operation of the QCA. The QCA uses customer logs to report disk space issues before all the space is used to reduce the possibility of completely filling the partition.

Every time the QCA creates a new file it will attempt check the available disk space, in the unlikely event that available space is not determinable the QCA will write a debug log to a file.

The QCA determines the number of free bytes available in the /data/qca partition and compares this with 3 boundary values; 1 GByte, 500 MBytes and 100 MBytes.

1 GByte boundary

If the available disk space is greater than 1 GByte then no further action is taken. However, if the available disk space is less than 1Gb and more than 500Mb, a minor customer log/alarm is generated.

If some disk space is made available in the /data/qca partition, after a customer alarm was raised, to make the available disk space great than 1GByte, the QCA raises a clear customer log for the minor alarm when the next new file is created.

However, if no action is taken and the available space still lies with between 1 GByte and 500 MBytes when the next file is created, the QCA will generate another minor customer log/alarm.

500 MByte boundary

If the available disk space is less than 500 MBytes and more than 100 MBytes, a major customer log/alarm is generated

If the available disk space goes above 500 MBytes, but below 1 GByte, the QCA raises a clear customer log for the major customer log/alarm when the next new file is created.

If the available disk space goes above 1 GByte the QCA raises clear customer logs for both the major and minor customer logs/alarms when the next new file is created.

However, if no action is taken and the available space still lies with between 500 MBytes and 100 MBytes when the next file is created, the QCA will generate another major customer log/alarm.

100 MByte boundary

If the available disk space is less than 100 MBytes a critical customer log/alarm is generated

If the available disk space goes above 100 MBytes, but below 500 MBytes, the QCA raises a clear customer log for the critical customer log/alarm when the next new file is created.

If the available disk space goes above 500 MBytes, but below 1 GByte, the QCA raises clear customer logs for both the critical and major customer logs/alarms when the next new file is created.

If the available disk space goes above 1 GByte, the QCA raises clear customer logs for the critical, major and minor customer logs/alarms when the next new file is created.

However, if no action is taken and the disk space is completely exhausted the QCA will generate a critical customer log/alarm and the QCA will be stopped.

In the scenario where write access is prevented the application will raise a critical customer log/alarm and the QCA will be stopped.

1.1.8 Growing the Size of /data/qca

See Appendix C for the Procedure to grow the size of Partition /data/qca.

1.1.9 QoS record processing

At the end of every call the client reports the QoS statistics to the QCA in a binary QoS record. The QCA validates the record, ensuring the record sequence number, version and length are correct. The QCA then converts the record to an IPDR form. The QCA IPDR record is then written to a file.

Untill SN07 the QoS record had only 1 version (size 132 Bytes). In SN08 the QoS Record message version is 2 (size 136 Bytes).

Begining SN09 the QoS record has version 3 (size ?? 136+8Bytes (Tstamps) + 32 Bytes (GW name changes from 32 Bytes to 64 Bytes)

1.1.9.1 Binary QoS record format

The QoS record sent from the client (GWC) is a binary message. A description of the binary QoS record fields is shown in Table 2, “Binary QoS record fields (version 1 SN07),” on page 796.

Table 2 Binary QoS record fields (version 1 SN07)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15

Table 2 Binary QoS record fields (version 1 SN07)

Name	Description	Range
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN	Consists of two separate fields; the Gateway name (32 Bytes) and End Pont (32 Bytes).	64-bytes
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	0 to 65534
Latency	Estimate of network latency (milliseconds)	0 to 65534

Table 2 Binary QoS record fields (version 2 SN08)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255

Table 2 Binary QoS record fields (version 2 SN08)

Name	Description	Range
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN	Consists of two separate fields; (the Gateway name and end point)	64-bytes
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	**0 to** 4294967294
Latency	Estimate of network latency (milliseconds)	**0 to** 4294967294

Table 3 Binary QoS record fields (version 3 SN09)

Name	Description	Range
MT (MGC Type)	The type of client (MGC) the QoS record was generated by	0 - GWC 1 - SPM
Msg Type	Message type	0 - QoS record 1 - heart beat
Sequence number	Record sequence number	0 to 16777215
RT (Report Type)	Report Type	0 - local 1 - remote
ver (version)	The QoS record version	0 to 15
MGC number	The number of the client (MGC) the QoS record was generated by	0 to 255

Table 3 Binary QoS record fields (version 3 SN09)

Name	Description	Range
Msg length	The length of the message (including header)	0 to 255 (should be 130)
Gateway port number	The port number on the Gateway used in the call	0 to 65535
Gateway IP Address	The IP Address of the Gateway used in the call	4-bytes
Gateway FQDN - GW Name	**Consists of two separate fields; (the Gateway name**	**64-bytes**
Gateway FQDN Endpoint	**End point**	**32-bytes**
Switch CLLI	The CLLI of the CS2K the client is subtended to	16-bytes
Correlation ID	The correlation id that can be used to correlate the QoS record to an AMA record	10-bytes
Packets Sent	The total number of packets transmitted	0 to 4294967294
Packets Received	The total number of packets received	0 to 4294967294
Octets Sent	The total number of payload octets transmitted	0 to 4294967294
Octets Received	The total number of payload octets received	0 to 4294967294
Packets Lost	The total number of packets lost	0 to 4294967294
Jitter	Estimate of packet interarrival time (milliseconds)	0 to 4294967294
Latency	Estimate of network latency (milliseconds)	0 to 4294967294
StartTimeStamp*	Call Start Timestamp	5 -bytes.
EndTimeStamp*	End Time Timestamp	5 -bytes.

*Start and End timestamp addressed in a later section.

1.1.10 Timestamp (Call Start Time and Call End Time)

1.1.10.1 DISCLAIMER:

1. QoS records contain performance measurement data only and they are never intended to be used as a source for billing information.

2. Call durations for billing/revenue generation purposes have to be based on the time data in the billing records, such as AMA and CDR records, and not QoS records.

1.1.10.2 Timestamp Support

Timestamp support (Call Start Time and Call End Time) for QoS IPDR records are supported begining SN09. This activity is tracked under A0009297 and provides support to display correct call start time and call end time in the QoS IPDR XML records.

All QoS (IPDR) records are stored on a QoS Collector Application(QCA) host. The QCA receives binary QoS records from the MGCs, converts these to QCA IPDR records and stores them in a file. The QCA IPDR records can be obtained by the OSS for processing

Prior to SN09, the timestamp parameter (Call Start time and Call End time) was hardocoded to a default value 1970-01-01T00:00:00.000Z and thus the QoS record output in the XML file show this default value for all calls irrespective of the actual call start time and call end time for the particular call and does not depict the correct value.

GWC sends end of call statistics to active QCA servers. Timestamps (Call Start and Call End Timestamp) are IPDR parameters that would be displayed on a QoS Report along with other IPDR parameters such as timezone, call completion code, hostname, subscriberID, unique Call ID, IP Address, port number, sequence number and End of Call QoS Statistics such as average packet latency, inbound byte count, outbound byte count, inbound packet count, outbound packet count, packet lost and packet delay.

1.1.10.3 Timestamp Format

Timestamp (Call Start Time and Call End TIme) are in ISO 8601 format. The format is shown below:

YYYY:MM:DD:HH:MM:SS:MS Where,

YYYY - Year

MM - Month

DD -Day

HH - Hour

MM - Minute

SS - Second

MS - Millisecond

This timestamp is included in the QoS Binary message and this inturn is parsed by the QCA to extract the Call Start Time and Call End Time. QCA IPDr records show these extracted timestamp.

The timestamp used for the QoS Binary records and QoS IPDR XML records (Call Start Time and Call End Time) will be in Universal coordinated time (UTC) priviously known as Greenwich Mean Time (GMT). Time represented as UTC will be universal and will not have to worry about Daylight saving time.

GMT is World Time and the basis of every world time zone which sets the time of day and is at the centre of the time zone map. Call Start Time and Call End Time use UTC time format and these timestamp will be represented in QCA XML reports.

1.1.10.4 Call Start Time and Call End Time

Call Start TimeStamp(STS) and End TimeStamp(ETS) will be depicted in the QCA Xml records. An example of the timestamp is given below:

<StartTime>2005-01-01T14:52:57.000Z</StartTime>

<EndTime>2005-01-01T14:59:01.000Z</EndTime>

1.1.11 QCA IPDR record format

The output of the QCA is a single stream (file) of IPDR Version 3.1-A.0.2 compliant records.

1.1.11.1 QCA IPDR elements

The IPDR elements used in the QoS output format are shown in the following table.

Table 4 QCA IPDR tags

QoS Field Tag	Type	Range
StartTime	dateTime	ISO 8601 format.

Table 4 QCA IPDR tags

QoS Field Tag	Type	Range
EndTime	dateTime	ISO 8601 format.
timeZoneOffset	integer	Time offset, in minutes, of local time zone referenced to GMT.
callCompletionCode	String	Final call completion code for billing use.
originalDestinationId	String	Called-party (designation) number
hostName	String	0 to 22 characters
subscriberId	**String**	**0 to 65 characters (version 1 and 2)**
		0 to 97 characters (version 3)
uniqueCallId	String	20 hexadecimal digits
ipAddress	String	7 to 15 numerical characters
portNumber	String	0 to 2147483647
seqNum	integer	0 to 16777215
averagePacketLatency	integer	0 to 65536 (version 1)
		0 to 2147483647 (version 2 and 3)
inboundByteCount	integer	0 to 2147483647
outboundByteCount	integer	0 to 2147483647
inboundPacketCount	integer	0 to 2147483647
outboundPacketCount	integer	0 to 2147483647
inboundLostPacketCount	integer	0 to 2147483647
packetDelayVariation	integer	0 to 65536 (version 1)
		0 to 2147483647 (version 2 and 3)

An example QCA IPDR record (for IP fabric):

```
<IPDR>
<StartTime>1970-01-01T00:00:00.000Z</StartTime>*
<EndTime>1970-01-01T00:00:00.000Z</EndTime>
<timeZoneOffset>0</timeZoneOffset>
<callCompletionCode>CC</callCompletionCode>
<originalDestinationId></originalDestinationId>
<hostName>GWC3@COMITIP</hostName>
<subscriberId>aaln/1@ttp018.mgsite-2.b4sky.ott</subscriberId>
<uniqueCallId>43c01738000f13e30d05</uniqueCallId>
<ipAddress>10.0.15.1</ipAddress>
<portNumber>2427</portNumber>
<seqNum>18</seqNum>
<averagePacketLatency>0</averagePacketLatency>
<inboundByteCount>41538</inboundByteCount>
<outboundByteCount>0</outboundByteCount>
<inboundPacketCount>301</inboundPacketCount>
```

```
<outboundPacketCount>0</outboundPacketCount>
<inboundLostPacketCount>0</inboundLostPacketCount>
<packetDelayVariation>0</packetDelayVariation>
</IPDR>

* Note: Starting SN09, the value of the timestamp in the IPDR
records will show the actual value and not the defaulted value
of 1970-01-01T00:00:00.000Z. This is tracked under the activity
A00009297 and is addressed in section <4.0.0.1>
```

The maximum size of a QCA IPDR record is around 840 characters, this equates to 840-bytes (using UTF-8 encoding).

Not all of the QoS statistics are provided by all media gateways, e.g. the UAS does not support the Jitter and Latency statistics, therefore if the received binary QoS record does not contain a valid value for any of the QoS statistics the element will not be included in the output QCA IPDR record.

1.1.11.2 QCA IPDR element values

See the following table.

Table 5 Mapping of input binary QoS Record fields to output QCA IPDR record elements

Output QCA IPDR elements	Input Binary QoS field	Comment
StartTime	Call Start Time	A00009297 feature: Starting SN09, QoS IPDR records will show correct timestamp(Call start Time) and not the Hardcoded value used: 1970-01-01T00:00:00.000Z earlier.
EndTime	Call End Time	A00009297 feature: Starting SN09, QoS IPDR records will show correct timestamp(Call End Time) and not the Hardcoded value used: 1970-01-01T00:00:00.000Z earlier.
timeZoneOffset	N/AN/A	Not applicable. Hardcoded value used: 0
callCompletionCode	N/A	Not applicable. Hardcoded value used: CC (call completed normally)
originalDestinationId	N/A	Not applicable. Empty String
subscriberId	Concatenation of Endpoint and Gateway Name (from Gateway FQDN)	<EndPoint>@<GW Name>
hostName	Concatenation of MT (MGC Type), MGC Number and Switch CLLI	<MGC Type><MGC Number>@<Switch CLLI>
uniqueCallId	Correlation Id	

Table 5 Mapping of input binary QoS Record fields to output QCA IPDR record elements

Output QCA IPDR elements	Input Binary QoS field	Comment
ipAddr	Gateway IP Address	standard 4-part format
portNumber	Gateway Port Number	
seqNum	Sequence number	
averagePacketLatency	Latency	Element not present in IPDR if the received binary QoS record value is less than 0, indicating that the GW did not support the statistic.
inboundByteCount	Octets Received	
outboundByteCount	Octets Sent	
inboundPacketCount	Packets Received	
outboundPacketCount	Packets Sent	
inboundLostPacketCount	Packet Loss	
packetDelayVariation	Jitter	

The following elements are ‘required’ IPDR elements so have been included in the QCA output for IPDR compliancy.

- StartTime
- EndTime
- timeZoneOffset
- CallCompletionCode
- originalDestinationId

1.1.11.3 QCA IPDR file format

The output of the QCA is a file with format conforming to the IPDR structure. The first line in the file is the header, providing details about the XML version and encoding. The next line is the ‘open’ IPDR tag which gives information about the version of QCA and indicates the start of records. The last line in the file is the ‘close’ IPDR tag which indicates the end of the file.

Please see the following figure for an example QoS XML file format.

Figure 3 QCA IPDR file format

Line no.	Line	Description

Figure 3 QCA IPDR file format

1	<?xml version="1.0" encoding="UTF-8" ?>	File header
2	<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" IPDRRecorderInfo ="qca.nortelnetworks.com" xsi:schemaLocation="http://www.ipdr.org/namespaces/ ipdr VoIP3.1-A.0.2.xsd" version="3.1-A.0.2">	IPDRDoc is the file open tag
3	<IPDR>	Start of record
	.	
	.	
	.	
	.	
	.	
n-1	</IPDR>	End of record
n	</IPDRDoc>	/IPDRDoc is the file close tag

The IPDRDoc tag gives information about the IPDR format used and the device that generated the IPDR file, e.g.

IPDRRecorderInfo = "qca.nortelnetworks.com"

1.1.12 Detecting Events and Errors

In the situation that the QCA detects an event (e.g. client closes the connection) or an error (e.g. out of sequence record), a customer log is generated and an error IPDR record is written to the output file.

The error IPDR record is generated so that the OSS does not require two interfaces to the QCA host, one to retrieve IPDR records and one to monitor events and errors. All the relevant information to the QCA output processing is provided in the single output stream.

The error IPDR record is compliant to the IPDR specification, i.e. contains all of the required IPDR elements, some of which will contain default or empty values.

Multiple errors
This is only applicable to unsupported QoS record version and unsupported QoS record length errors.

The QCA allows up to 9 consecutive unsupported QoS record version and up to 9 consecutive unsupported QoS record length errors. When the 10th consecutive error is detected a customer log is generated to indicate this and the connection is being closed.

If a client sends a QoS record with valid length or version before sending 10 unsupported QoS record version or 10 unsupported QoS record length records, a customer log is generated to indicate that the alarm condition has been cleared.

Table 6 QCA Error and Event actions

Error/Event	QCA Action
out of sequence record	customer log generated error IPDR record generated binary QoS record processed
unsupported QoS record version (less than 10 consecutive records)	customer log generated error IPDR record generated binary QoS record discarded
unsupported QoS record version (10th consecutive records)	customer log generated error IPDR record generated binary QoS record discarded connection closed
unsupported QoS record length (less than 10 consecutive records)	customer log generated error IPDR record generated binary QoS record discarded
unsupported QoS record length (10th consecutive records)	customer log generated error IPDR record generated binary QoS record discarded connection closed
unknown message type	customer log generated error IPDR record generated binary QoS record discarded connection closed
unable to read binary QoS record header	customer log generated error IPDR record generated binary QoS record discarded connection closed

Table 6 QCA Error and Event actions

Error/Event	QCA Action
unable to process binary QoS record body	customer log generated
	error IPDR record generated
	binary QoS record discarded
connection closed (not by QCA)[a]	customer log generated
	error IPDR record generated
	connection closed (from QCA end)
QCA stopped	customer log generated
	error IPDR record generated
QCA started	error IPDR record generated
New GWC Connection	customer log generated
	error IPDR record generated

a. Note: This includes the 'GWC Swact' scenario.

Note: please refer to Appendix A for more details of the customer logs generated by the QCA.

1.1.12.1 QCA Error IPDR record

Depending on the type of error, different information can be used in the error IPDR record.

For example, if a message with an 'unknown message type' is received the whole message is unreliable so only the connection information can be used. Whereas, if an 'out of sequence' record is received the message format is valid so information from the connection and record header can be used.

Default values are used in the QCA error IPDR record for the following required IPDR elements:

- callCompletionCode - CC
- originalDestinationId - empty string
- subscriberId - empty string
- uniqueCallId - empty string

Depending on the type of error or event the following QCA error IPDR record elements may contain information:

- hostName - MGC Id, if the MGC Id is not available it is an empty string and the Node name (the value of the nodeName property in the qca.properties file). Below are some examples.
  - GWC3@CS2K_LAB (if MGC Id is available)
  - CS2K_LAB (if MGC Id is an empty string)
- seqNum - the sequence number of the QoS record with the error, the sequence number is not available it is 0

The following QCA error IPDR record elements are always used to convey information:

- ipAddress
- portNumber
- proprietaryErrorCode

The values for each element in the error IPDR record, other than the default elements, is given in the following table.

Table 7 Error IPDR record elements

Error/Event	Element	Value
Unexpected Record Sequence Number	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	0 (plus previous valid record sequence number, e.g. previous sequence number = 1638, proprietaryErrorCode = 01638)
Record Lost: Unsupported Version	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	1
Record Lost: Unsupported Record Length	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection

Table 7 Error IPDR record elements

Error/Event	Element	Value
	proprietaryErrorCode	2
Connection closed: Unrecognised Message Type	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	3
Connection closed: Error while processing QoS record header	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	4
Record Lost: Error while processing binary QoS data	hostname	MGC Id, Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	5
Connection closed	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	6
QCA Stopped	hostname	Node name
	seqNum	0
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	7
QCA Started	hostname	Node name
	seqNum	0

Table 7 Error IPDR record elements

Error/Event	Element	Value
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	8
New GWC Connection[a]	hostname	MGC Id, Node name
	seqNum	record sequence number
	ipAddress	IP Address of connection
	portNumber	Port number of connection
	proprietaryErrorCode	9

a. These records will be produced for every new connection from the GWCs.

1.1.12.1.1 Error IPDR record format

Examples for each of the QCA IPDR error records:

Unexpected Record Sequence Number

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>GWC99@CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37559</portNumber>
  <seqNum>4</seqNum>
  <proprietaryErrorCode>02</proprietaryErrorCode>
</IPDR>
```

Record Lost: Unsupported Version

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>GWC99@CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37665</portNumber>
  <seqNum>2</seqNum>
  <proprietaryErrorCode>1</proprietaryErrorCode>
</IPDR>
```

Record Lost: Unsupported Record Length

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>GWC99@CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37676</portNumber>
   <seqNum>2</seqNum>
   <proprietaryErrorCode>2</proprietaryErrorCode>
</IPDR>
```

Connection closed: Unrecognised Message Type

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37642</portNumber>
   <seqNum>0</seqNum>
   <proprietaryErrorCode>3</proprietaryErrorCode>
</IPDR>
```

Connection closed: Error while processing QoS record header

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37642</portNumber>
   <seqNum>0</seqNum>
   <proprietaryErrorCode>4</proprietaryErrorCode>
</IPDR>
```

Record Lost: Error while processing binary QoS data

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>GWC99@CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
```

```
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37676</portNumber>
  <seqNum>2</seqNum>
  <proprietaryErrorCode>5</proprietaryErrorCode>
</IPDR>
```

Connection closed

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>47.96.0.243</ipAddress>
  <portNumber>37676</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>6</proprietaryErrorCode>
</IPDR>
```

QCA Stopped

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>0.0.0.0</ipAddress>
  <portNumber>20000</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>7</proprietaryErrorCode>
</IPDR>
```

QCA Started

```
<IPDR>
  <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
  <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
  <timeZoneOffset>0</timeZoneOffset>
  <callCompletionCode>CC</callCompletionCode>
  <originalDestinationId></originalDestinationId>
  <hostName>CS2K_LAB</hostName>
  <subscriberId></subscriberId>
  <uniqueCallId></uniqueCallId>
  <ipAddress>0.0.0.0</ipAddress>
  <portNumber>20000</portNumber>
  <seqNum>0</seqNum>
  <proprietaryErrorCode>8</proprietaryErrorCode>
</IPDR>
```

New GWC Connection

```
<IPDR>
   <StartTime>1970-01-01T00:00:00.000Z</StartTime>*
   <EndTime>1970-01-01T00:00:00.000Z</EndTime>*
   <timeZoneOffset>0</timeZoneOffset>
   <callCompletionCode>CC</callCompletionCode>
   <originalDestinationId></originalDestinationId>
   <hostName>GWC77@CS2K_LAB</hostName>
   <subscriberId></subscriberId>
   <uniqueCallId></uniqueCallId>
   <ipAddress>47.96.0.243</ipAddress>
   <portNumber>37559</portNumber>
   <seqNum>567</seqNum>
   <proprietaryErrorCode>9</proprietaryErrorCode>
</IPDR>
* Note: Starting SN09, the value of the timestamp in the IPDR
records will show the actual value and not the defaulted value of
1970-01-01T00:00:00.000Z. This is tracked under the activity
A00009297 and is addressed in section <4.0.0.1>
```

1.1.13 Streaming to OSS

Real-Time streaming of the QCA IPDR record stream to the OSS is provided via the streamQoS utility. It should be used as follows:

1. Connect to the machine on which QCA is running, e.g. via telnet
2. Change directory to the QCA home directory, e.g. /opt/nortel/qca/
3. Start the logging to file of the window.
4. Type streamQoS to start the stream
5. The streaming utility is stopped by closing the connection

1.1.14 Display tool

A tool to display QCA IPDR records in an output QCA file is provided. There are three outputs from the tool:

- display all the QCA IPDR Records in the file
- display all the QCA IPDR Records for a particular Subscriber Id in the file
- display all the QCA IPDR Records for a particular MGC in the file

The command must have at least one argument, the file name.The command is able to handle the compressed and also uncompressed QCA output files.

To display only the records for a particular Subscriber Id, the Subscriber Id must be provided to the utility.

To display only the records for a particular MGC, the following information is necessary:

- MGC type (GWC or SPM), *mgcType* or *mt* field in QCA IPDR record
- MGC number (0 to 255), *mgcNumber* or *num* in QCA IPDR record

Displaying all QCA IPDR records in a file:

```
displayQoS <file name>
```

Displaying all QCA IPDR record from a particular client in a file:

```
displayQoS <file name> <Subscriber Id>
```

Displaying all QCA IPDR record from a particular client in a file:

```
displayQoS <file name> <MGC type> <MGC number>
```

If the file can not be found an error is displayed.

The first argument is always the file name. If only two arguments are provided the second argument is taken as the Subscriber Id. If more than two arguments are provided they are taken as the MGC type and MGC number.

Example displayQoS output :

```
Displaying QoS Records for GWC 80 from file:
GWC.Telco_Switch_35.QoS.2002.04.11_02.45_EDT.xml

Record:
Start Time*     = 1970-01-01T00:00:00.000Z
End Time*       = 1970-01-01T00:00:00.000Z
TimeZone Offset  = 0
Call Comp Code   = CC
Orig Dest Id     =
Host name        = GWC171@3911296719576333
Subscriber id    = 7096155751708778@4995546324
Correlation Id   = 14714216668188184186
IP Address       = 96.143.185.15
Port Number      = 35187
Sequence Number  = 9
Latency          = 19685
Octets Received  = 1894381033
Octets Sent      = 1785294279
Packets Received = 648495757
Packets Sent     = 286520160
Packets Lost     = 922391632
Jitter           = 14826

Record:
Start Time*     = 1970-01-01T00:00:00.000Z
End Time*       = 1970-01-01T00:00:00.000Z
TimeZone Offset  = 0
Call Comp Code   = CC
Orig Dest Id     =
Host name        = GWC99@CS2K_LAB
```

```
Subscriber id     =
Correlation Id    =
IP Address        = 47.96.0.243
Port Number       = 37559
Sequence Number   = 4
Previous seq num = 2
Error Code        = 0 (Unexpected Record Sequence Number)


End of XML QoS File.



* Note: Starting SN09, the value of the timestamp in the IPDR
records will show the actual value and not the defaulted value of
1970-01-01T00:00:00.000Z. This is tracked under the activity
A00009297 and is addressed in section <4.0.0.1>
```

Note: when displaying error IPDR records, the displayQoS utility adds a textual description to the error code value.

Note: when displaying Unexpected Record Sequence Number error IPDR records, the displayQoS utility extracts the previous sequence number value from the proprietryErrorCode and displays it as a separate field, Previous seq num.

1.1.15 Installation

The QCA application (NTQCA.pkg) is available in the CS2M[2] software package. Below are the steps to install the QCA

- Insert the CD with the CS2M load and log onto the SESM server as root. Then change the directory to the bin directory on the CD.

```
cd /cdrom/cdrom0/bin
```

- To start the install process, enter the following command.

```
./appl_mgr.ksh
```

Note: Select option 1 to install all the application along with QCA.

Below are the steps when QCA needs to be installed on a SSPFS machine which does not run the CS2M load.

- FTP the NTQCA.pkg onto the SSPFS machine. Log in as root.
- Install the new QCA software using: pkgadd -d NTQCA.pkg

Below are the steps to follow to uninstall the QCA package.

2. CS2M (CS 2000 Management Components) refers to a NCL software package used on the CS 2000 management tools server. This package includes SESM, NPM, SAM21EM, QCA.

- Connect to the host where the QCA is running.
- Log in as root.
- Stop the QCA server: stop_qca.
- Uninstall the original QCA package: pkgrm NTQCA.

1.1.16 Upgrades

As of SN06.2, the QCA is a patchable component. The patchability mechanism conflicts with the in-service upgrade mechanism. So the support for in-service upgrade of QCA on a single SSPFS machine is removed. Please see section 2.2.15 for more details.

The QCA software upgrades are performed using the install scripts provided with QCA as part of the new software release. Software upgrades of QCA must be coordinated with the OSS to avoid loss of data. The OSS would be redirected to an alternative QCA instance while the primary QCA is being updated. Once the primary instance is updated, the OSS can be redirected back to the primary instance and the other instances can be updated.

1.1.17 QCA customer logs

In addition to QCA Error IPDR Records the QCA raises alarms and events via the customer logging stream.

The QCA uses the logging API introduced by activity 89008996 “Log Reporting and Storage Mechanism for Managed Elements”.

Figure 4 Sample customer log message generated by QCA

```
Oct 11 12:00:02 wmdhs0j8 main:0001 QCA201 WARNING init wmdhs0j8
RetainFileTime property in properties/qca.properties is out of
range. QCA is starting with default retain file time of 5 days
```

The QCA customer logs contain the following fields

- Report name
- Report Number
- Priority
- Event Type
- Device ID
- Message

All the QCA customer logs contain the following information:

- Report name = “QCA”
- Device ID = QCA host name

See Appendix A - QCA Customer Logs for a summary of QCA customer logs and the contents of the other fields in the logs.

The QCA also generates debug logs to report software errors.

1.1.18 Patchability

In SN06.2, the activity A00003229 provides the functionality of making the QCA a patchable OAM device. The Network Patch Manager is responsible for administering individual fixes to QCA. Patches for the QCA will be in the same format and have the same naming convention of OAM patches such as NPM, SAM21EM, etc

When a QCA patch (containing modified Java-based classes) is delivered to a customer site, the patch is applied and then the QCA application is required to be stopped and then restarted by the NPM for the patch to be ‘enabled’. The restart enables a new Java Virtual Machine to be started that picks up the patched/modified Java classes. This procedure also applies to removal of QCA patches. For a QCA patch to be truly removed, the patch is removed and then a restart must be performed via the NPM on the application.

The QCA application must be inservice to perform any maintenance operations such as application, removal, or restart. In addition, the QCA application must be inservice for an audit to succeed. Because QCA is monitored or polled by an external system (OSS) for performance data or SLA agreements, it is important that any changes to QCA be coordinated to avoid loss of data or duplication of data. The OSS should be moved from monitoring the primary instance of QCA to an alternative QCA instance while the primary QCA is being updated via the restart request initiated by NPM. Once the primary instance is updated, the OSS should be redirected back to the primary instance and the other instances can be updated.

Since QCA is an OAM software application, it will be registered in the NPM database upon system start-up and initialization, and it will appear as a device with the device name QCA_<node_name>, where node_name is the name of the SSPFS machine where the QCA is running. Reports and queries at the NPM Graphical User Interface (GUI) and NPM Command Line User Interface (CLUI) will show the QCA as a device.

In SN06.2, the support for in-service QCA upgrade (on a single SSPFS machine) is removed to enable QCA patchability. Hence, the scripts to start and stop the second instance of QCA (qca_server2 and stop_qca2) will be obsoleted in this release.

The following sections briefly give information about applying/removing patches to/from QCA.

1.1.18.1 Applying patch to QCA

The following steps are a recommended procedure in applying QCA patches to a QCA application.

- QCA patch files are delivered to a customer site to the SSPFS machine containing the NPM server via RPS/PFRS or by manual action.
- QCA patches are introduced to the NPM database via the NPM CLUI with the ‘getpatch’ command.
- QCA patches are applied to the QCA application via the NPM apply command at the NPM GUI or NPM CLUI.

After all the QCA patches are applied, a restart command from the NPM GUI or NPM CLUI is invoked on the QCA application to enable or activate the patches.

> ***Note:*** A restart consists of stopping the QCA application and then starting the application. It is important that any maintenance activities associated with the QCA should be completed or stopped before the restart from the NPM GUI or CLUI is invoked. Also, the OSS should be directed from the primary instance of QCA to an alternative instance prior to the restart. The NPM restart will result in current active file being moved into the *today* directory and a new active file will be opened. The whole of this operation will take around **60 seconds**, during this period any QoS records sent from GWC to QCA will be lost.

Also, a NPM restart will result in following logs.

1. NPM 620: Initiated restart on device,<qca_devicename>.
2. GWC 312: QCA connection failure, indicating that GWC is having communication problems with QCA.
3. NPM 620: A restart initiated by the NPM on device <qca_devicename> has completed.
4. QCA 322: New GWC Connection, indicating that QCA has come up after the restart, and is accepting connections.

5. GWC 399: Clear event for GWC312, indicating that previous ‘Raise’ event is cleared.

   Note: It is important to note the NPM database could show patches to be applied to an OAM device, but the patch is not actually enabled or performing its task to address the original problem. It is only after a restart is performed from the NPM GUI or CLUI on the OAM device that the patch is enabled.

- After the restart is performed on the QCA an NPM audit needs to be executed to update OAM patch enabled statuses in the NPM database. The audit can be performed manually from the NPM GUI or CLUI or it will be done automatically on the device approximately 20-25 minutes after the restart has been completed.

1.1.18.2 Removing Patch from QCA

The following steps are a recommended procedure in removing QCA patches from QCA.

- QCA patches are removed via the NPM remove command at the NPM GUI or NPM CLUI.
- After all QCA patches are removed, a restart command from the NPM GUI or NPM CLUI is invoked on the QCA to disable the patches.

  Note: A restart consists of stopping the QCA application and then starting the QCA application. It is important that any maintenance activities associated with QCA should be completed or stopped before the restart from the NPM GUI or CLUI is invoked. Also, the OSS should be directed from the primary instance of QCA to an alternative instance prior to the restart. The NPM restart will result in current active file being moved into the *today* directory and a new active file will be opened. The whole of this operation will take around **60 seconds**, during this period any QoS records sent from GWC to QCA will be lost.

Also, a NPM restart will result in following logs.

1. NPM 620: Initiated restart on device,<qca_devicename>
2. GWC 312: QCA connection failure, indicating that GWC is having communication problems with QCA.
3. NPM 620: A restart initiated by the NPM on device <qca_devicename> has completed.
4. QCA 322: New GWC Connection, indicating that QCA has come up after the restart, and is accepting connections.

5. GWC 399: Clear event for GWC312, indicating that previous ‘Raise’ event is cleared.

   Note: It is important to note the NPM database could show patches to be removed from an OAM device, but the patch is still enabled or performing its task to address the original problem. It is only after a restart is performed from the NPM GUI or CLUI on the OAM device that the patch is disabled.

- After the restart is performed on the QCA, an NPM audit needs to be executed to update QCA patch enabled statuses in the NPM database. The audit can be performed manually from the NPM GUI or CLUI or it will be done automatically on the device approximately 20-25 minutes after the restart has been completed.

1.1.18.3 AutoApply

QCA patches can be automatically applied if the end user has the automated process scheduled to run. Refer to the NPM online help for more information on this automated process.

1.1.18.4 Restart and AutoRestart Restrictions

Due to the implications to the OSS, restrictions are placed on the NPM restart command for QCA devices. The following restrictions are enforced by the NPM:

- QCA devices are not included in the set of OAM devices that can be auto-restarted, nor can a QCA restart be included in any plans scheduled at a designated time. Only a manual restart of a QCA device is supported.
- Only one QCA at a time can be restarted. The multitasking ability of NPM is not utilized for QCA.

A warning will be displayed to the user by the NPM CLUI or GUI explaining the implications of restarting QCA. The user will be forced to choose whether to continue with the restart command or to cancel.

1.1.19 QCA Software Management

The QCA application is designed to allow multiple copies to run in the network to provide increased levels of reliability. Additional copies of the QCA application should be installed on different servers and assigned in the GWC EM. Two instances of QCA can not be installed on the two halves of the same high availability cluster; they must be on separate servers. Because QCA is monitored or polled by an external system (OSS) for performance data or SLA agreements, it is important that any changes to QCA be coordinated with the OSS to avoid loss of

data or duplication of data. These changes include starting or stopping the application, applying corrective content, or applying upgrades. The OSS must be able to move from monitoring one instance of QCA to another during patching or upgrades or any activity that interrupts the QCA application. The OSS can either be manually redirected to another instance of QCA or programmed to automatically redirect on command.

1.2 Hardware Requirements or Dependencies

The QCA application has the following requirements:

- SUN Netra T1400

440Mhz UltraSPARCC IIi with QFE card, 4MB Cache, 512MB RAM, 2x18.2GB Disk Running SUN Solaris 8 Oracle DB 8.1.6 Enterprise and Java Virtual Machine.

Note: The QCA can run on the same SUN Netra T1400 that SESM and other network management tools are running on.

1.3 Software Requirements or Dependencies

- SSPFS 3d party software suite Version 06.

1.4 Limitations and restrictions

1.4.1 Upgrades

To ensure that the QCA support the version of QoS record used in the network, the QCA must be upgraded before the QoS reporting clients are upgraded..

Note: For a major release upgrade, where the SSPFS software is upgraded before the QCA, a QCA running on a separate host is required to ensure no loss of QoS records.

Note: For a QCA maintenance release upgrade or when applying patches, a QCA running on a separate host is required to ensure no loss of QoS records.

Note: Corrective content is applied and managed by the Network Patch Manager (NPM) in SN06.2. Because of the need to coordinate QCA changes like patching with the external OSS, QCA patches are manually applied and activated. This allows the OSS to be redirected to an alternative QCA instance while the primary QCA is being updated. Once the primary instance is updated, the OSS

can be redirected back to the primary instance and the other instances can be updated.

1.5 Interactions

- Syslog daemon server

1.6 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

Data Schema _____

User Interface _____

Element Management _____

Security _____

Service Order _____

Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements)_____

1.7 Glossary

Term	Description
ATM	Asynchronous Transfer Mode
CLLI	Common Language Location Identifier
CLUI	Command Line User Interface
CMTS	Cable Modem Terminal System
DPT	Dynamic Packet Trunk
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
GW	Gateway
GWC	Gateway Controller
IP	Internet Protocol

Term	Description
IOM	Input/Output Module
OC	Optical Carrier
OSS	Operations Support System
MGC	Media Gateway Controller
MS	Message Switch
NCS	Network Control System
NE	Network Element
NPM	Network Patch Manager
OL	Octets Lost
OR	Octets Received
OS	Octets Lost
PFRS	Patch File Receipt System
PL	Packets Lost
PR	Packets Received
PL	Packets Sent
PSE	Patching Server Element
PVG	Passport Voice Gateway
QCA	QoS Collector Application
QoS	Quality of Service
RPS	Regional Patch Selector
SDM	SuperNode Data Manager
SESM	Succession Element and Subelement Manager
SLA	Service Level Agreement
SPM	Spectrum Peripheral Module
STM	Synchronous Transfer Mode
USP	Universal Signalling Processor
UTF	Universal Text Format
VMG	Virtual Media Gateway
VoIP	Voice over IP

Term	Description
XML	eXtensible Markup Language

1.8 References.

1. Activity 89007790 - QoS Reporting: Correlation ID and billing
2. Activity 89007749 - QoS Reporting: GWC QoS Reporting Application and Connection Management
3. Activity 89007781 - QoS Reporting: Provisioning
4. Activity 59039902 - SNMP Performance Measurement Poller
5. Activity 89008996 - Log Reporting and Storage Mechanism for Managed Elements
6. Activity 00009297 - QoSR Support of AAL2 and Timestamp.
7. Activity 00009189 - CS2M support for 64 Character Gateway name.

1.9 Appendix A for 89007819 - QCA Customer logs

Table 8 Service summary (initialization) warning logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
Qca.properties not available at QCA start-up.	201	Warning	INIT	Properties file (properties/qca.properties) not available. QCA is starting with default settings.	Default used	None
portNumber property not in properties/qca.properties at QCA start-up.	201	Warning	INIT	portNumber property not in properties/qca.properties. QCA is starting with default port number of 20000	Default used	None
portNumber property in properties/qca.properties not in range at QCA start-up.	201	Warning	INIT	portNumber property in properties/qca.properties not in range. QCA is starting with default port number of 20000	Default used	None
portNumber property in properties/qca.properties not a number at QCA start-up.	201	Warning	INIT	portNumber property in properties/qca.properties could not be used. QCA is starting with default port number of 20000	Default used	None

Table 8 Service summary (initialization) warning logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
MaxFileSize property not in properties/qca.properties.	201	Warning	INIT	MaxFileSize property not in properties/qca.properties. QCA is starting with default maximum file size of 1 MByte	Default used	None
MaxFileSize property in properties/qca.properties not in range.	201	Warning	INIT	MaxFileSize property in properties/qca.properties not in range. QCA is starting with default maximum file size of 1 MByte	Default used	None
MaxFileSize property in properties/qca.properties not a number.	201	Warning	INIT	MaxFileSize property in properties/qca.properties could not be used. QCA is starting with default maximum file size of 1 MByte	Default used	None
MaxFileTime property not in properties/qca.properties.	201	Warning	INIT	MaxFileTime property not in properties/qca.properties. QCA is starting with default maximum file time of 15 minutes	Default used	None
MaxFileTime property in properties/qca.properties not in range.	201	Warning	INIT	MaxFileTime property in properties/qca.properties not in range. QCA is starting with default maximum file time of 15 minutes	Default used	None
MaxFileTime property in properties/qca.properties not a number.	201	Warning	INIT	MaxFileTime property in properties/qca.properties could not be used. QCA is starting with default maximum file time of 15 minutes	Default used	None
RetainFileTime property not in properties/qca.properties.	201	Warning	INIT	RetainFileTime property not in properties/qca.properties. QCA is starting with default retain file time of 5 days	Default used	None
RetainFileTime property in properties/qca.properties not in range.	201	Warning	INIT	RetainFileTime property in properties/qca.properties not in range. QCA is starting with default retain file time of 5 days	Default used	None
RetainFileTime property in properties/qca.properties not a number.	201	Warning	INIT	RetainFileTime property in properties/qca.properties could not be used. QCA is starting with default retain file time of 5 days	Default used	None

Table 8 Service summary (initialization) warning logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
recycleToD property not in properties/qca.properties.	201	Warning	INIT	recycleToD property not in properties/qca.properties. QCA is starting with default recycle hour of day of 0	Default used	None
recycleToD property in properties/qca.properties not in range.	201	Warning	INIT	recycleToD property in properties/qca.properties not in range. QCA is starting with default recycle hour of day of 0	Default used	None
recycleToD property in properties/qca.properties not a number.	201	Warning	INIT	recycleToD property in properties/qca.properties could not be used. QCA is starting with default recycle hour of day of 0	Default used	None
fileExt property not in properties/qca.properties.	201	Warning	INIT	fileExt property not in properties/qca.properties. QCA is starting with default file extension of xml	Default used	None
oldFileCompression property not in properties/qca.properties.	201	Warning	INIT	oldFileCompression property not in properties/qca.properties. QCA is starting with default value of true	Default used	None
oldFileCompression property in properties/qca.properties not true or false.	201	Warning	INIT	oldFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true	Default used	None
closedFileCompression property not in properties/qca.properties.	201	Warning	INIT	closedFileCompression property not in properties/qca.properties. QCA is starting with default value of true	Default used	None
closedFileCompression property in properties/qca.properties not true or false.	201	Warning	INIT	closedFileCompression property in properties/qca.properties could not be used. QCA is starting with default value of true	Default used	None
nodeName property not in properties/qca.properties.	201	Warning	INIT	nodeName property not in properties/qca.properties. QCA is starting with default value of QCA	Default used	None
old file retention directory (today-x) is being removed.	202	None	INIT	File Recovery: removing closed file retention directory: *directory* as it is older than *x* days.	Directory removed	None

Table 8 Service summary (initialization) warning logs

Event / Error	Report #	Priority	Event Type	Description	QCA Action	Customer Action
File found in active directory when QCA started.	202	None	INIT	File Recovery: file *file name* found in active directory. This could indicate that the QCA failed. Please check debug logs.	File completed (if necessary) and moved to today directory.	Check debug logs.

To comply with X.733, the structure of the logs will also contain following attributes. The logs are differentiated from each other by Specific Problem and Description attributes.

- Location : QCA Host Name
- Category : Appropriate category from X.733 list of available categories.
- Cause : Appropriate category from X.733 list of available cause-values.
- Time : Time at which log was generated.
- ComponentID : File /Directory path, GWC name (components causing generation of log)
- SpecificProblem : Text giving details of the specifc-problem
- Description : Text describing the problem and/or giving more information.

Table 9 Trouble logs

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
File handler or server socket could not be started.	300	None	FAIL	QCA not started: Could not open server socket: +*reason* or QCA not started: Could not create File Handler: +*reason*	QCA not started	Rectify problem and re-start QCA.

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
Out of sequence QoS record received.	302	None	FLT	Out of Sequence QoS Record received. '*MGC Type MGC number*': sequence number = '*record sequence number*' previous sequence number = '*last record sequence number*'	XML Error record generated.	None
Problem processing binary QoS record.	302	None	FLT	Problem processing binary QoS record: Sequence number = '*record sequence number*' Relevant MGC is mentioned in *Component ID* attribute of the log.	XML Error record generated. XML QoS Record not written to file.	None
QoS Record received with Unsupported Length. (Notification Id : 9)	301	Minor	FLT	Location : <hostName> Notification ID: 9 State : Raise Category :Processig Error Cause: Corrupt Data. Time :<time> Component Id : 'MGCType MGCNum' Specific Problem : The QCA has received records with < numberOfLengthErrors> length errors from the source. Description: If 10 (or more) records with unsupported length are received consecutively, Major fault log is generated and the connection is closed.	XML Error record generated. XML QoS Record not written to file.	Investigate why client is sent QoS Record with Unsupported Length
10 sequential QoS Records received with Unsupported Length.	301	Major	FLT	Location : <hostName> Notification ID: 9 State : Raise Category :Processig Error Cause : Version mismatch. Time :<time> Component Id : 'MGCType MGCNum' Specific Problem : 10 unsupported length records received. The connection to the client will be closed	Connection to client closed	Investigate why client is repeatedly sending Unsupported Length QoS records

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
QoS Record received with Unsupported Version. (Notification Id : 57)	301	Minor	FLT	Location : <hostName> Notification ID:57 State : Raise Category :Processig Error Cause : Version mismatch. Time :<time> Component Id : 'MGCType MGCNum' Specific Problem : The QCA has received records with <NumberOfVersionErrors> version errors from the source. Description : If 10 (or more) records with unsupported version are received consecutively, Major fault log is generated and the connection is closed.	XML Error record generated. XML QoS Record not written to file.	Investigate why client is sent QoS Record with Unsupported Version
10 sequential QoS Records received with Unsupported Version.	301	Major	FLT	Location : <hostName> Notification ID: 57 State : Raise Category :Processig Error Cause : Version mismatch. Time :<time>Component Id : 'MGCType MGCNum' Specific Problem : 10 unsupported version records received. The connection to the client will be closed.	Connection to client closed	Investigate why client is repeatedly sending Unsupported Length QoS records
The binary QoS Record header could not be processed.	305	None	FLT	Connection closed: Error while processing QoS record header: Client at, IP Address '*client IP Address*'. Local Port '*local port number*' closed connection.	Connection to client closed	Investigate why client is sent QoS Record with faulty header
Disk space shortage, local disk requires more free space. Disk Space is below 100Mb.	310	Critical	TBL	Location : <hostName> Notification ID: 49 State : Raise Category :Processig Error Cause : StorageCapacityproblem. Time :<time>Component Id : /data/qca Specific Problem : checkDiskSpace() has shown that there is less than 104857600 bytes available on the local disk. More Space is required immediately.	None	More space must be created.

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
Disk Space is starting to run seriously low. This means that the available space is below 500Mb.	310	Major	TBL	Location : <hostName> Notification ID: 49 State : Raise Category :Processig Error Cause : StorageCapacityProblem. Time :<time>Component Id : /data/qca . Specific Problem :Less than 524288000 bytes available on the local disk.Critical alarm will be raised if disk space continues to drop.	None	More space must be created.
Disk space is below the minimum threshold. Initially set at 1Gb.	310	Minor	TBL	Location : <hostName> Notification ID: 49 State : Raise Category :Processig Error Cause : StorageCapacityProblem. Time :<time>Component Id : /data/qca . Specific Problem : Less than 1073741824 bytes available on the local disk. Major alarm will be raised if the disk space continues to drop.	None	More space must be created.
A request to get a new file name has failed, there are either 10000 files with the same name or the new file can not be created.	315	Warning	FLT	Unable to get an unused file name for <fileName> Please check the output directory.	file null.xml used	Output directories need to be checked.
The QCA has failed to write the footer information to the active file whilst attempting to close. The active file might have been compressed without the footer information.	315	Warning	FLT	Cannot write the FOOTER to the active file. This file is corrupted FileName = <fileName>.	None	Check the file and confirm that all XML tags have been closed.
The active file did not exist when trying to write to it. Attempt to get new file then failed. Further failures will result in the QCA being shutdown.	315	None	FLT	Active file <fileName> has been removed. Data may have been lost. Creating new file, and attempting to write record again. Failure to do so will result in shutdown of the QCA	Attempts to create a new output file	File IO problems, if problem is resolved the Major alarm will be withdrawn .

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
Attempting to write data to file, the active file does not exist. Try to get new file. This has failed. Sleep The thread and try and get new file again.This also failed. No file to write to, QCA will shutdown.	315	None	FAIL	Could not get new file to write records. File <fileName> is corrupted or removed. QCA shutting down.	QCA is stopped.	check: disk space and write permissions. If all is well try starting QCA again.
The XML writer and the file all seem well, unfortunately the file cannot be accessed at in either the first or second attempt, serious problem with file IO. QCA will shutdown.	315	None	FAIL	Could not write to the activefile. Active file exists but cannot write records to it. Reason unknown. QCA shutting down	QCA is stopped.	check: disk space and write permissions. If all is well try starting QCA again.
The QCA has encountered inconsistent errors when building the directory structure for old files, old files may have been deleted and directory locked. The error should never appear , as it is the last resort.	315	None	FAIL	Cannot create directories under *output* directory. Cannot write records. QCA shutting down	QCA is stopped.	Check: directory structure, active and old files.
Attempt to rename the active file from the active directory to the today directory has failed. Serious error, but no loss of data immediately. Files can be moved by hand if required.	315	None	FLT	Could not rename active file <fileName> to file <newFileName>. Please check write permissions for the output directory	Closed file remains in active directory.	Check the directories exist and all the write permissions.
Could not create new active file. Data is being lost.QCA must shut down.	315	None	FAIL	Could not get new file for writing. Critical Error: <reason>. QCA shutting down.	QCA is stopped.	Check the active directory for old files and permissions.

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
Attempt to compress an old active file has failed.	315	None	FLT	Could not compress file: <fileName>. File compression failed.	None	Check the active directory for old files and permissions.
Failed to rename directories on the Recycle_day proc. This is where all files are moved along a level and the last gets deleted.	315	None	FLT	Could not rename director from <dirName> to <newDirName>. Check disk space and permissions.	None	Check disk space and permissions.
New GWC connection received.	322	None	INFO	New GWC COnnection : '*MGC Type MGC number*': sequence number = '*record sequence number*'	XML Error record generated	

Table 10 Information and alarm clear logs

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
Connection closed.	305	None	INFO	Connection closed. Client at, IP Address '*client IP Address*'. Local Port '*local port number*' closed connection.	Connection to client closed	None
Client has stopped sending records with unsupported length (clear for QCA 301 Notification Id : 9)	399	None	INFO	Location: <Hostname> Notification Id : 9 State : Alarm Cleared Time : <time>	None	None
Client has stopped sending records with unsupported version (clear for QCA 301 Notification Id : 57)	399	None	INFO	Location: <Hostname> Notification Id : 57 State : Alarm Cleared Time : <time>	None	None
Critical disk space issue cleared (clear for 310 Critical Alarm)	399	None	INFO	Location: <Hostname> Notification Id : 49 State : Alarm Cleared Time : <time>	None	None

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
Major disk space issue cleared (clear for 310 Major Alarm)	399	None	INFO	Location: <Hostname> Notification Id : 49 State : Alarm Cleared Time : <time>	None	None
Minor disk space issue cleared (clear for 310 Minor Alarm)	399	None	INFO	Location: <Hostname> Notification Id : 49 State : Alarm Cleared Time : <time>	None	None
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category:PROCESSINGERROR Cause:CONFIGERROR Time: ComponenetID: SpecificProblem:QCA not running on specified port: Description:Cannot stop QCA Action:Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file."	Connection to client closed	None
QCA cannot be stopped	203	None	INIT	Location: <Hostname> Category:PROCESSINGERROR Cause:CONFIGERROR Time: ComponenetID: SpecificProblem:Missing qca.properties file. Description:Could not read properties. QCA cannot be stopped.Action:Restore qca.properties file.	None	None
QCA cannot be stopped	203	None	INIT	**Location**: <Hostname> **Category**:PROCESSINGERROR **Cause**:CONFIGERROR Time: **ComponenetID**: **SpecificProblem**:Attribute portNumber missing from qca.properties while trying to stop QCA.**Description**:Cannot determine QCA port number to stop QCA . **Action**:Add portNumber information to qca.properties file.	None	None

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
QCA cannot be stopped	203	None	INIT	**Location**: <Hostname> **Category**:PROCESSINGERROR **Cause**:CONFIGERROR Time: **ComponenetID**: **SpecificProblem**:Incorrect portNumber specified in qca.properties**. Description**:Cannot determine QCA port number to stop QCA **Action:**Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file.	None	None
QCA cannot be stopped	203	None	INIT	**Location**: <Hostname> **Category**:PROCESSINGERROR **Cause**:CONFIGERROR Time: **ComponenetID**: **SpecificProblem**:Out of range portNumber specified in qca.properties.**Description**:Cannot determine QCA port number to stop QCA. **Action**: Use query_qca command to determine the port QCA is running on. Make sure it matches with portNumber in qca.properties file.	None	None
Connection closed.	305	None	ERROR	**Location**: <Hostname> **Category**:COMMUNICATIONS **Cause**:COMMSUBFAIL **Time**: **SpecificProblem**:. MSGTYPEERROR **Description**:Client at, IP Address: closed connection.	None	None
Connection closed.	305	None	INFO	**Location**: <Hostname> **Category**:COMMUNICATIONS **Cause**:COMMSUBFAIL **Time**: **SpecificProblem**: CONNECTIONCLOSED **Description**:Client at, IP Address: closed connection.	None	None
Connection closed.	305	None	ERROR	**Location**: <Hostname> **Category**:COMMUNICATIONS **Cause**:COMMSUBFAIL **Time**: **SpecificProblem**: HEADERERROR .**Description**:Client at, IP Address: closed connection	None	None

Event / Error	Report #	Priority	Event Type	Message	QCA Action	Customer Action
Connection closed.	305	None	INFO	**Location**: <Hostname> **Category**:COMMUNICATIONS **Cause**:COMMSUBFAIL **Time**: **SpecificProblem**: CONNECTIONCLOSED.**Description**:Client at, IP Address: closed connection	None	None
Connection closed.	305	None	INFO	**Location**: <Hostname> **Category**:COMMUNICATIONS **Cause**:COMMSUBFAIL **Time**: **SpecificProblem**: nCONNECTIONCLOSED **Description**:Client at, IP Address: closed connection	None	None

Appendix B for 89007819- QCA Customer log Sample Exact Format

Log Report 201:

Table 2 201 Message

Report Number	Message
201	May 27 16:41:45 rtpysesm1 QCA: _V2_~I=rtpysesm1~H=rtpysesm1~A=QCA~S=0000~~ QCA201 WARNING INIT rtpysesm1 ^M Location: rtpysesm1^M Category: processingError^M Cause: configurationOrCustomizationError^M Time: May 27 16:41:45 2005^M ComponentID: /opt/nortel/qca/properties/qca.properties^M SpecificProblem: Missing qca.properties file.^M Description: Could not read properties. QCA is starting with default settings.^M

Log Report 202:

Table 3 202 Message

Report Number	Message
202	Aug 19 22:22:02 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0000~~ QCA202 NONE INIT wnc0s0qu ^M Location: wnc0s0qu^M Category: processingError^M Cause: fileError^M Time: Aug 19 22:22:02 2004^M ComponentID: /data/qca/20000/output/active/^M SpecificProblem: Old file(s) present in active directory.^M Description: Moving old file: QCA.QCA.QoS.2004.08.19_22.19_EDT.xml, found in active directory. This could indicate that QCA failed.^M

Log Report 203

Table 4 203 Message

Report Number	Message
203	May 30 22:55:50 india1sesm QCA_STOP: _V2_~I=india1sesm~H=india1sesm~A=QCA_STOP~S=0000~~ QCA203 NONE INIT india1sesm ^M Location: india1sesm^M Category: processingError^M Cause: configurationOrCustomizationError^M Time: May 30 22:55:50 2005^M ComponentID: /opt/nortel/qca/properties/qca.properties^M SpecificProblem: Missing qca.properties file.^M Description: Could not read properties. QCA cannot be stopped.^M Action: Restore qca.properties file.^M

Log Report 300

Table 5 300 Message

Report Number	Message
300	May 31 04:22:08 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0002~~ QCA300 NONE FAIL india1sesm ^M Location: india1sesm^M Category: processingError^M Cause: communicationsSubsystemFailure^M Time: May 31 04:22:08 2005^Ml ComponentID: GWC-99^M SpecificProblem: Socket creation error.^M Description: QCA not started:^M

Log Report 302

Table 6 302 Message

Report Number	Message
302	May 31 04:22:08 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0002~~ QCA302 NONE FLT india1sesm ^M Location: india1sesm^M Category: processingError^M Cause: informationOutOfSequence^M Time: May 31 04:22:08 2005^M ComponentID: GWC-99^M SpecificProblem: Unexpected Record Sequence Number^M Description: Out of sequence QoS record received. Sequence Number = 1670001 Previous sequence number = 0^M

Log Report 305

Table 7 305 Message

Report Number	Message
305	Aug 19 22:18:34 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0121~~ QCA305 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M Category: communications^M Cause: communicationsSubsystemFailure^M Time: Aug 19 22:18:34 2004^M SpecificProblem: Connection closed^M Description: Client at, IP Address: kiran-1.ca.nortel.com. Port: 2512 closed connection.^M

Log Report 310

Table 8 310 Message

Report Number	Message
310	May 30 22:52:45 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0000~~ QCA310 CRIT TBL india1sesm ^M Location: india1sesm^M NotificationID: 49^M State: Raise^M Category: Processing Error^M Cause: storageCapacityProblem^M Time: May 30 22:52:44 2005ComponentID: /data/qca/^M SpecificProblem: checkDiskSpace() has shown that thereis less than ^M 104857600 bytes available on the local disk.^M Description: More Disk space is required immedietly.^M

Log Report 315

Table 9 315 Message

Report Number	Message
315	Aug 19 22:15:43 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0001~~ QCA315 NONE FLT wnc0s0qu ^M Location: wnc0s0qu^M Category: processingError^M Cause: fileError^M Time: Aug 19 22:15:43 2004^M ComponentID:/data/qca/20000/output/active//data/qca/20000/output/active/QCA.QCA.QoS.2004.08.19_22.12_EDT.xml^M SpecificProblem: Active file: /data/qca/20000/output/active/QCA.QCA.QoS.2004.08.19_22.12_EDT.xmlhas been removed/deleted.^M Description: Data may have been lost. Creating new file, and attempting to write records again. Failure to do so will result in QCA shutdown.^M

Log Report 322

Table 10 322 Message

Report Number	Message
322	Aug 19 22:15:43 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0004~~ QCA322 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M Category: communications^M Time: Aug 19 22:15:43 2004^M ComponentID: GWC-17^M SpecificProblem: New GWC connection^MDescription: New connection from GWC-17. Sequence Number = 1^M

Log Report 399

Table 11 399 Message

Report Number	Message
399	Aug 18 06:49:08 wnc0s0qu QCA: _V2_~I=wnc0s0qu~H=wnc0s0qu~A=QCA~S=0087~~ QCA399 NONE INFO wnc0s0qu ^M Location: wnc0s0qu^M NotificationID: 49^M State: Cleared^M Time: Aug 18 06:49:08 2004^M

*** NOTE: (There are no changes in Alarms as a result of feature A00008338)

1> There are 3 different Types of Alarms uniquely identified by the Notification ID

a> Notification ID: 9

Event: Client is sending Records with unsupported Length.

Raise Severity (Major or Minor)

Raise Customer Log Report Number: QCA 301

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

b> Notfication ID: 57

Event: Client is sending Records with unsupported Version.

Raise Severity (Major or Minor)

Raise Customer Log Report Number: QCA 301

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

c> Notfication ID: 49

Event: Critical/Major/Minor Disk Space issue.

Raise Severity (Critical, Major or Minor)

Raise Customer Log Report Number: QCA 310.

Clear Severity: (None)

Clear Customer Log Report Number: QCA 399.

Example of Raise/Clear Alarms:

Table 1 301 Message- Raise

Report Number	Message
301	May 31 07:37:20 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0001~~ QCA301 MINOR FLT india1sesm ^M Location: india1sesm^M NotificationID: 9^M State: Raise^M Category:Processing Error^M Cause: corruptData^M Time: May 31 07:37:20 2005^M ^M ComponentID: GWC99^M SpecificProblem: The QCA has received records with 1 length errors from the source.^M Description: If 10 (or more) records with unsupported length^M are received consecutively, Major fault log is generated^M and the connection is closed.^M

Table 2 399 Message- Clear

Report Number	Message
399	May 31 07:39:47 india1sesm QCA: _V2_~I=india1sesm~H=india1sesm~A=QCA~S=0001~~ QCA399 NONE INFO india1sesm ^M Location: india1sesm^M NotificationID: 9^M State: Cleared^M Time: May 31 07:39:47 2005^M

Appendix B- Increasing the size of a file system on a Sun server

Application

Use one of the following procedures to increase the size of a file system on a Succession Server Platform Foundation Software (SSPFS)-based server:

- Simplex configuration (one server)
- High-availability configuration (two servers)

It is recommended you perform this procedure during off-peak hours.

The Succession Server Platform Foundation Software (SSPFS) creates file systems to best fit the needs of applications. However, it may be necessary to increase the size of a file system.

Not all file systems can be increased. The table below lists the file systems that cannot be increased, and lists examples of those that can be increased.

SSPFS file systems

Cannot be increased	Can be increased (examples)

/ (root)	/data
/var	/opt/nortel
/opt	/data/oradata
/tmp	/audio_files
/PROV_data	
/user_audio_files	
/data/qca	
/data/mg9kem/logs	

During the time file systems are being increased, writes to the file system are blocked, and the system activity increases. The more size that is added to the file system, the greater the impact on performance.

Prerequisites

Before you perform this procedure, verify that the file system is full or nearly full and that its content is valid application data. Remove any unneeded files or files generated in error that could be taking up disk space.

Action

Perform the following steps to complete this procedure.

Simplex configuration (one server)

At your workstation

1> Telnet to the Sun server by typing

> telnet <server>

and pressing the Enter key.

where

server
is the IP address or host name of the Sun server that has the file system you want to increase

2> When prompted, enter your user ID and password.

3> Change to the root user by typing

$ su - root

and pressing the Enter key.

4> When prompted, enter the root password.

5> Access the command line interface by typing

cli

and pressing the Enter key.

Example response

Command Line Interface 1 - View

2 - Configuration

3 - Other
X - exitselect -

6> Determine which file system to increase by checking the current disk capacity utilization as follows:

a> Enter the number that corresponds to the “View” option in the menu.

Example response

View 1 - sspfs_soft (Display Software Installation Level Of SSPFS) 2 - chk_sspfs (Check SSPFS Processes) 3 - sw_conf (The software configuration of the znc0s0jx) 4 - cpu_util (Overall CPU utilization) 5 - cpu_util_proc (CPU utilization by process) 6 - port_util (I/O port utilization) 7 - disk_util (Filesystem utilization) X - exitselect -

b> Enter the number that corresponds to the “disk_util” option in the menu.

Example response

7> Determine the appropriate size for the file systems based on your specific needs.

8> Exit each menu level of the command line interface to eventually exit the command line interface, by typing

select - x

and pressing the Enter key.

9>

ATTENTION
Once you increase the size of a file system, you cannot decrease it.

Increase the size of the file system by typing

filesys grow -m <mount_point> -s <size>{m,g}

Where

mount_point
is the name associated with the file system

- /data
- /opt/nortel
- /data/oradata
- /PROV_data
- /audio_files
- /user_audio_files
- **/data/qca**
- /data/mg9kem/logs

size
is the size in megabytes (m) or gigabytes (g) you obtained in step 7

Example# filesys grow -m /data/qca -s 512m

Note: The example above increases the “/data” file system by 512 megabytes (MB).

10> You have completed this procedure.

High-availability configuration (two servers)

ATTENTION
During this procedure, the cluster will be running without a standby node. The duration is estimated at approximately one hour.

At your workstation

1> Telnet to the inactive node of the server cluster by typing

> telnet <server>

and pressing the Enter key.

where

server
is the physical IP address of the inactive node in the server cluster

2> When prompted, enter your user ID and password.

3> Change to the root user by typing

$ su - root

and pressing the Enter key.

4> When prompted, enter the root password.

5> Ensure the cluster is in a good state as follows:

a> Run the udstat command by typing

udstat

and pressing the Enter key.

If the system response contains “nodaemon”, “offline”, “down, “not mounted”, contact your next level of support. Otherwise, proceed to the next step.

b> Run the ubmstat command by typing

ubmstat

and pressing the Enter key.

If the system response is other than “ClusterIndicatorSTBY”. contact your next level of support. Otherwise, proceed to the next step.

c> Run the CheckConfiguration command by typing

CheckConfiguration

and pressing the Enter key.

If the system response is other than “Checking local cluster configuration against <other node>, contact your next level of support. Otherwise, proceed to the next step.

At the Inactive node

6>

ATTENTION
Once you increase the size of a file system, you cannot decrease it.

Increase the size of the desired file system by typing

GrowClusteredFileSystem.ksh <mount_point> <size>{m,g}

Where

mount_point
is the name associated with the file system, for example

- /data
- /opt/nortel
- /data/oradata
- /PROV_data
- /audio_files
- /user_audio_files
- **/data/qca**
- /data/mg9kem/logs

size
is the size in megabytes (m) or gigabytes (g)

Example# GrowClusteredFileSystem.ksh **/data/qca** 10m

Note: The example above increases the “/data/qca” file system by 10 megabytes (MB).

7> Reboot the Inactive node by typing

init 6

and pressing the Enter key.

8> Wait for the Inactive node to reboot, then log in again using its physical IP address.

9> Telnet to the active node of the Sun server cluster by typing

> telnet <server>

and pressing the Enter key.

where

server
is the physical IP address of the active node in the Sun server cluster

10> When prompted, enter your user ID and password.

11> Change to the root user by typing

$ su - root

and pressing the Enter key.

12> When prompted, enter the root password.

At the Active node

13> Stop the cluster by typing

StopCluster

and press the Enter key.

This action causes a cluster failover and makes the active node inactive, and the inactive node active.

At the newly Active node

14> Clone the other node using procedure Cloning the image of one node in a cluster to the other node on page 9 in this document.

15> You have completed this procedure.

Document Reference :

For increasing the size of a file system on an SSPFS-based server refer NN10402-600 (I)SN07 Standard 01.05.
Also given below - Helmsman URL

http://helmsman.us.nortel.com:8080/cgi-bin/HelmExpress/srchlite?Collec-

tion=PTIP07&SEARCH=Power+Search&PF=m&srchTerm=&boolSelection1=AND&srchTerms1=&sl=&CollCount=1&SearchType=2&ShowMeta=1&ShowDates=2&SortOrder=1&startDoc=1&sl=@34.0/

Appendix C for 89007819: List of GWs that Report End of Call QoS Statistics.

GWs Supported

Table 1 : SN06

GW	SN06 Validation Level	SN06 Comments	Future Plans (Beyond SN06)
UAS (H.248)	Full	Does not currently report all stats. The stats that are reported depend on the mode: SendOnly: PS, OS SendRecv: PS, OS, PR, OR, PL RecvOnly: PR,OR,PL	
Motorola CG4500 (NCS)	Full	5.x stream. all stats reported. Latency calculation is not PacketCable compliant.	
PVG (Aspen/ VSP2)	Full	All stats reported.	
PVG (Aspen/ VSP3)	None	All stats reported.	
PVG (H.248)	None	All stats reported.	
Mediatrix (MGCP)	Partial		
Arris PacketPort (MGCP)	Full		
Arris TTM/ TTP (NCS)	Partial		
Askey	Partial	Validated basic functionality during End to End IT. Will do further testing during PV.	

Table 1 : SN06

GW	SN06 Valida-tion Level	SN06 Comments	Future Plans (Beyond SN06)
CICM	None	CICM does not currently report end of call stats to the GWC.	Requirement submitted to CICM team, negotiating inclusion into SN07.

Table 2

GW	SN06.2 Valida-tion Level	SN06.2 Comments	Future Plans (Beyond SN06.2)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported.	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported.	
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN06.2 Valida-tion Level	SN06.2 Comments	Future Plans (Beyond SN06.2)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported.	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported.	
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN07.0 Valida-tion Level	SN07.0 Comments	Future Plans (Beyond SN07.0)
UAS		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/H.248)		Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)		All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32		All Stats supported	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported	

GW	SN07.0 Valida-tion Level	SN07.0 Comments	Future Plans (Beyond SN07.0)
PVG PP15K and PP7k (VSP2)		All parameters reported other than Jitter and inter-arrival latency which not measured.	

GW	SN08.0 Valida-tion Level	SN08.0 Comments	Future Plans (Beyond SN08.0)
Motorola MTA2	Y	All Stats Reported	
TTM/TTP Profile	Y	All Stats Reported	
ASKEY (4/12/30 Port Profile)	Y	All Stats Reported.	
Mediatrix 1104/1124 Profile	Y	All Stats Reported.	
UAS	Y	Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
MS2010 (Megaco/H.248)	Y	Does not currently report all stats. Does not report Jitter and Inter-arrival Latency.	
PVG (H.248)	Y	All stats reported.	
H.248M2K		All Stats reported.	
Ambit MG1K		All Stats reported.	
Ambit 32	Y	All Stats supported	
PVG PP15K (VSP3 and VSP3oCard)		All Stats supported	
PVG PP15K and PP7k (VSP2)	Y	All parameters reported other than Jitter and inter-arrival latency which not measured.	

Product = CS 2000

A00007217--ITRANS Media Proxy Selection

Functional Description

1: Applicable Solution(s)

CHS

This feature is mapped to Actid A00007217 and A00009367. This FN covers the functionality added by both activities.

1.1 Description

Media Proxies (MPs) have been used in Internet Transparency features since SN06.2. They allow Media Streams to be sent to/from devices that are behind Network Address Translators (NAT).

Prior to this enhancement, the MPs were provisioned against Gateway Controllers (GWC). The MPs on the GWC were selected using a "round robin" approach when a call involving one of its subtending gateways required a MP. This did not completely satisfy customer requirements because a GWC could have Media Gateways (MG) from diverse locations. The round robin approach to MP selection could cause an MG to use a MP located a great distance from it. Another MP on the same GWC could have been a better choice because it was better located relative to the MG.

This SN09 activity will improve the method of selection of a MP by allowing customers to provision Media Proxy (MP) preferred groups. A MP preferred group will represent a subset of Media Proxies that are preferable for use in a particular part of the network configuration. For example a cluster of media Proxies in a particuar location could be put in a group to be used exclusively by a set of gateways in the same location. By enabling sub-division and restricted access of Media Proxies greater flexibility is given in the use of the MPs known to the GWC.

Media Proxy Groups can be allocated to Itrans Network Zones (Nats, LBLs and composite Nat/Lbl zones). The GWC will select the MP to use for the media stream at call setup time by finding the first Media Proxy Group in the Network Zone hierarchy linked to the Gateway and selecting an MP from that group on a round robin basis. Customers will be able to allocate MPs more efficiently (in terms of increased speed and cost savings) by grouping them according to location and reducing the distance travelled through the nextwork.

In addition to the capability to create preferred Media Proxy Groups, this feature will also retain the pre-SN09 capability to allow media proxies to be

associated to GWCs. The media proxies associated to a GWC will be refered to as the GWC's default media proxies (see more detail below).

A Media Proxy may belong to more than one Media Proxy Group as well as a GWCs default media proxies. A Media Proxy Group may be associated with more than one Network Zone.

This feature also provides the capability to group Nat Itrans Network Zones into virtual private networks (VPNs). A VPN can contain one or more Nats. The VPN identifiers of the parties involved in a call will be used during call setup time to determine if a media proxy is required (see the call processing section below for more details).

Media Proxy Group (MPG) and Virtual Private Network (VPN) functionality will be included in the SN09 release and will be enabled in the CS2000 Management Tools User Interface. No additional action is required to enable this functionality.

This feature comprises provisioning enhancements and call processing enhancements.

1.1.1 Provisioning Enhancements

This enhancement will facilitate the creation, deletion and alteration of Media Proxy Groups (MPG) by means of a graphical user interface (GUI) incorporated into the CS2000 management Tools GUI. A MPG can consist of up to 5 MPs selected from a list of available MPs.

The pre-SN09 capability to provision media proxies against the whole GWC will remain. Media proxies that are provisioned against the GWC are referred to as the GWC's default media proxies, and can be used if no preferred Media Proxy Groups are provisioned. Thus, at provisioning time, a media proxy can be either:

1. Associated with one or more GWCs, but not be part of any preferred media proxy group. This is the retention of the SN08 functionality. This media proxy will be refered to as a default media proxy in SN09. And/or,

2. Made part of one or more preferred media proxy groups, And/or,

3. Made part of one or more preferred media proxy groups, and also be associated with one or more GWCs. I.e. a media proxy can be in one or more Media Proxy Groups, and also be a default media proxy for one or more GWCs.

A GWC may have none or several default media proxies associated to it.

The architecture is shown in Figure 1 below.

Figure 1 Functional Behaviour Diagram: Media Proxy Selection

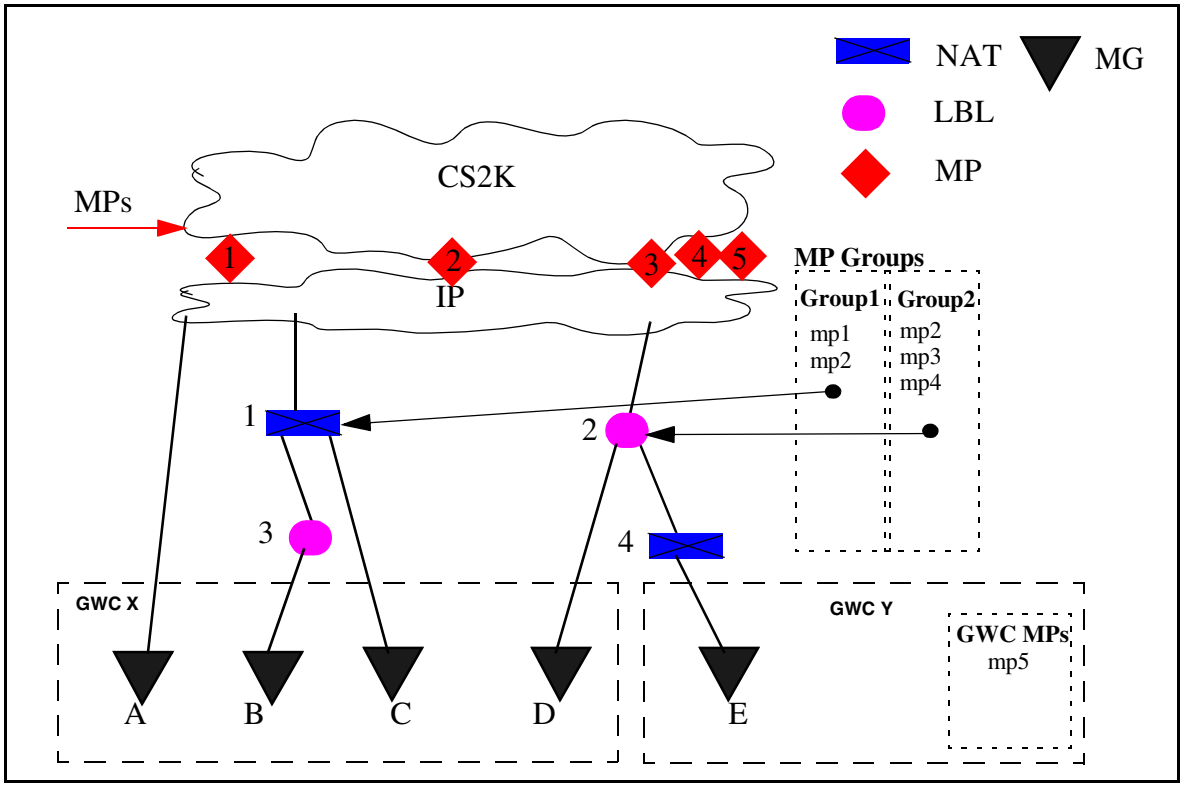


Figure 1 shows that MPs are assigned in MP Groups with some MPs being assigned as default MPs on a GWC. The MP Groups are then assigned to Nat, LBL and composite Nat/LBL Network Zones by the customer. If a call being set up on a MG requires a MP, the GWC would search the Itrans Middlebox hierarchy of the MG until it got to a NAT or LBL with a MP group. The MP would then be selected from the group on a round robin basis. If no MP Group was found in the hierarchy the GWC would select an MP from the default MPs provisioned on the GWC.

The following provisioning functionality will be added in this feature:

The capability to Provision a Media Proxy Group - a Media Proxy Group may be created with up to 5 Media proxies. A media proxy may be in more than one group and/or be one of the GWC's default media proxies.

The capability to modify a Media Proxy Group - The Media Proxies associated with a Media Proxy Group may be changed, and the number of media proxies in the group may be increased or decreased (subject to a maximum of 5 and minimum of 1). A Media Proxy Group that has been provisioned on a GWC(s) may not be modified unless it is first disassociated from the GWC(s). Disassociating the Media Proxy Group (s) from a GWC will affect call processing in that the Media proxies in the

group will not be available for selection for the duration of the modification operation.

The capability to query a Media Proxy Group - The Media Proxy Group may be queried as follows:

To return the media proxies in the group.

To return a list of all media Proxy Groups.

To return a list of GWCs that are provisioned with the Group.

To return a list of groups that have a particular Media Proxy.

The capability to delete a Media Proxy Group - The Media Proxy Group may be removed from the system. The Media Proxy Group must first be disassociated from any Itrans Network Zones that are present on any GWC.

The capability to associate a Media Proxy Group with an ITRANS Network Zone - A user may add a media proxy group to an Itrans Network Zone. A group may be associated with more than one Itrans Network Zone.

The capability to change the Media Proxy Group associated with an Itrans Network Zone - A user may change the Media Proxy Group that is selected for an Itrans Network Zone. This operation is likely to affect call processing and the availability of Media Proxies for the duration of the change.

The capability to associate a NAT Itrans Network Zone with a Virtual private network (VPN) - A NAT Network Zone may be assigned a VPN identifier. NAT Network Zones with the same VPN identifier are considered as being in the same VPN. Gateways may be moved to different network zones in a VPN even if the top-level network zones are different.

The capability to delete a VPN - A VPN may only be deleted if no NAT Network Zones are associated with it. This means that all Network Zones in a VPN must first be changed to remove the association with the VPN.

The capability to query a VPN - The NAT network Zones in the VPN may be queried.

The capability to Change a VPN - NAT Network Zones may be added or removed from a VPN by changing the VPN that a NAT Network Zone is associated with.

If any of the above listed actions fails to be executed on the server, the data will either be rolled back and the system restored to its original state or an alarm will be set to indicate a potential database mismatch. A message window will be displayed to alert the user to the provisioning fault.

1.1.2 Call Processing Enhancements

1.1.2.1 Media Proxy Selection During Call Processing.

During call setup, the GWC will determine whether or not the call requires a media proxy in order to facilitate call completion (see 2.2.2.2). If a media proxy is determined to be required, a media proxy is selected using the process in 2.2.2.3. If the selected media proxy is successfully contacted, it will be inserted into the media stream and call setup completed.

1.1.2.2 Criteria For Determining If A Media Proxy Is Required

Prior to SN09, whether or not a call required a media proxy to facilitate call completion depended on whether the parties involved in the call were behind NATs, and if so, whether the NATs of each party belonged to different Network Zones.

In SN09, whether or not a call requires a media proxy to facilitate call completion depends on whether the parties involved in that call are in the same virtual private network (VPN). A media proxy will be deemed to be required for call completion if either:

1. The two parties involved in the call belong to different VPNs. Or,

2. The call is an inter-domain SIP-T call, and the non-SIP-T media endpoint is not located in the common public domain. Or,

3. One of the endpoints is a SIP line.

1.1.2.3 Media Proxy Selection Process

At call setup time, if the GWC has determined that the call requires a media proxy to achieve call completion, a media proxy will be selected using the following process. At any point in the selection process, if a media proxy is successfully selected and contacted, then this media proxy selection process will stop and call processing will continue to insert the media proxy into the media stream, and set up the call.

MEDIA PROXY SELECTION PROCESS:

If it is determined that Early Slave Insertion of a media proxy is required, then the Slave GWC will "walk up" its Itrans Network Zone hierarchy, starting from the Itrans Network Zone adjacent to the Slave gateway, looking for a preferred media proxy group. It will select a media proxy, using a round-robin approach, from the first preferred media proxy group that it finds associated with a NAT, LBL or combined NAT-LBL zone. If none of the media proxies in that preferred media proxy group can be used, (e.g. all are out of capacity, or not active), then the Slave GWC will select a media proxy, using a round-robin approach, from its default media proxies.

If The Slave GWC does not have any default media proxies associated to it, or, if none of its default media proxies can be used (e.g. all are full to capacity), then it means that the call required a media proxy, but no useable media proxy could be found. The call will then be taken down.

However, if Early Slave Insertion is not required, then the Master GWC will "walk up" its Itrans Network Zone hierarchy, starting from the Itrans Network Zone adjacent to the gateway, looking for a preferred media proxy group. It will select a media proxy, using a round-robin approach, from the first preferred media proxy group that it finds associated with a NAT, LBL or composite NAT-LBL zone. If none of the media proxies in that preferred media proxy group can be used, (e.g. all are out of capacity, or not active), then the Master GWC will select a media proxy, using a round-robin approach, from its default media proxies.

If the Master GWC does not have any default media proxies associated to it, or,if none of its default media proxies can be used (e.g. all are full to capacity), then the Master GWC will request the Slave GWC to perform media proxy insertion, provided that the Slave GWC has media proxies provisioned.

If Slave media proxy insertion is invoked by the Master GWC, the Slave GWC will perform a media proxy selection process that is the same as that described for Early Slave Insertion above.

1.1.2.4 Load Sharing Among Media Proxies

Load sharing among media proxies is implemented as follows:

1. Within each preferred media proxy group, media proxies are selected using a round-robin approach.

2. Selection of a default media proxy, from the default media proxies allocated to a GWC, is also performed using a round-robin approach

1.2 Hardware Requirements or Dependencies

There are no additional Hardware requirements for this feature.

1.3 Software Requirements or Dependencies

- The GWC should be running a software load of an equivalent stream to that of the SESM/GWC-EM, and should be running under a profile that enables ITrans functionality.
- The GWC should be running a software load that allows the use of a preferred Media proxy group.

1.4 Limitations and restrictions

A maximum of 5 Media Proxies may be assigned to a Media Proxy group.

A maximum of 20 Media Proxies are permitted on a GWC.

A maximum of 8 Media Proxy Groups are permitted on a GWC.

A maximum of 512 Media Proxy Groups can be provisioned in the system.

A maximum of 20 GWCs can be provisioned with a particular Media Proxy.

Only an Itrans Network Zone (Nat, LBL or composite Nat/LBL) may be assigned a Media Proxy group.

An Itrans Network Zone may be assigned only one Media Proxy Group.

A Media Gateway that does not have a media Proxy Group assigned via its Itrans Network Zone Hierarchy will use the default Media Proxies provisioned on the GWC.

Media Proxies must be provisioned before Media Proxy Groups can be created.

Media Proxy Groups must be provisioned before association with an Itrans Network Zone.

Only a Nat or Composite Nat Network Zone can be provisioned with a VPN.

A VPN cannot be deleted if it contains Nat Zones that are associated on a GWC.

A Media Proxy Group cannot be deleted if it is associated with a Network Zone that is on a GWC.

A Media Proxy cannot be deleted from the system if it belongs to a media proxy group.

A Media Proxy cannot be deleted from the system if it is a default media proxy on a GWC.

A Media Proxy Group cannot be changed if it is on a GWC. Changes to a Media Proxy Group and the Media Proxies in the group must be done in such a way that the Media Proxy Group is first removed from all GWCs. This can be done by disassociating the network zone with the group from GWCs or by changing the group associated with that network zone. Changes of this nature will affect the availability of Media Proxies (for call processing) for the duration of the change.

1.5 Interactions

Changes have been made to include the Media Proxy Group association with a Network Zone. These changes are, in part, on interfaces which are common to both the Call server 2000 Management Tools (CS2MT) and the Session Policy Controller (SPC). In particular the xml schemas used by the OSSGATE interface for network Zones, are common to both systems. Therefore the changes made in the xml for the purposes of this feature are expected to be implemented in the SPC. The SPC implementation of the xml interface changes is not a part of this feature.

NAT traversal for CICM gateways is unchanged by this feature.

SIP line Provisioning is not affected by this feature. Any topology changes will flow through to the SIP GW to ensure that NAT traversal is correctly calculated. CS2K MP insertion will then proceed as normal. Media Proxy insertion by the SIP GW is unchanged and is done according to the existing SIP GW rules, using the common topology.

The provisioning of Media Proxy Group data brings changes to the following GUIs:

- GWC-EM Network Panel
- GWC Media Proxies Panel
- Add Itrans Network Zone Dialogs
- Change Itrans Network Zone Dialogs
- Itrans Network Zone Panels
- Network Devices Media Proxies Panel

See the GUI section in Configuration for full details of the changes to the GUIs.

See the OSS Gate section in Configuration for details of the xml changes.

See the Walkthrough section in Configuration for details of the provisioning use cases.

1.6 Glossary

Term	Description
Media Proxy Group	a group of Media Proxies

2: Configuration for A00007217

2.1 Initial Configuration

N/A

2.2 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

2.3 Upgrade Considerations

There are two sets of upgrade consideration. Upgrade of a GWC to SN09 and the upgrade of the CS2000 Management Tool Element manager to SN09.

For the CS2000 MT the impact is as follows:

On an upgrade of the CS2000MT to SN09, Media Proxies already provisioned on a GWC (as GWC Media Proxies) will remain as GWC default media proxies, whether or not the GWC is upgraded to SN09. If a GWC has been upgraded to SN09, The GWC media proxies will be sent to the GWC with an additional field indicating that they are GWC media Proxies.

The Media Proxies already on the system can be used after upgrade to create Media Proxy Groups regardless of whether they have been allocated to a GWC as a GWC Media Proxy.

One effect of an upgrade of the CS2000MT to SN09 will be to change the ID of all Media Proxies to use the new global ID structure. The Global ID is a unique ID across call servers representing a Network element. Each type of network element (eg Media Proxy) is allocated a set range of available IDs. The upgrade will convert the ID of any existing Media Proxies and Network Zones to the new format. New VPNs that are added will also use the new global ID format.

On the CS2000 MT User interface, the result of the upgrade will be to display the new gui panels for Media Proxy Groups and associated actions.

Upgrades of the CS2000MT from SN07 and SN08 to SN09 will be supported.

For a GWC upgrade the impact is as follows:

Once the CS2000 MT has been upgraded, the user can then begin to provision MP Groups and associate them with Network Zones (in order that the media Proxy Groups be used during call processing) as appropriate. However these changes will only be added to GWCs that are at SN09. GWCs with older loads will not be sent the Media Proxy Group or VPN data.

If a GWC is upgraded to SN09 on a newly upgraded SN09 CS2000MT, the Itrans NAT and LBL Network Zones will be sent to the GWC(s) with a “none” or “0” value for the Media Proxy group and VPN fields.

The upgrade should not have any additional impact on call processing.

SN07 and SN08 based GWCs will not support the Media Proxy Group and VPN functionality.

2.3.1 Dump and Restore (CM)

2.3.2 Element Management Upgrade

2.3.3 Downgrade impact

If the upgrade of a GWC to SN09 is aborted, the Media Proxy Group and VPN data will be removed from the GWC and all Media Proxies will revert back to being GWC default Media Proxies only.

2.4 Data schema (DS) (CM, MIBS, RDB)

2.4.1 MIB Interface

The mib is used to communicate provisioning information to the GWC. The design of the mib takes into account restrictions imposed by GWC architecture and SESM architecture.

This section describes the changes that will be made to the Mibs in order to enable the feature functionality. The Mibs that will be changed are the GWC-MIDDLE-BOX-MIB and the GWC-MEDIA-PROXY-MIB.

2.4.1.1 GWC-MIDDLE-BOX-MIB

GWC-MIDDLE-BOX-MIB adds two new fields:

- The **MiddleBoxMPGroupId** field is used to identify the preferred MediaProxyGroup for the middle box. The value of this field is used to index into the MediaProxyGroup table on the GWC. A GWC can have a maximum of 8 groups and there may be up to 512 MP groups in the system. The design component determines what range the above field can take in the mib.
- The **MiddleBoxVpnGID** field represents a global Identifier indicating the VPN that the MiddleBox is part of (applies to NATs only). If this field is set to 0, it means that the NAT does not belong to any provisioned or shared VPN.

MIB Definition

```
-- DMS Call Server GateWay Controller Middle Box Table Data MIB


GWC-MIDDLE-BOX-MIB DEFINITIONS ::= BEGIN
    IMPORTS
       OBJECT-TYPE, MODULE-IDENTITY, enterprises, IpAddress, Integer32
            FROM SNMPv2-SMI
        DisplayString, RowStatus
            FROM SNMPv2-TC
        GWCDeviceType, GWCDeviceProtocol, GWCDeviceProtVersion
            FROM NORTEL-GWC-COMMON-TC;


--
-- Define the location of this MIB within the MIB tree
--
```

```
nortel    OBJECT IDENTIFIER ::= { enterprises 562 }
voip      OBJECT IDENTIFIER ::= { nortel 28 }
ptn             OBJECT IDENTIFIER ::= { voip 0 }
serviceControlOBJECT IDENTIFIER ::= { ptn 1 }
legacyCallServerOBJECT IDENTIFIER ::= { serviceControl 4 }
lcsGateWayController OBJECT IDENTIFIER ::= { legacyCallServer 1 }

--
-- Define the elements in the GWC Middle Box Table Data MIB
--

gwcMiddleBoxTblMIB MODULE-IDENTITY
      LAST-UPDATED "200209240000Z"   -- 24th September 2002
      ORGANIZATION "Nortel DMS Call Server"
      CONTACT-INFO "Eman Jado-Adham
           Nortel Networks Inc.
                    1285 Baseline Road
                    Ottawa, Canada
                    Phone: (613) 763-3089
                    email: emanjado@nortelnetworks.com"
      DESCRIPTION  "The MIB module defines information about
           the Middle Box table(s) provision supported
                    by the GateWay Controller (GWC)."

      REVISION     "200209240000Z"
      DESCRIPTION  "add new fields for Internet Transparency
                    functionality (CAC, NAT traversal)"

      REVISION     "200409080000Z"
      DESCRIPTION  "Add new PORT field for support of ALG\par
                    Middle box"

      REVISION     "200411010000Z"
      DESCRIPTION  "Correct the MiddleBox GID to expand the
                    range greater than 65535.  This is required
                    for the larger ids that can result with the
                    CallAgent Id being set."

  ::= { lcsGateWayController 18 }

middleBoxTable OBJECT-TYPE
    SYNTAX SEQUENCE OF MiddleBoxEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
       "This table contains Middle Box data.
        The number of entries in this table
        depends on the type of the Middle Box
        for this GWC."
    ::= { gwcMiddleBoxTblMIB 1 }

--
-- Define the row objects in the table middleBoxTable
--

middleBoxEntry OBJECT-TYPE
    SYNTAX MiddleBoxEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "An entry describes the characteristics of the
         Middle Box, e.g. Policy Enforcement Point (PEP),
              needed for setting up calls with DQoS or Admission
              Control quality, .... ."
       INDEX { middleBoxGID }
    ::= { middleBoxTable 1 }
```

```
-- Define the fields

MiddleBoxEntry ::= SEQUENCE {
    middleBoxGID            Integer32,
    middleBoxName           DisplayString (SIZE(1..32)),
    middleBoxAddress        IpAddress,
    middleBoxType           GWCDeviceType,
    middleBoxStatus          INTEGER,
    middleBoxEntryStatus     RowStatus,
    middleBoxProtocol        GWCDeviceProtocol,
    middleBoxProtVers        GWCDeviceProtVersion,
    middleBoxCacType         INTEGER,
    middleBoxRUfactor        Integer32(0..255),
    middleBoxMaxCount        Integer32,
    middleBoxNatType         INTEGER,
    middleBoxParentMB        Integer32,
    middleBoxPort            Integer32(0..65535),
    middleBoxMPGroupId       Integer32(0..512),
    middleBoxVPNGID          Integer32
     }

middleBoxGID OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Middle Box Global Identifier."
    ::= { middleBoxEntry 1 }

middleBoxName OBJECT-TYPE
    SYNTAX DisplayString (SIZE(1..32))
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "String that identifies FQDN of theMiddle Box."
    ::= { middleBoxEntry 2 }

middleBoxAddress OBJECT-TYPE
        SYNTAX IpAddress
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
            "IP Address of the Middle Box."
        DEFVAL { '00000000'h }
        ::= { middleBoxEntry 3 }

middleBoxType OBJECT-TYPE
    SYNTAX GWCDeviceType
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Type of device in the GWC defined in GWC-TC."
    ::= { middleBoxEntry 4 }

middleBoxStatus OBJECT-TYPE
    SYNTAX INTEGER { unintialized (0),
                     connecting   (1),
                     connected    (2),
                     initializing (3),
                     initalized   (4),
                     deleting     (5) }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
        "Status of Middle Box."
    ::= { middleBoxEntry 5 }

middleBoxEntryStatus  OBJECT-TYPE
```

```
    SYNTAXRowStatus
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Status column for row entry."
    ::= { middleBoxEntry 6 }

middleBoxProtocol OBJECT-TYPE
        SYNTAX GWCDeviceProtocol
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
            "Comms protocol supported by the middlebox.
             This enumerated list matches the list of supported
             protocols as defined in the GWC."
        DEFVAL { 0 }
        ::= { middleBoxEntry 7 }

middleBoxProtVers OBJECT-TYPE
        SYNTAX GWCDeviceProtVersion
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
        "Version of the comms protocol supported
         by the middlebox."
        DEFVAL { "0.0" }
        ::= { middleBoxEntry 8 }

middleBoxCacType OBJECT-TYPE
    SYNTAX INTEGER { none         (0),
                     internal     (1) }
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Type of Connection Admissions Control (CAC)
         for a given middlebox. Internal indicates that
         the GWC must provide a virtual CAC function."
        DEFVAL { 0 }
    ::= { middleBoxEntry 9 }

middleBoxRUfactor OBJECT-TYPE
    SYNTAX Integer32(0..255)
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Resource Usage factor, used in carrying out
         virtual CAC."
        DEFVAL { 0 }
    ::= { middleBoxEntry 10 }

middleBoxMaxCount OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Max resource value for a link on which virtual
         CAC will be performed."
        DEFVAL { 0 }
    ::= { middleBoxEntry 11 }

middleBoxNatType OBJECT-TYPE
    SYNTAX INTEGER { none            (0),
                     noncontrolled   (1) }
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "NAT capability of a given middlebox.
         non_controlled indicates that NAT is present
```

```
        but that we don't control it directly,
        therefore need to resort to other means"
        DEFVAL { 0 }
    ::= { middleBoxEntry 12 }

middleBoxParentMB OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "GID of next middlebox between this one and the
        the network core."
        DEFVAL { 0 }
    ::= { middleBoxEntry 13 }

middleBoxPort OBJECT-TYPE
        SYNTAX Integer32
        MAX-ACCESS  read-create
        STATUS current
        DESCRIPTION
            "ALG Middle Box UDP Port Number used by GWC
        to communicate to ALG."
        DEFVAL { 0 }
        ::= { middleBoxEntry 14 }


middleBoxMPGroupId OBJECT-TYPE
    SYNTAX Integer32(0..512)
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "ID of MPG group that is associated with this middlebox. 0
indicate
        no MPG is assigned."
        DEFVAL { 0 }
    ::= { middleBoxEntry 15 }

middleBoxVPNGID OBJECT-TYPE
        SYNTAX Integer32(0..64)
        MAX-ACCESS  read-create
        STATUS current
        DESCRIPTION
            "GID to indicate which VPN a NAT is part of. Used when
multiple
            NATs are in a single VPN. 0 indicates this NAT is the only
            NAT in this VPN"
        DEFVAL { 0 }
        ::= { middleBoxEntry 16 }

middleBoxLastOperationErrorMessage OBJECT-TYPE
        SYNTAX DisplayString (SIZE(1..128))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
            "Error Message holds a descriptive error message
            in case of an snmp failure of the last operation."
        ::= { gwcMiddleBoxTblMIB 2 }

middleBoxLastOperationErrorType OBJECT-TYPE
    SYNTAX INTEGER { information    (0),
                     warning        (1),
                     error          (2) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
            "This value contains the type of error that occurred on
            the last SET failure on any variable in a middleBox table.
              The combination of this type and the error message give
```

```
                the manager enough information to process the failure."
        ::= { gwcMiddleBoxTblMIB 3 }

END
```

2.4.1.2 GWC-MEDIA-PROXY-MIB

GWC-MEDIA-PROXY-MIB adds two new fields.

MediaProxyInGWCGroup is used to indicate whether or not the Media proxy has been provisioned as a media Proxy on the GWC. This field can be set to Y or N. A value of Y indicates that the Media Proxy belongs to the group of default media Proxies on the GWC (it may or may not be in one or more MP groups as well). A value of N means that the Media Proxy is not part of the group of default media Proxies but that it must be in at least one MP group because it is present on the GWC.Service Orders (SO) (CM & SESM).

MediaProxyGlobalID This fields represents a unique global ID for a specific MediaProxy within the system.

There is also a new table added to the GWC-MEDIA-PROXY-MIB. This is a new table to convey MediaProxy Group Data to the GWC. The new structure is defined as follows:

mediaProxyGroupTable - table containing data on MediaProxyGroups. Each Entry in the table consists of a sequence of the following sets of fields:
mediaProxyGroupID - The global id of the Media Proxy Group.
mediaProxyID - The global id that identifies a Media Proxy in the Media Proxy Group.

mediaProxyGroupEntryStatus - the entry status of the row.

The table has been designed to accommodate any number of media proxies in a group, however, the number of media proxies in a group in SN09 is restricted to a maximum of 5.

MIB Definition

```
-- DMS Call Server GateWay Controller Media Proxy MIB


GWC-MEDIA-PROXY-MIB DEFINITIONS ::= BEGIN
    IMPORTS
       OBJECT-TYPE, MODULE-IDENTITY, enterprises, IpAddress, Integer32
            FROM SNMPv2-SMI
        RowStatus, DisplayString
            FROM SNMPv2-TC
        GWCDeviceProtocol, GWCDeviceProtVersion
            FROM NORTEL-GWC-COMMON-TC;

--
-- Define the location of this MIB within the MIB tree
--
```

```
nortel    OBJECT IDENTIFIER ::= { enterprises 562 }
voip      OBJECT IDENTIFIER ::= { nortel 28 }
ptn             OBJECT IDENTIFIER ::= { voip 0 }
serviceControlOBJECT IDENTIFIER ::= { ptn 1 }
legacyCallServerOBJECT IDENTIFIER ::= { serviceControl 4 }
lcsGateWayController OBJECT IDENTIFIER ::= { legacyCallServer 1 }

--
-- Define the elements in the GWC Media Proxy MIB
--

gwcMediaProxyMIB MODULE-IDENTITY
      LAST-UPDATED "200210220000Z"   -- 22nd October 2002
      ORGANIZATION "Nortel DMS Call Server"
      CONTACT-INFO "Mike Fryars
           Nortel Networks UK Limited
                    Maidenhead Office Park, Westacott Way
                    Maidenhead, Berks, SL6 3QH
                    United Kingdom
                    Phone: +44 (0)1628 431603
                    email: mfryars@nortelnetworks.com"
      DESCRIPTION  "The MIB module defines information about
           Media Proxy Devices."

  ::= { lcsGateWayController 23 }


mediaProxyTable OBJECT-TYPE
    SYNTAX SEQUENCE OF MediaProxyEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
       "Table containing data on Media Proxy devices."
    ::= { gwcMediaProxyMIB 1 }

--
-- Define the row objects in the table middleboxRsrcUsageTable
--

mediaProxyEntry OBJECT-TYPE
    SYNTAX MediaProxyEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table entry containing data on a particular Media
              Proxy device."
      INDEX { mediaProxyName }
    ::= { mediaProxyTable 1 }

-- Define the fields

MediaProxyEntry ::= SEQUENCE {
    mediaProxyName          DisplayString (SIZE(1..32)),
    mediaProxyAddress       IpAddress,
    mediaProxyProtocol      GWCDeviceProtocol,
    mediaProxyProtVersion   GWCDeviceProtVersion,
    mediaProxyEntryStatus   RowStatus,
    mediaProxyInGWCGroup    DisplayString (SIZE (1)),
    mediaProxyGlobalID      Integer32
    }


mediaProxyName OBJECT-TYPE
    SYNTAX DisplayString (SIZE(1..32))
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "String that identifies the Media Proxy."
```

```
    ::= { mediaProxyEntry 1 }

mediaProxyAddress OBJECT-TYPE
        SYNTAX IpAddress
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
            "IP Address of the Media Proxy."
        DEFVAL { '00000000'h }
        ::= { mediaProxyEntry 2 }

mediaProxyProtocol OBJECT-TYPE
    SYNTAX GWCDeviceProtocol
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
             "Comms protocol supported by the Media Proxy.
              This enumerated list matches the list of supported
              protocols as defined in the GWC."
    ::= { mediaProxyEntry 3 }

mediaProxyProtVersion OBJECT-TYPE
    SYNTAX GWCDeviceProtVersion
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Version of the comms protocol supported
         by the Media Proxy."
    ::= { mediaProxyEntry 4 }

mediaProxyEntryStatus  OBJECT-TYPE
    SYNTAXRowStatus
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Status column for row entry."
    ::= { mediaProxyEntry 5 }

mediaProxyInGWCGroup  OBJECT-TYPE
    SYNTAX DisplayString (SIZE (1))
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
       "A character indicating if this MP is part of the GWC's default
list. Y if it is in the list N if not."
    ::= { mediaProxyEntry 6 }

mediaProxyGlobalID  OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "A unique ID within the system identifying a specific MP."
    ::= { mediaProxyEntry 7 }


mediaProxyLastOperationErrorMessage OBJECT-TYPE
        SYNTAX DisplayString (SIZE(1..128))
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
           "Error Message holds a descriptive error message
            in case of an snmp failure of the last operation."
        ::= { gwcMediaProxyMIB 2 }

mediaProxyLastOperationErrorType OBJECT-TYPE
    SYNTAX INTEGER { information    (0),
                     warning        (1),
```

```
                    error          (2) }
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
            "This value contains the type of error that occurred on
             the last SET failure on any variable in the resource
             usage table. The combination of this type and the error
             message give the manager enough information to process
             the failure."

        ::= { gwcMediaProxyMIB 3 }

mediaProxyGroupTable OBJECT-TYPE
    SYNTAX SEQUENCE OF MediaProxyGroupEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
       "Table containing data on Media Proxy Groups."
    ::= { gwcMediaProxyMIB 4 }

mediaProxyGroupEntry OBJECT-TYPE
    SYNTAX MediaProxyGroupEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
        "Table entry containing data on a particular MediaProxy
group"
    INDEX { mediaProxyGroupID}
    ::= { mediaProxyGroupTable 1 }

-- Define the fields

MediaProxyGroupEntry ::= SEQUENCE {
      mediaProxyGroupID      Integer32 (0..512),
      mediaProxyID1      Integer32 ,
      mediaProxyID2      Integer32 ,
      mediaProxyID3      Integer32 ,
      mediaProxyID4      Integer32 ,
      mediaProxyID5      Integer32 ,
      mediaProxyID6      Integer32 ,
      mediaProxyID7      Integer32 ,
      mediaProxyID8      Integer32 ,
      mediaProxyID9      Integer32 ,
      mediaProxyID10     Integer32 ,
      mediaProxyGroupEntryStatus      RowStatus
    }

mediaProxyGroupID OBJECT-TYPE
    SYNTAX Integer32 (0..512)
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Media Proxy Group ID."
         DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 1 }

mediaProxyID1 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
       "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
         DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 2 }

mediaProxyID2 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
```

```
    STATUS current
    DESCRIPTION
        "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
         DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 3 }

mediaProxyID3 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
         DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 4 }

mediaProxyID4 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
    DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 5 }

mediaProxyID5 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "ID that identifies the Media Proxy. 0 indicate no Media Proxy."
    DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 6 }

-- mediaProxyIDs 6-10 are reserved for furture expansion in SN09 the
-- customer will only be allowed to provision 5 MediaProxies per group.

mediaProxyID6 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
         DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 7 }

mediaProxyID7 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
         DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 8 }

mediaProxyID8 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
       DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 9 }


mediaProxyID9 OBJECT-TYPE
    SYNTAX Integer32
```

```
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
    DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 10 }

mediaProxyID10 OBJECT-TYPE
    SYNTAX Integer32
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Reserved for future expansion"
       DEFVAL { 0 }
    ::= { mediaProxyGroupEntry 11 }

mediaProxyGroupEntryStatus  OBJECT-TYPE
    SYNTAXRowStatus
    MAX-ACCESS read-create
    STATUS current
    DESCRIPTION
        "Status column for row entry."
    ::= { mediaProxyGroupEntry 12 }

mediaProxyGroupLastOperationErrorMessage OBJECT-TYPE
    SYNTAX DisplayString (SIZE(1..128))
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
       "Error Message holds a descriptive error message
        in case of an snmp failure of the last operation."
    ::= { gwcMediaProxyMIB 5 }

mediaProxyGroupLastOperationErrorType OBJECT-TYPE
     SYNTAX INTEGER { information    (0),
              warning    (1),
              error    (2) }
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
       "This value contains the type of error that occurred on
         the last SET failure on any variable in the resource
         usage table. The combination of this type and the error
         message give the manager enough information to process
         the failure."

    ::= { gwcMediaProxyMIB 6 }
```

END

2.5 Service Orders (SO) (CM & SESM)

N/A

2.6 Software optionality control (SOC)

N/A

2.7 Element Management

The GWC Element manager part of the CS2M Configuration Management Tools will be used to perform the configuration procedures for this component.

2.7.1 New/modified GUIs

All new and modified GUIs are part of the CS2M Configuration Management Tool GUI.

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Add Media Proxy Group dialog	New
Change Media Proxy Group Dialog	New
Media Proxies Tab	Changed
Media Proxies Details Dialog	New
Media Proxy Groups Tab	New
Media Proxy Group Details Dialog	New
Add Nat Dialog	Changed
Add NAT/LBL Dialog	Changed
Nat Network Zone Panel	Changed
NAT/LBL Network Zone Panel	Changed
Change Nat Dialog	Changed
Change NAT/LBL Dialog	Changed
Zone Details	New
VPN Details	New
Zone GWCID Details	Changed
Zone GW Report Details	Changed
GWC Media Proxies Tab	Changed

2.7.1.1 GUI name:AddMPGroup

Add Media Proxy Group Dialog

2.7.1.1.1 Functional description

The purpose of this Dialog is to add a new Media Proxy group and add up to five Media Proxies to the group. Only previously provisioned Media Proxies can be added to a Media Proxy group. A Media Proxy can be added to more than one group.

There are a maximum of 512 Media Proxy Groups allowed in the system. A Media Proxy group may be selected from the left hand list and the “Add>>”

button used to transfer it to the right hand list of selected media Proxies for the Group.

A Media Proxy group may be selected from the right hand list and the "<<Rem" button used to transfer it to the list of available Media Proxies on the left.

A name must be entered in the dialog box at the top. This should be a unique and meaningful name.

When an appropriate number of Media Proxies have been selected and the name filled in, the ok button can be selected.

2.7.1.1.2 GUI usage and implications

This gui is used to create a new group containing a subset of the Media Proxies on the system. The group can then be allocated to an ITRANs Middlebox and in turn associated with a gateway. When this happens the GWC for the gateway is provisioned with details of the Media Proxies in the group.

A group must have been provisioned using this dialog before an ITRANs Middlebox can be associated with a group.

The Media Proxies must have been provisioned on the system prior to this GUI being invoked. If this is not the case then no Media Proxies will be available to be added to the group.

2.7.1.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
AddMPGroup	0	1	N/A

2.7.1.1.4 GUI fields

The following table lists fields for GUI AddMPGroup.Media Proxies must have been provisioned before the AddMPGroup dialog is invoked.

Table 3 GUI field descriptions

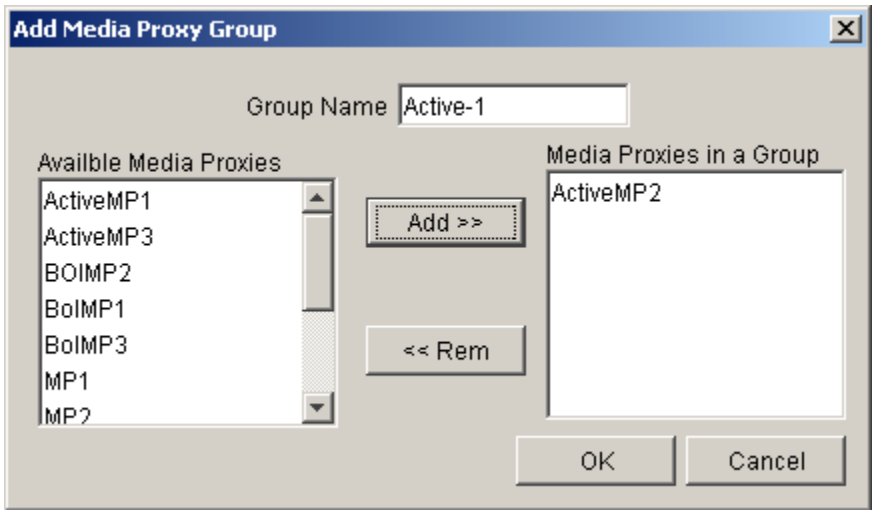
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Group Name	New	none	media proxy group name	This field holds the name of the media proxy group.	

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxies	New	none	range of Media proxies	This displays the media proxies which can be added to the group	
Media Proxy Group	New	none	selected media proxies (max of 5)	This box shows the list of media proxies which have been selected for the group.	

2.7.1.1.5 Usage example

The following example shows sample datafill or menu selection for GUI AddMPGroup:



2.7.1.1.6 GUI release history update

This is a new GUI. First release.

2.7.1.1.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.1.8 Supplementary information

NONE

2.7.1.2 GUI name: ChangeMPGroup

Change Media Proxy Group Dialog

2.7.1.2.1 Functional description

The Change Media Proxy Group Dialog is a new Dialog to allow the alteration of the Media Proxies contained within a selected Media Proxy group. It is similar in appearance to the AddMPGroup Dialog.

A Media Proxy group may be selected from the left hand list and the “Add>>” button used to transfer it to the right hand list of selected Media Proxies for the Group.

A Media Proxy group may be selected from the right hand list and the “<<Rem” button used to transfer it to the list of available Media Proxies on the left.

The name of the group may not be changed.

2.7.1.2.2 GUI usage and implications

This Gui is to be used when any changes to the number of media proxies in the group are to be made (subject to the maximum limit). It is also to be used when one or more of the Media Proxies in the group is to be replaced with another.

Any additional Media Proxies must exist prior to this GUI being invoked. If this is not the case then no additional Media Proxies will be available to be added to the group. The addMediaProxy dialog enables Media Proxies to be added.

Media Proxies cannot be deleted from the system if they are in a Media Proxy group.

2.7.1.2.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
ChangeMPGroup	0	1	N/A

2.7.1.2.4 GUI fields

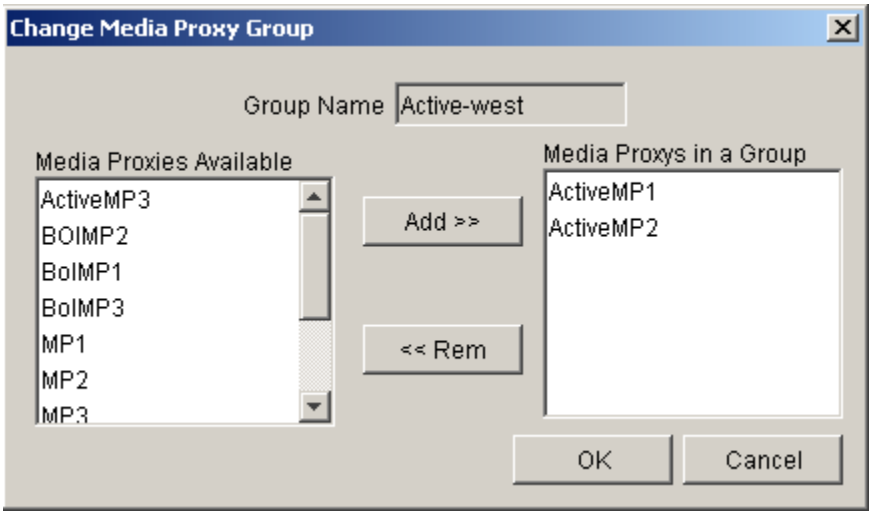
The following table lists fields for GUI ChangeMPGroup.Media Proxies must have been provisioned before the ChangeMPGroup dialog is invoked.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxies	New	none	range of Media proxies	this displays the media proxies which can be added to the group	
Media Proxy Group	New	none	selected media proxies (max of 5)	This box shows the list of media proxies which have been selected for the group.	

2.7.1.2.5 Usage example

The following example shows sample datafill or menu selection for GUI ChangeMPGroup:



2.7.1.2.6 GUI release history update

New Dialog, first release.

2.7.1.2.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.2.8 Supplementary information

NONE

2.7.1.3 GUI name: MPGroupTab

Media Proxy Groups Tab

2.7.1.3.1 Functional description

This tab is designed to show a list of Media Proxy Groups along with a comma separated list of the Media Proxies belonging to that group.

The tab also displays the following buttons:

Add - to add a new Media Proxy Group. When clicked this will launch the AddMPGroup Dialog described in section 12.8.2.3.

Delete - to delete a Media Proxy Group that has been selected from the list. When selected a dialog will ask for confirmation that the selected Media proxy group is to be deleted. This delete will fail if the Media Proxy Group is associated with any ITRANs Middleboxes that are on a GWC.

Change - to change the Media Proxies listed against a selected Media Proxy Group. When selected this will launch the ChangeMPGroup" Dialog described in section 12.8.2.4.

Properties - The properties button will launch the "Describe Media Proxy Group."

2.7.1.3.2 GUI usage and implications

This GUI is used for display purposes and to provide a central point of access for all Media Proxy Group operations.

2.7.1.3.3 GUI size

Table 6 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
MPGTab	1	1	N/A

2.7.1.3.4 GUI fields

The following table lists fields for the MPGroup Tab

Table 7 GUI field descriptions

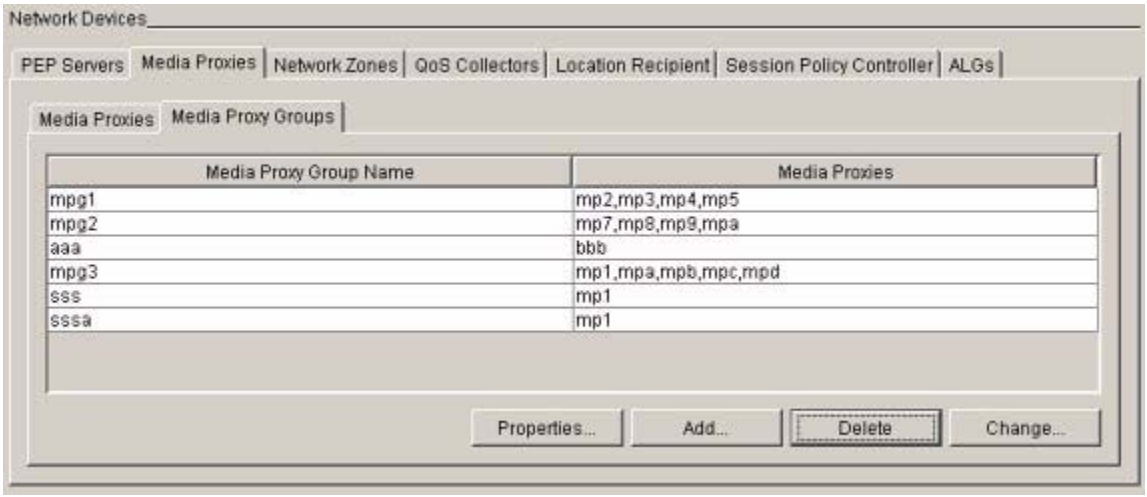
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxy Group Name	New	none	values of media proxy groups	A column showing the list of media proxy groups	

Table 7 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxies	New	None	values of the selected media Proxies	a column showing a comma separated list of the media proxies which have been selected for the Group in column one.	

2.7.1.3.5 Usage example

The following example shows sample datafill or menu selection for GUI MPGroupTab:



2.7.1.3.6 GUI release history update

New Tabbed panel. First release

2.7.1.3.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.3.8 Supplementary information

NONE

2.7.1.4 GUI name: MP Tab

Media Proxies Tab

2.7.1.4.1 Functional description

The Media Proxies tab has been modified to contain two sub-tabbed panels. The first sub tab will contain the content of the existing Media Proxy tabbed panel.

The second sub panel will contain the new Media Proxy Group tabbed panel.

The purpose of the Media Proxies tab is to make available information relating to the Media Proxies provisioned on the system. This tab is visible in the Network devices domain.

2.7.1.4.2 GUI usage and implications

This is the first gui to go to when viewing or performing operations involving system Media Proxies or Media Proxy Groups.

2.7.1.4.3 GUI size

Table 8 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
MPTab	1	1	N/A

2.7.1.4.4 GUI fields

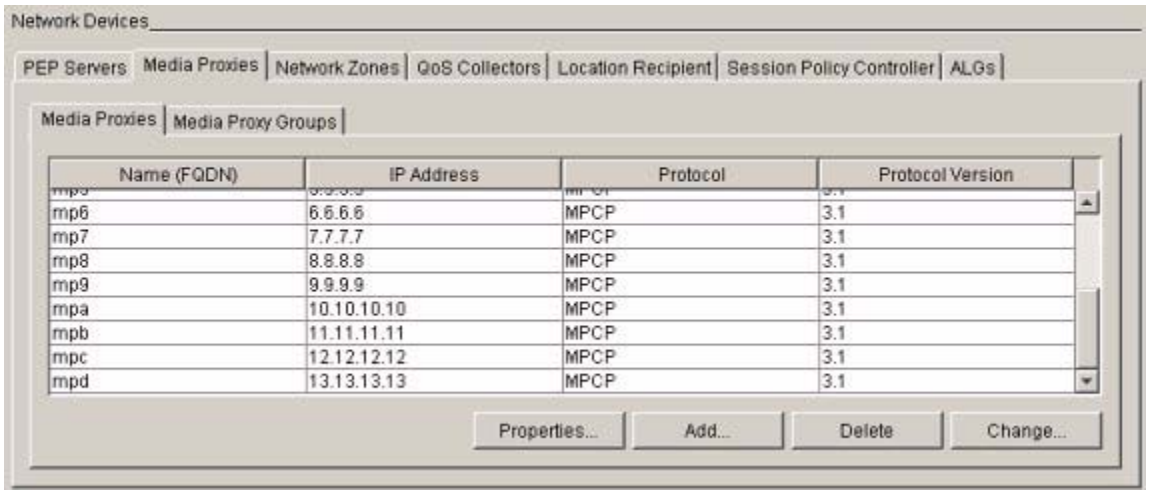
The following table lists fields for the MP tab.

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

2.7.1.4.5 Usage example

The following example shows sample datafill or menu selection for GUI MP Tab:



2.7.1.4.6 GUI release history update

Two sub tabs have been added to this tabbed Panel. The first contains the original content of the tab and the second contains information about the Media Proxy Groups.

2.7.1.4.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.4.8 Supplementary information

NONE

2.7.1.5 GUI name: Media Proxy Description

Media Proxies Description Dialog

2.7.1.5.1 Functional description

The Media Proxy description dialog is there to provide handy information about what is using the Media Proxy.

The dialog will contain lists of all of the gateway controllers that are using the Media Proxy and the Media Proxy Groups that contain the selected Media Proxy.

The button that displays this dialog is available on the Media Proxy panel. A Media Proxy must be selected from the panel for the details to be shown.

2.7.1.5.2 GUI usage and implications

This GUI is used when the user wishes to find out more information on a specific Media Proxy group without having to navigate to the gateway controller GUI or the Media Proxy group GUI.

2.7.1.5.3 GUI size

Table 10 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Media Proxy Description Dialog	1	1	N/A

2.7.1.5.4 GUI fields

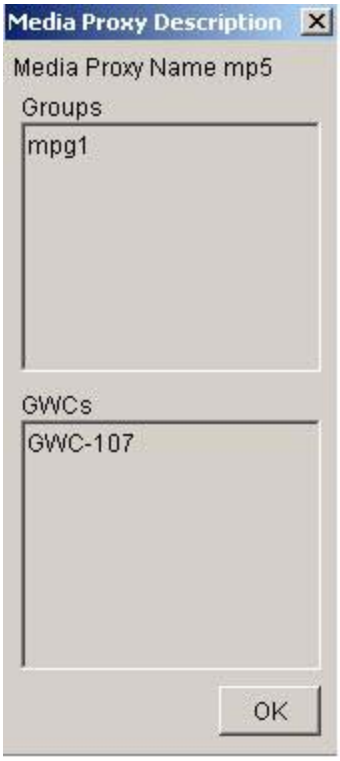
The following table lists fields for the MP tab.

Table 11 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

2.7.1.5.5 Usage example

The following example shows a sample Media Proxy that is used in two Media Proxy Groups:



2.7.1.5.6 GUI release history update

2.7.1.5.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.5.8 Supplementary information

NONE

2.7.1.6 GUI name: Media Proxy Groups Description

Media Proxy Groups Description

2.7.1.6.1 Functional description

The Media Proxy Group description dialog is there to provide handy information about what is using the Media Proxy Group.

The dialog will contain lists of all of the gateway controllers and the NATs that are using the Media Proxy Group.

The button that displays this dialog is available on the Media Proxy Group panel. A Media Proxy Group must be selected from the panel for the details to be shown.

2.7.1.6.2 GUI usage and implications

This GUI is used when the user wishes to find out more information on a specific Media Proxy Group without having to navigate to the gateway controller GUI or the Media Proxy GUI.

2.7.1.6.3 GUI size

Table 12 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Media Proxy Group Details Dialog	1	1	N/A

2.7.1.6.4 GUI fields

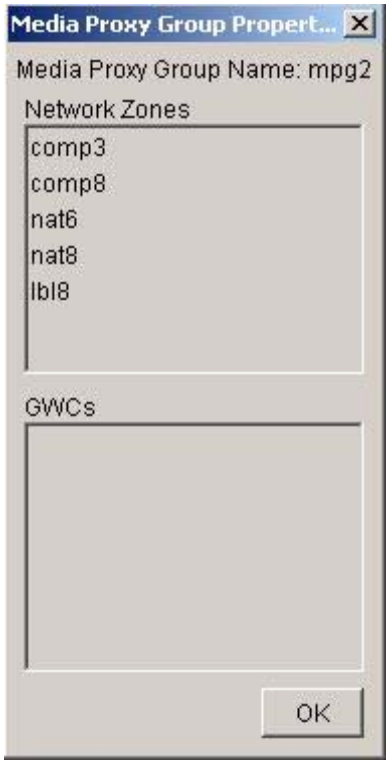
The following table lists fields for the MP tab.

Table 13 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

2.7.1.6.5 Usage example

The following example shows a sample Media Proxy Group that is used by a NAT and is present on a GWC.



2.7.1.6.6 GUI release history update
This is a new dialog.

2.7.1.6.7 Context sensitive launching information
This is launched using the CS2000 Management Tools interface

2.7.1.6.8 Supplementary information
NONE

2.7.1.7 GUI name: NAT Panel
NAT Panel

2.7.1.7.1 Functional description
Two new fields have been added to the list in the NAT Panel. The first displays any selected Media Proxy Group name and the second any chosen VPN name. Two new buttons have also been added to the panel. The first, called “VPN” is the link the VPN details dialog. This displays details of the VPNs.

The “details” button is the replacement for the buttons to display the zone ID and the gateway report.

2.7.1.7.2 GUI usage and implications

This GUI will now display Media Proxy Group and VPN names for NATs.

2.7.1.7.3 GUI size

Table 14 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NATMiddlebox Panel	1	1	N/A

2.7.1.7.4 GUI fields

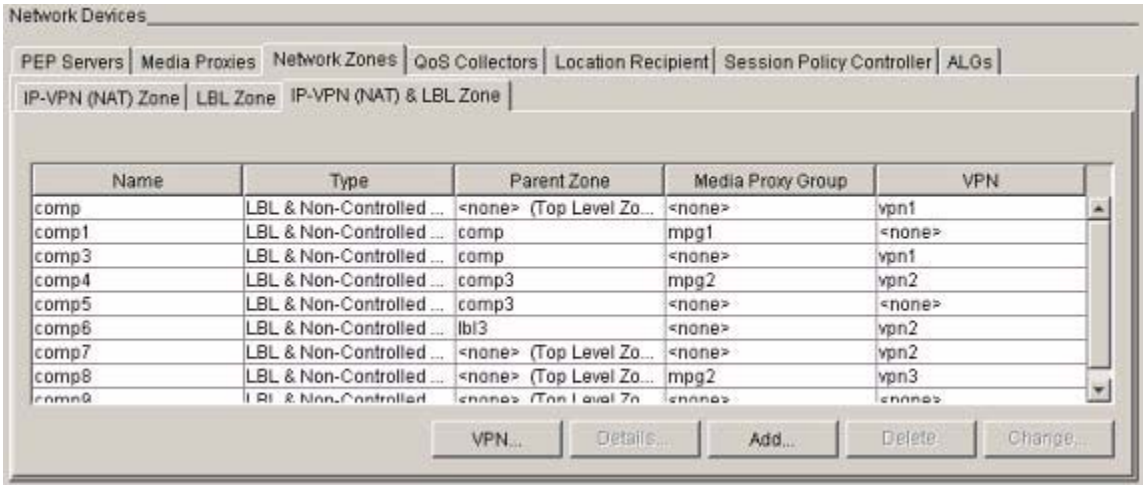
The following table lists fields for the MP tab.

Table 15 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxy Group	New			Displays the selected media proxy group.	?
VPN	New			Displays the selected VPN.	?

2.7.1.7.5 Usage example

The following example shows sample NAT and LBL Zones with Media Proxy Groups and/or a VPN :



2.7.1.7.6 GUI release history update

Two fields have been added to display the chosen Media Proxy Group and the chosen VPN.

Two buttons have been added - " VPN" and "details"

2.7.1.7.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.7.8 Supplementary information

NONE

2.7.1.8 GUI name: Add NAT

Add NAT Middlebox Dialog

2.7.1.8.1 Functional description

The add NAT dialog box has been modified to allow the selection of a Media Proxy Group and the option of adding a NAT to a VPN.

A new drop down box has been added which displays the list of the datafilled Media Proxy Groups. The default option is no Media Proxy Group.

The default display also includes a VPN check box. VPN information is only available if this tick box is selected. Selection of this box gives the user the choice of either selecting an existing VPN or creating a new one. Choosing the "create VPN" button will display a further dialog.

2.7.1.8.2 GUI usage and implications

This gui is used when a new NAT is created. It can also be used to create a new VPN.

2.7.1.8.3 GUI size

Table 16 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
AddNat	1	1	N/A

2.7.1.8.4 GUI fields

The following table lists fields for the MP tab.

Table 17 GUI field descriptions

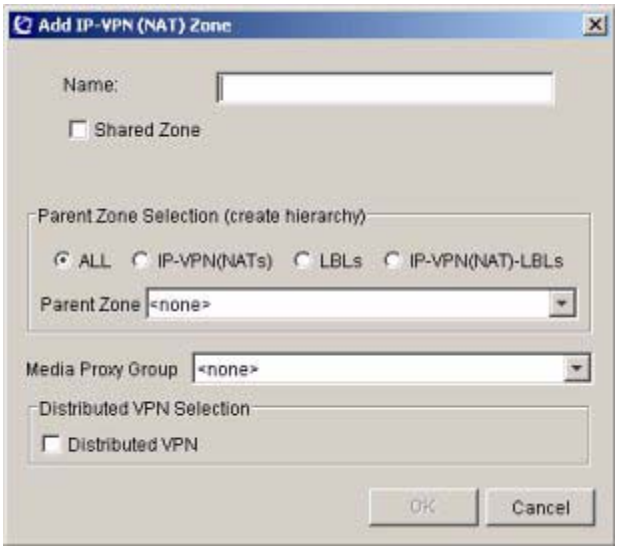
Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Media Proxy Group	New			To select a media proxy group	

Table 17 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
VPN	New			To select a VPN	

2.7.1.8.5 Usage example

The following example shows a new NAT being added which uses the London Media Proxy Group and is part of VPN1.



2.7.1.8.6 GUI release history update

The Media Proxy Group combo box has been added along with the Use VPN checkbox, VPN combo box and create vpn button.

2.7.1.8.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.8.8 Supplementary information

NONE

2.7.1.9 GUI name:Change NAT

Change NAT

2.7.1.9.1 Functional description

Please see Add NAT for details.

2.7.1.9.2 GUI usage and implications

Please see Add NAT for details.

2.7.1.9.3 GUI size

Table 18 New or modified GUIs

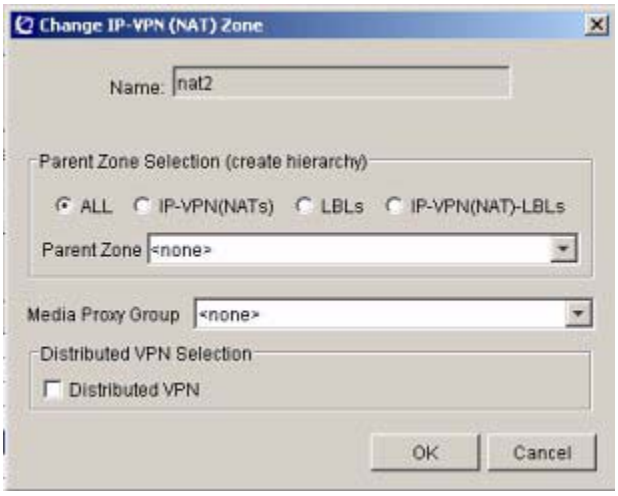
Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
ChangeNAT	1	1	N/A

2.7.1.9.4 GUI fields

Please see Add NAT for details.

2.7.1.9.5 Usage example

The following example shows a media proxy group and a VPN being added to an existing NAT.



2.7.1.9.6 GUI release history update

Please see Add NAT for details.

2.7.1.9.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.9.8 Supplementary information

NONE

2.7.1.10 GUI name: Add VPN

Add VPN Dialog.

2.7.1.10.1 Functional description

This is a new dialog box that is used when a new VPN is being created. The dialog contains a text box in which the user adds a new VPN name. On clicking the OK button the VPN is created but is not assigned to any NAT. The new VPN will automatically be added to the VPN combo box on the addnat dialog.

An optional check box “Shared Id” will display a field into which a specific Global ID can be entered for the VPN. This is to be used when the VPN is shared across Element managers. It does reuire that the ID to be shared is not already allocated to another VPN.

This dialog can only be called from the Add NAT dialog or the “Add” Button on the VPN details dialog.

2.7.1.10.2 GUI usage and implications

This dialog can only be called from the Add NAT dialog or by clicking the “Add” button on the VPN Details Dialog. It is used to create a new VPN.

2.7.1.10.3 GUI size

Table 19 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Add VPN	1	1	N/A

2.7.1.10.4 GUI fields

The following table lists fields for the addVPN dialog.

Table 20 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Name	New			Contains the new VPN name	

2.7.1.10.5 Usage example

The following example shows the default dialog with no data yet entered.

2.7.1.10.6 GUI release history update
This is a new dialog.

2.7.1.10.7 Context sensitive launching information
This is launched using the CS2000 Management Tools interface

2.7.1.10.8 Supplementary information
NONE

2.7.1.11 GUI name: Details
NAT Details

2.7.1.11.1 Functional description
This GUI will replace existing dialogs to display the GWC ID and GW information for Zones.

A new details button will be added to the network zone panels and the Display ID and Retrieve GW buttons will be removed. On clicking the details button the details dialog will be presented.

This will contain a pull down containing up to two items. The dialog choices are to display the GWC NAT ID and the gateway report. These options will only be available if the user selected a specific Network Zone. The original dialogs have been changed to panels and included in this dialog.

2.7.1.11.2 GUI usage and implications
This GUI is used to display Zone information, including GWC IDs and Gateways using the Zones.

2.7.1.11.3 GUI size
Table 21 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
NATDetails	1	1	N/A

2.7.1.11.4 GUI fields
The following table lists fields for the Details dialog.

Table 22 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Detail selection	New			Chooses NAT information.	

2.7.1.11.5 Usage example

The following example shows the default dialog.

2.7.1.11.6 GUI release history update

This is a new dialog.

2.7.1.11.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.11.8 Supplementary information

NONE

2.7.1.12 GUI name: Details - VPN

VPN Details Dialog

2.7.1.12.1 Functional description

The dialog panel will show a table containing all VPNs and the NATs which make them up. An add and delete button will also be included to allow the user to manage the VPNs.

2.7.1.12.2 GUI usage and implications

This gui is selected by pressing the “VPN” button on the NAT or composite NAT/LBL tabbed panels.

2.7.1.12.3 GUI size

Table 23 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
VPN Details	1	1	N/A

2.7.1.12.4 GUI fields

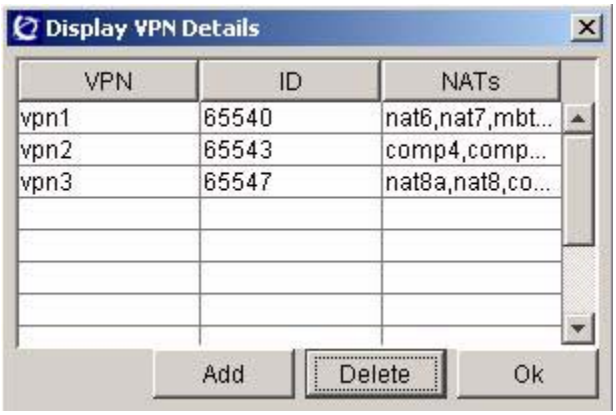
The following table lists fields for the VPN dialog.

Table 24 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
VPN Table	New			Displays VPN information.	

2.7.1.12.5 Usage example

The following example shows VPNs and the NATs that they consist of.



2.7.1.12.6 GUI release history update

This is a new panel.

2.7.1.12.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.12.8 Supplementary information

NONE

2.7.1.13 GUI name: Details GWC ID

GWC ID panel part of the details dialog

2.7.1.13.1 Functional description

This panel displays the NAT ID in the GWC.

Please note this is existing functionality which has been included in the details dialog.

2.7.1.13.2 GUI usage and implications

This gui displays the NAT ID which is GWC uses.

2.7.1.13.3 GUI size

Table 25 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWCID	1	1	N/A

2.7.1.13.4 GUI fields

Table 26 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

2.7.1.13.5 Usage example

The following example shows the ID of the selected Zone.

2.7.1.13.6 GUI release history update

This is a new panel that contains existing information.

2.7.1.13.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.13.8 Supplementary information

NONE

2.7.1.14 GUI name: Details Gateway Report

Gateway report panel part of the Zone details dialog.

2.7.1.14.1 Functional description

This panel contains the gateway report table that was previously in its own dialog.

2.7.1.14.2 GUI usage and implications

This gui is obtained from the NAT details dialog.

2.7.1.14.3 GUI size

Table 27 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWReport	1	1	N/A

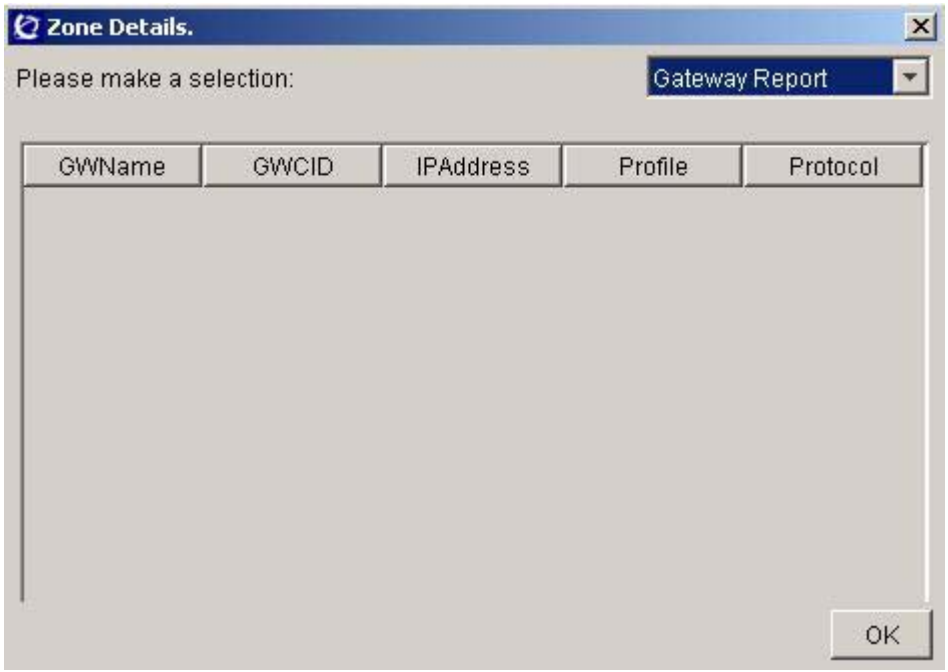
2.7.1.14.4 GUI fields

Table 28 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry

2.7.1.14.5 Usage example

The following example shows the panel embedded in the details dialog.



2.7.1.14.6 GUI release history update

This is an existing GUI that's been moved to the details dialog box.

2.7.1.14.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.14.8 Supplementary information
NONE

2.7.1.15 GUI name: GWC Media Proxies Tab
Gateway controller media proxy tab.

2.7.1.15.1 Functional description
This panel contains the list of media proxies that are provisioned on a GWC. New group information has been added.

2.7.1.15.2 GUI usage and implications
This gui is obtained from the GWC provisioning panel.

2.7.1.15.3 GUI size

Table 29 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GWCMPPanel	1	1	N/A

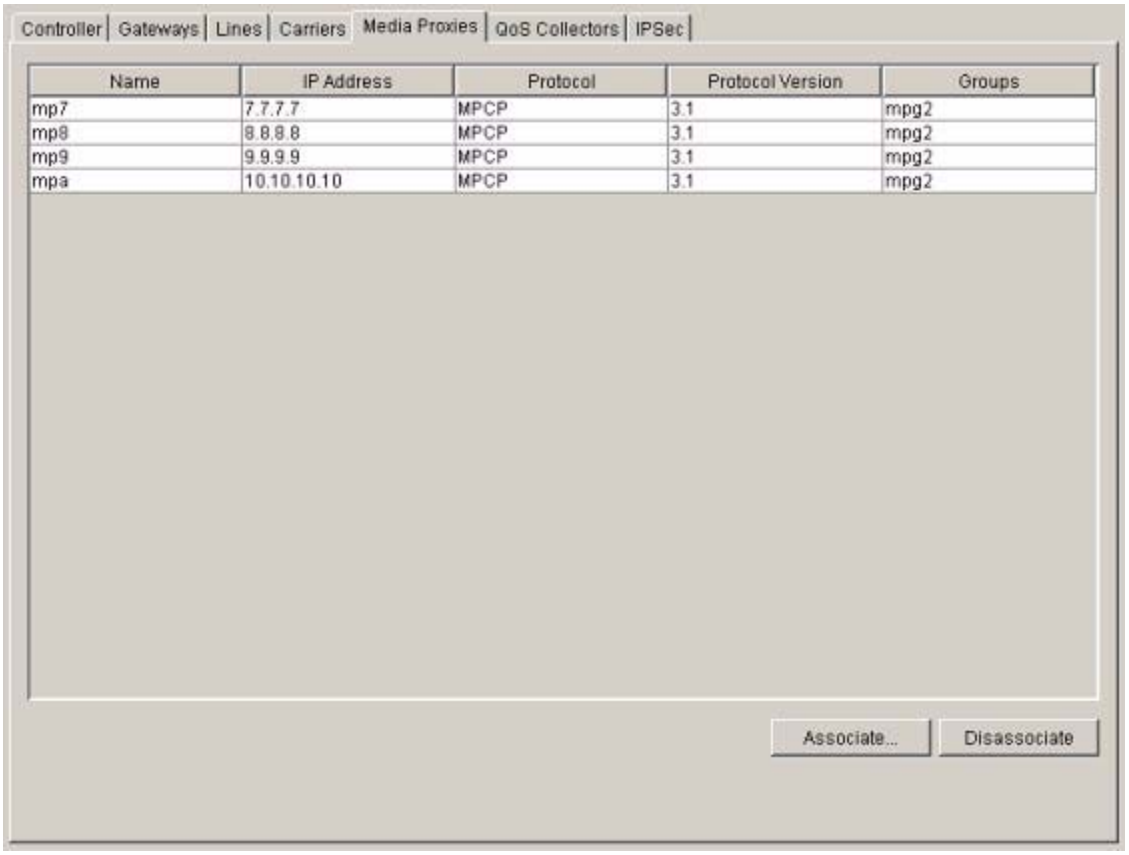
2.7.1.15.4 GUI fields

Table 30 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
MP Groups	New			Shows whether the media proxy is part of a group.	

2.7.1.15.5 Usage example

The following example shows the added groups column to the media proxy panel.



2.7.1.15.6 GUI release history update

This is an existing GUI that has been extended.

2.7.1.15.7 Context sensitive launching information

This is launched using the CS2000 Management Tools interface

2.7.1.15.8 Supplementary information

NONE

2.7.2 CLUI Interface

None

2.8 User interface changes

None

2.9 OSSGate Interface Changes

2.9.1 XML Command Changes

The following new interfaces introduced in SN09 to manage Media Proxy Groups:

- Add Media Proxy Group - Add a new Media Proxy Group and the Media Proxys associated with that group.
- Query Media Proxy Group. - There are three types of query:
  - — List all the Media Proxys within a Media Proxy Group.
  - — List all Media Proxy Groups assigned against a Gateway Controller.
  - — List all the Media Proxy Groups that a Media Proxy belongs to.
- Change Media Proxy Group - Modify the list of Media Proxys assigned to a group.
- Delete Media Proxy Group - Delete a Media Proxy group.

The following new interfaces introduced in SN09 to manage VPNs.

- Add VPN - Add a new VPN with the specified name.
- Delete VPN - Delete a VPN from the list of VPNs.

The following interfaces will be modified in SN09 to make use of Media Proxy groups:

- Add Network Zone - When a Network zone is created, allow it to be optionally associated with a Media Proxy Group and/or a VPN. This requires changes to Add NAT and add LBL.
- Add NAT - When a Nat middlebox is created, allow it to be optionally associated with a Media Proxy Group and/or a VPN.
- Add LBL - When a LBL middlebox is created, allow it to be optionally associated with a Media Proxy Group.
- Query Network Zone - Extend the query to return the Media Proxy Group and VPN.
- Query Nat - Extend the query to return the Media Proxy Group and VPN.
- Query LBL - Extend the query to return the Media Proxy Group.
- Change Network Zone - Change the Media Proxy Group and/or VPN assigned to a middlebox.
- Change NAT - Change the Media Proxy Group and/or VPN assigned to a Middlebox.
- Change LBL - Change the Media Proxy Group assigned to a Middlebox.

2.9.1.1 Add MP Group XML command

Add Media Proxy Group is a new command in SN09. The command defines a new group and adds between one and five Media Proxies to that group.

The XML for this command is shown in Figure 1, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 1 XML command to Add Media Proxy Group

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addMPGroup usn="1" version="1.0">
      <Parameters>
       <MPGroupName>aGroup</MPGroupName>
       <MPname>mp1</MPname>
       <MPname>mp11</MPname>
       <MPname>mp111</MPname>
       <MPname>mp1111</MPname>
       <MPname>mp11111</MPname>
     </Parameters>
     </addMPGroup>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.2 Response XML

Example:

```
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addMPGroup usn="1" version="1.0"><ReturnData><ReturnCode value="0"
text="Successful result" /></ReturnData></AddMPGroup> </Methods>
  </Response>
</CommandList>
```

2.9.1.3 Query MP Group XML command

Query Media Proxy Group is a new command in SN09. Three versions of the command provide queries to return the following information:

- The list of Media Proxies contained in a Media Proxy Group
- List all Media Proxy Groups
- The list of Media Proxy Groups a Media Proxy belongs to
- The list of Media Proxy Groups associated with a Gateway Controller

The three versions of XML for this command are shown in Figure 2, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 2 XML command to Query MP Group

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryMPGroup usn="1" version="1.0">
      <Parameters>
       <MPGroupName>aGroup</MPGroupName>
      </Parameters>
     </queryMPGroup>
    </Methods>
  </Command>
 </CommandList>
## get all MPG entries
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryMPGroup usn="1" version="1.0">
      <Parameters>
      </Parameters>
     </queryMPGroup>
    </Methods>
  </Command>
 </CommandList>
## get MPGs that MP belongs to
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryMPGroup usn="1" version="1.0">
      <Parameters>
       <MPname>mp1</MPname>
      </Parameters>
     </queryMPGroup>
    </Methods>
  </Command>
 </CommandList>
## get MPGs that are on a GWC
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryMPGroup usn="1" version="1.0">
      <Parameters>
       <GWCname>GWC-1</GWCname>
      </Parameters>
     </queryMPGroup>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.4 Response XML

Two types of response are provided, the detailed single MPG response, and the multiple MPG name response. The single response is only provided when a single MPG is request.

```
## single MPG response
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryMPGroup usn="1" version="1.0"><ReturnData><MPGGroupName>MPG-
ABC</MPGGroupName><MPname>MP-
ABC</MPname><MPname></MPname><MPname></MPname><MPname></MPname><MPname></MPnam
e><ReturnCode value="0" text="Successful result" /></ReturnData></queryMPGroup>    </Methods>
  </Response>
</CommandList>

## multiple MPG response
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryMPGroup usn="1" version="1.0"><ReturnData><MPGGroupName>MPG-
ABC</MPGGroupName><ReturnCode value="0" text="Successful result" /></ReturnData></queryMPGroup>
</Methods>
  </Response>
</CommandList>
```

2.9.1.5 Change MP Group XML command

Change Media Proxy Group is a new command in SN09. The command redefines the list of Media Proxies contained within a Media Proxy Group. The new list will replace the previous list.

The XML for this command is shown in Figure 3, the schema is defined in Appendix B and error messages returned are described in Appendix C.Appendix D provides a description of each tag.

Figure 3 XML Command to Change MP Group

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeMPGroup usn="1" version="1.0">
      <Parameters>
       <MPGroupName>aGroup</MPGroupName>
       <MPname>mp1</MPname>
       <MPname>mp2</MPname>
      </Parameters>
     </changeMPGroup>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.6 Response XML

```
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<changeMPGroup usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></ChangeMPGroup>     </Methods>
  </Response>
</CommandList>
```

2.9.1.7 Delete MP Group XML command

Delete Media Proxy Group is a new command in SN09. The command deletes the definition of a Media Proxy Group.

The XML for this command is shown in Figure 4, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 4 XML Command to Delete MP Group

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <deleteMPGroup usn="1" version="1.0">
      <Parameters>
       <MPGroupName>aGroup</MPGroupName>
      </Parameters>
     </deleteMPGroup>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.8 Response XML

```
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<deleteMPGroup usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></deleteMPGroup>     </Methods>
  </Response>
</CommandList>
```

2.9.1.9 Add VPN XML command

Add VPN is a new command in SN09. The command adds the definition of a new VPN.

The XML for this command is shown in Figure 5, the schema is defined in Appendix B and error messages returned are described in Appendix C.Appendix D provides a description of each tag.

Figure 5 XML Command to Add VPN

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addVPN usn="1" version="1.0">
     <Parameters>
        <vpnName>VPN11</vpnName>
      </Parameters>
     </addVPN>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.10 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addVPN usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful result"
/></ReturnData></addVPN>     </Methods>
  </Response>
</CommandList>
```

2.9.1.11 Delete VPN XML command

Delete VPN is a new command in SN09. The command deletes the definition of a VPN.

The XML for this command is shown in Figure 6, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 6 XML Command to Delete VPN

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <deleteVPN usn="1" version="1.0">
     <Parameters>
         <vpnName>VPN11</vpnName>
      </Parameters>
     </deleteVPN>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.12 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<deleteVPN usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></deleteVPN>     </Methods>
  </Response>
</CommandList>
```

2.9.1.13 Add Network Zone XML command

The existing Add Network Zone command is extended in SN09. The additional tag <preferredMPGroup> allows a Media Proxy Group to be optionally associated with a Network Zone when a Network Zone is created. The additional tag <vpnName> allows a VPN to be optionally be associated with a Network Zone providing its type is NAT or Composite Nat.

The XML for this command is shown in Figure 7, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 7 XML Command to Add a Network Zone

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addNetworkZone usn="1" version="1.0">
     <Parameters>
         <Name>NZ1</Name>
         <Service>NAT</Service>
        <PreferredMPGroup>MPG1</PreferredMPGroup>
      </Parameters>
     </addNetworkZone>
    </Methods>
  </Command>
</CommandList>
```

2.9.1.14 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addNetworkZone usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></addNetworkZone>     </Methods>
  </Response>
</CommandList>
```

2.9.1.15 Add NAT XML command

The existing Add NAT command is extended in SN09. The additional tag <preferredMPGroup> allows a Media Proxy Group to be optionally associated with a NAT when a NAT is created. The additional tag <vpnName> allows a VPN to be optionally be associated with a NAT.

The XML for this command is shown in Figure 8, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 8 XML Command to Add a NAT middlebox

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <addNAT usn="1" version="1.0">
     <Parameters>
        <NATname>MkI</NATname>
             <PreferredMPGroup>MPG1</PreferredMPGroup>
      </Parameters>
     </addNAT>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.16 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addNAT usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful result"
/></ReturnData></addNAT>     </Methods>
  </Response>
</CommandList>
```

2.9.1.17 Add LBL XML command

The existing Add LBL command is extended in SN09. The additional tag <preferredMPGroup> allows a Media Proxy Group to be optionally associated with a LBL middlebox when a LBL middlebox is created.

The XML for this command is shown in Figure 9, the schema is defined in Appendix B and error messages returned are described in Appendix C. Appendix D provides a description of each tag.

Figure 9 XML Command to Add a LBL middlebox

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
 <Command>
  <Interface>ITransIf</Interface>
   <Methods>
    <addLBL usn="1" version="1.0">
    <Parameters>
       <LBLname>LBL1</LBLname>
            <RUDescription>SPC_Default_RU</RUDescription>
            <MaxCount>10</MaxCount>
            <PreferredMPGroup>MPG1</PreferredMPGroup>
     </Parameters>
    </addLBL>
   </Methods>
 </Command>
</CommandList>
```

2.9.1.18 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<addLBL usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful result"
/></ReturnData></addLBL>     </Methods>
  </Response>
</CommandList>
```

2.9.1.19 Query Network Zone XML command

The existing Query Network Zone command is extended in SN09. When either individual or multiple network Zones are queried the response is extended to include the Media Proxy Group and VPN, if any, the Network Zone has.

- List all Network Zoness
- The details of a single network Zone.
- The list of Network Zones having a specified Media Proxy Group.

The optional tag <preferredMPGroup> is used to allow the query to be based on a specified Media Proxy Group.

The XML for this command is shown in Figure 10, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 10 XML Command to Query Network Zone

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryNetworkZone usn="1" version="1.0">
     <Parameters>
      </Parameters>
     </queryNetworkZone>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.20 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
     <Interface>ITransIf</Interface>
     <Methods>
<queryNetworkZone usn="1" version="1.0"><ReturnData>
<NetworkZone>
       <ID>10</ID>
       <Name>COMP1</Name>
       <ParentID>0</ParentID>
</NetworkZone>
<NetworkZone>
       <ID>11</ID>
       <Name>NZ1</Name>
       <ParentID>0</ParentID>
</NetworkZone><ReturnCode value="0" text="Successful result"
/></ReturnData></queryNetworkZone>    </Methods>
  </Response>
</CommandList>
```

2.9.1.21 Query NAT XML command

The existing Query NAT command is extended in SN09. When either individual or multiple NAT middleboxes are queried the response is extended to include the Media Proxy Group and VPN, if any, that each NAT has.

- List all NATs
- The details of a single NAT.
- The list of NATs having a specified Media Proxy Group.

The optional tag <preferredMPGroup> is used to allow the query to be based on a specified Media Proxy Group.

The XML for this command is shown in Figure 11, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 11 XML Command to Query NAT Middlebox

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
 <Command>
  <Interface>ITransIf</Interface>
   <Methods>
    <queryNAT usn="1" version="1.0">
    <Parameters>
       <NATname>Nat1</NATname>
     </Parameters>
    </queryNAT>
   </Methods>
 </Command>
</CommandList>
```

2.9.1.22 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryNAT                                                                    usn="1"
version="1.0"><ReturnData><NATname>sssssss</NATname><NATType>1</NATType><Parent
MB></ParentMB><PreferredMPGroup>LONDON</PreferredMPGroup><VPNname>UK<VPNn
ame>  <ReturnCode  value="0"  text="Successful  result"  /></ReturnData></queryNAT>
</Methods>
  </Response>
</CommandList>
```

2.9.1.23 Query LBL XML command

The existing Query LBL command is extended in SN09. When either individual or multiple LBL middleboxes are queried the response is extended to include the Media Proxy Group, if any, each LBL has. There are three types of query for this element:

- List all LBLs
- The details of a single LBL.
- The list of LBLs having a specified Media Proxy Group.

The optional tag <PreferredMPGroup> enables this extended query.

The XML for this command is shown in Figure 12, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 12 XML Command to Query LBL Middlebox

```
Query single LBL:
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryLBL usn="1" version="1.0">
     <Parameters>
        <LBLname>LBL1</LBLname>
      </Parameters>
     </queryLBL>
    </Methods>
  </Command>
 </CommandList>

 Query All LBLs:
  <?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryLBL usn="1" version="1.0">
     <Parameters>
      </Parameters>
     </queryLBL>
    </Methods>
  </Command>
 </CommandList>

  MPG based query:
 <?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <queryLBL usn="1" version="1.0">
     <Parameters>
       <PreferredMPGroup>MPG1</PreferredMPGroup>
      </Parameters>
     </queryLBL>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.24 Response XML

```
single response:
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryLBL usn="1" version="1.0"><ReturnData><LBLname>LBL1</LBLname><CounterGWC>0</
CounterGWC><RUDescription>SPC_Default_RU</RUDescription><MaxCount>10</
MaxCount><ParentMB></ParentMB><PreferredMPGroup>MPG2</PreferredMPGroup><ReturnCode value="0"
text="Successful result" /></ReturnData></queryLBL> </Methods>
  </Response>
</CommandList>

multiple response:
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryLBL usn="1" version="1.0"><ReturnData><LBLname>LBL1</LBLname><LBLname>LBL2</
LBLname><ReturnCode value="0" text="Successful result" /></ReturnData></queryLBL> </Methods>
  </Response>
</CommandList>

response for MPG query:
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<queryLBL usn="1" version="1.0"><ReturnData><LBLname>LBL2</LBLname><ReturnCode value="0"
text="Successful result" /></ReturnData></queryLBL> </Methods>
  </Response>
</CommandList>
```

2.9.1.25 Change Network Zone XML command

The existing Change Network Zone command is extended in SN09. When the MediaProxyGroup of the network Zone is to be changed the optional tag <preferredMPGroup> is used to specify the new Media Proxy Group. The optional tag <vpnName> is used to specify the VPN name.

The XML for this command is shown in Figure 13, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 13 XML Command to Change Network Zone

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeNetworkZone usn="1" version="1.0">
     <Parameters>
        <Name>NZ1</Name>
        <PreferredMPGroup>MPG2</PreferredMPGroup>
      </Parameters>
     </changeNetworkZone>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.26 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
     <Interface>ITransIf</Interface>
     <Methods>
<changeNetworkZone usn="1" version="1.0"><ReturnData><ReturnCode value="0"
text="Successful result" /></ReturnData></changeNetworkZone> </Methods>
  </Response>
</CommandList>
```

2.9.1.27 Change NAT XML command

The existing Change NAT command is extended in SN09. When the MediaProxyGroup or VPN associated with the NAT is to be changed the optional tag <preferredMPGroup> is used to specify the new Media Proxy Group. The optional tag <vpnName> is used to specify the new VPN name.

The XML for this command is shown in Figure 14, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 14 XML Command to Change NAT

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeNAT usn="1" version="1.0">
     <Parameters>
        <NATname>MkI</NATname>
             <PreferredMPGroup>MPG2</PreferredMPGroup>
      </Parameters>
     </changeNAT>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.28 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<changeNAT usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></changeNAT>    </Methods>
  </Response>
</CommandList>
```

2.9.1.29 Change LBL XML command

The existing Change LBL command is extended in SN09. When the MediaProxyGroup associated with the LBL is to be changed the optional tag <preferredMPGroup> is used to specify the new Media Proxy Group.

The XML for this command is shown in Figure 15, the schema is defined in Appendix B and error messages returned are described in Appendix C.

Figure 15 XML Command to Change LBL

```
<?xml version="1.0" encoding="UTF-8" ?>
 <CommandList>
  <Command>
   <Interface>ITransIf</Interface>
    <Methods>
     <changeLBL usn="1" version="1.0">
     <Parameters>
        <LBLname>LBL1</LBLname>
                <PreferredMPGroup>MPG2</PreferredMPGroup>
      </Parameters>
     </changeLBL>
    </Methods>
  </Command>
 </CommandList>
```

2.9.1.30 Response XML

```
<?xml version='1.0'?>
<CommandList>
  <Response>
    <Interface>ITransIf</Interface>
    <Methods>
<changeLBL usn="1" version="1.0"><ReturnData><ReturnCode value="0" text="Successful
result" /></ReturnData></changeLBL>     </Methods>
  </Response>
</CommandList>
```

2.9.2 Additional OSSGate Changes

The Network Zone xml interface is common to both the CS2KMT and the SPC. Any changes added made to the network Zone xml must be implemented for the SPC as well as the CS2KMT. As this feature has introduced changes to the network Zone xml files shared by the SPC, the expectation is that there will be a feature on the SPC to absorb the impact of these changes.

2.10 Configuration Walkthrough

2.10.1 Creating a Media Proxy Group

A MPG is allocated as follows using the CS2000 Management tools GUI:

1) In the main network devices Panel, select the Media Proxies Tab.

2) In the “Media Proxies” Tab select the “Media Proxy Groups” Tab.

3) Click on the “Add” button to display the “Add Media Proxy Group” dialog.

4) Enter the name of the Media Proxy Group in the field at the top of the dialog

5) Select in turn up to 5 media proxies to add to the group by highlighting each and pressing the “add>>” button. If a MP is added in error it can be removed using the “<<rem” button.

6) If the creation fails, a message window will be displayed and the media proxy group will not be added.

2.10.2 Changing a Media Proxy Group

A MPG is modified as follows using the CS2000 Management tools GUI:

1) In the main network devices Panel, select the Media Proxies Tab.

2) In the “Media Proxies” Tab select the “Media Proxy Groups” Tab.

3) Select (highlight) the Media Proxy Group to be changed.

4) Click on the “Change” button to display the “Change Media Proxy Group” dialog.

5) Select any media proxies to be removed from the group by highlighting each and pressing the “<<rem” button. If a MP needs to be added it can be added using the “add>>” button.

6) If the change fails, a message box will be displayed and the change will not take effect.

A Media Proxy Group may not be modified in this way if it is associated with a Network Zone that is associated with a Gateway on a Gateway Controller. If such a Media Proxy Group must be changed, the Media Proxy Group must first be disassociated from the Gateway Controller. This can be achieved by changing the Group on the Network Zone, then changing the Media Proxy Group, before changing the network zone to have the group again.

WARNING: If the Media Proxy Group on the network Zone is changed or removed, this will affect the media proxies that are available for call processing for the duration of the change.

2.10.3 Deleting a Media Proxy Group

A MPG is deleted as follows using the CS2000 Management tools GUI:

1) In the main network devices Panel, select the Media Proxies Tab.

2) In the “Media Proxies” Tab select the “Media Proxy Groups” Tab.

3) Select the Media Proxy Group to be deleted.

4) Click on the “Delete” button at the bottom of the panel to delete the selected media Proxy Group.

5) if the deletion fails, a message box will be displayed.

A Media Proxy Group cannot be deleted if it is associated with a Network Zone.

2.10.4 Assigning a media Proxy Group

When a Network Zone is created using the CS2000 Management Tools Gui, a Media Proxy Group can be assigned to it as follows:

1) From the relevant Network Zone tab (NAT, LBL or composite) click the “Add..” button.

2) Using the “Media Proxy Group” drop down box, select a preferred media proxy group from the list of groups available.

3) proceed with the rest of the provisioning of the network Zone as normal.

4) If the creation fails, the details will be displayed in a message pane. The Network Zone will not be added.

When the Network Zone has been created, it can be used by a gateway as follows:

5) When provisioning a Media Gateway on a GWC, select an ITrans capable profile for the Media Gateway.

6) The Network Zone having the Media Proxy Group should be set as the adjacent middlebox for the media gateway. If the Network Zone is part of a chain of middleboxes then, in order for the gateway to use its Media Proxy Group, the network Zones closer to the media gateway in the chain must not have a preferred Group.

2.10.5 Changing the associated Media Proxy Group

To change the media proxy group associated with a Network Zone the following steps must be followed:

1) In the appropriate Network Zones tab, highlight the Network Zone that you wish to change.

2) Hit the “change” button to display the “Change Network Zone” Dialog

3) Select the new Media proxy Group from the drop down list box that appears on the Change Network Zone dialog and click on ok to action the change.

5) If the change fails, details will be displayed in a message pane. The change will not take effect.

WARNING: Changing a Media Proxy Group on a Network Zone that is provisioned on a gateway controller may affect call processing. Media Proxies may be made unavailable for the duration of the change.

2.10.6 Assigning a shared VPN when creating a Network Zone

When a Network Zone is created using the CS2000 Management Tools Gui, a VPN can be assigned to it as follows:

1) From the relevant Network Zone tab (NAT, LBL or composite) click the “Add..” button.

2) If available Click the “use VPN” check (tick) box.

3) From the drop down list which is made visible, select a VPN name. Or click the “create VPN” button to create a new one.

4) A specific VPN ID may be selected. This is used when a VPN spans multiple Call Servers.

5) Proceed with the rest of the provisioning of the network Zone as normal.

6) If the creation fails, the details will be displayed in a message pane. The Network Zone will not be added.

2.11 Appendix A for A00007217: Authorisation groups

The table below shows the Authorisation groups and permissions given for the new methods and operations that are being introduced for this feature. The access rights are aligned with those of the existing Itrans functionality (Media Proxies and Network Zones). Existing authorisation groups remain unchanged by this feature.

Command	**User Group**				
	mgcadm	**mgcrw**	**mgcmtc**	**mgcsprov**	**mgcro**
addMPGroup	X	X			
changeMPGroup	X	X			
queryMPGroup	X	X	X	X	X
deleteMPGroup	X	X			
addVPN	X	X			
deleteVPN	X	X			
queryVPN	X	X	X	X	X

2.12 Appendix B for A00007217: XML validation schemas

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addMPGroup Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addMPGroupmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addMPGroupparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addMPGroupparamsType">
```

```
    <xsd:sequence>
      <xsd:element name="MPGroupName" type="NoSpaceNameType" />
      <xsd:element name="MPname" type="NoSpaceNameType" minOccurs="1" maxOccurs="5" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************************** -->
  <!-- * Define queryMPGroup Method Parameters -->
  <!-- ********************************************************************************************************** -->
  <xsd:complexType name="queryMPGroupmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="queryMPGroupparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryMPGroupparamsType">
   <xsd:choice minOccurs="0">
      <xsd:element name="MPGroupName" type="NoSpaceNameType" />
      <xsd:element name="MPname" type="NoSpaceNameType" />
      <xsd:element name="GWCname" type="GWCNameType"  />
   </xsd:choice>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************************** -->
  <!-- * Define changeMPGroup Method Parameters -->
  <!-- ********************************************************************************************************** -->
  <xsd:complexType name="changeMPGroupmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeMPGroupparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeMPGroupparamsType">
    <xsd:sequence>
      <xsd:element name="MPGroupName" type="NoSpaceNameType" />
      <xsd:element name="MPname" type="NoSpaceNameType" minOccurs="0" maxOccurs="5" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************************** -->
  <!-- * Define deleteMPGroup Method Parameters -->
```

```
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="deleteMPGroupmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="deleteMPGroupparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="deleteMPGroupparamsType">
    <xsd:all>
      <xsd:element name="MPGroupName" type="NoSpaceNameType" />
    </xsd:all>
  </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addVPN Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addVPNmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addVPNparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addVPNparamsType">
    <xsd:sequence>
      <xsd:element name="vpnName" type="NoSpaceNameType" />
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define deleteVPN Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="deleteVPNmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="deleteVPNparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="deleteVPNparamsType">
    <xsd:all>
      <xsd:element name="vpnName" type="NoSpaceNameType" />
    </xsd:all>
  </xsd:complexType>
</xsd:schema>
```

```
<xsd:schema version="1.0" xml:lang="en" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <!-- **** Warning! This module is cloned from SPC module addNZ.xsd       **** -->
        <!-- **** All changes to the master SPC module should be replicated here **** -->
    <xsd:include schemaLocation="SPCcommon.xsd"/>
    <!-- ******************************************** -->
    <!-- * Define Add Network Zone Method Parameters * -->
    <!-- ******************************************** -->
    <xsd:complexType name="addNetworkZoneMethodType">
        <xsd:all>
            <xsd:element name="Parameters" type="addNetworkZoneParamsType"/>
        </xsd:all>
        <xsd:attributeGroup ref="Usn_VersionAttrbGroup"/>
    </xsd:complexType>
    <xsd:complexType name="addNetworkZoneParamsType">
        <xsd:sequence>
            <xsd:element ref="ID" minOccurs="0"/>
            <!-- only for SESM, the ID is optional -->
            <xsd:element ref="Name"/>
            <xsd:element name="Service" type="NZServiceType" minOccurs="0"/>
            <xsd:element name="Parent" type="ParentType" minOccurs="0"/>
           <xsd:element name="IntraZoneBWInfo" type="BWInfoType" minOccurs="0"/>
            <xsd:element name="LogicalNetworkLink" type="AddLogicalLinkType" minOccurs="0"/>
   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
     <xsd:element name="VPNname" type="NoSpaceNameType" minOccurs="0"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addNAT Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addNATmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addNATparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addNATparamsType">
    <xsd:all>
      <xsd:element name="NATname" type="NoSpaceNameType" />
      <xsd:element name="NATid" type="MiddleBoxIndexType" minOccurs="0"/>
      <xsd:element name="ParentMB" type="NoSpaceNameType" minOccurs="0"/>

   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
      <xsd:element name="VPNname" type="NoSpaceNameType" minOccurs="0"/>
    </xsd:all>
  </xsd:complexType>
</xsd:schema>

<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
                version="1.0"
                xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define addLBL Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="addLBLmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="addLBLparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="addLBLparamsType">
    <xsd:all>
      <xsd:element name="LBLname" type="NoSpaceNameType" />
      <xsd:element name="CounterGWC" type="IPAddressType" minOccurs="0" />
      <xsd:element name="RUDescription" type="xsd:string" />
      <xsd:element name="MaxCount" type="RUMaxCountType" />
      <xsd:element name="ParentMB" type="NoSpaceNameType" minOccurs="0" />
      <xsd:element name="LBLid" type="MiddleBoxIndexType" minOccurs="0" />
   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
    </xsd:all>
  </xsd:complexType>
</xsd:schema>


<xsd:schema version="1.0" xml:lang="en" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <!-- **** Warning! This module is cloned from SPC module changeNZ.xsd    **** -->
        <!-- **** All changes to the master SPC module should be replicated here **** -->
    <xsd:include schemaLocation="SPCcommon.xsd"/>
    <!-- ****************************************** -->
    <!-- * Define Change Network Zone Method Parameters * -->
    <!-- ****************************************** -->
    <xsd:complexType name="changeNetworkZoneMethodType">
        <xsd:all>
            <xsd:element name="Parameters" type="changeNetworkZoneParamsType"/>
        </xsd:all>
        <xsd:attributeGroup ref="Usn_VersionAttrbGroup"/>
    </xsd:complexType>
    <xsd:complexType name="changeNetworkZoneParamsType">
        <xsd:sequence>
            <xsd:group ref="IDNameGroup"/>
            <xsd:sequence>
                <xsd:element name="Parent" type="ParentType" minOccurs="0"/>
        <xsd:element name="IntraZoneBWInfo" type="IntroZoneBWInfoType" minOccurs="0"/>
        <xsd:element name="LogicalNetworkLink" type="ChangeLogicalLinkType" minOccurs="0"/>
   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
      <xsd:element name="VPNname" type="NoSpaceNameType" minOccurs="0"/>
            </xsd:sequence>
        </xsd:sequence>
    </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                version="1.0"
```

```
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define changeNAT Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="changeNATmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeNATparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeNATparamsType">
    <xsd:all>
      <xsd:element name="NATname" type="NoSpaceNameType" />
      <xsd:element name="ParentMB" type="NoSpaceNameType" minOccurs="0"/>
<xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
      <xsd:element name="VPNname" type="NoSpaceNameType" minOccurs="0"/>
    </xsd:all>
  </xsd:complexType>
</xsd:schema>


<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define changeLBL Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="changeLBLmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="changeLBLparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="changeLBLparamsType">
    <xsd:all>
      <xsd:element name="LBLname" type="NoSpaceNameType" />
      <xsd:element name="CounterGWC" type="IPAddressType" minOccurs="0" />
      <xsd:element name="RUDescription" type="xsd:string" minOccurs="0" />
      <xsd:element name="MaxCount" type="RUMaxCountType" minOccurs="0" />
      <xsd:element name="ParentMB" type="NoSpaceNameType" minOccurs="0" />
   <xsd:element name="PreferredMPGroup" type="NoSpaceNameType" minOccurs="0"/>
    </xsd:all>
  </xsd:complexType>
</xsd:schema>


<xsd:schema version="1.0" xml:lang="en" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
        <!-- **** Warning! This module is cloned from SPC module queryNZ.xsd     **** -->
        <!-- **** All changes to the master SPC module should be replicated here **** -->
    <xsd:include schemaLocation="SPCcommon.xsd"/>
    <!-- ****************************************** -->
    <!-- * Define Query/QueryAll Network Zone Method Parameters * -->
    <!-- ****************************************** -->
    <xsd:complexType name="queryNetworkZoneMethodType">
```

```
        <xsd:all>
            <xsd:element name="Parameters" type="queryNetworkZoneParamsType" nillable="true"/>
        </xsd:all>
        <xsd:attributeGroup ref="Usn_VersionAttrbGroup"/>
    </xsd:complexType>
    <xsd:complexType name="queryNetworkZoneParamsType">
        <xsd:sequence>
            <xsd:choice minOccurs="0">
                <xsd:element ref="ID"/>
                <xsd:element ref="Name"/>
            </xsd:choice>
            <xsd:element name="IDMin" type="xsd:unsignedInt" minOccurs="0"/>
            <xsd:element name="IDMax" type="xsd:unsignedInt" minOccurs="0"/>
            <xsd:element name="MaxZones" type="xsd:unsignedInt" minOccurs="0"/>
                        <xsd:choice minOccurs="0">
        <xsd:element name="PreferredMPGroup" type="NoSpaceNameType"/>
                        </xsd:choice>
        </xsd:sequence>
    </xsd:complexType>
</xsd:schema>
```

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define queryNAT Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="queryNATmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="queryNATparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryNATparamsType">
    <xsd:sequence>
      <xsd:choice minOccurs="0">
        <xsd:element name="NATname" type="NoSpaceNameType" />
        <xsd:element name="GWCname" type="GWCNameType" />
      </xsd:choice>
      <xsd:choice minOccurs="0">
        <xsd:element name="ListNATid" type="NoSpaceNameType" />
      </xsd:choice>
      <xsd:choice minOccurs="0">
        <xsd:element name="PreferredMPGroup" type="NoSpaceNameType"/>
      </xsd:choice>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
```

```
                xml:lang="en" >

  <!-- ********************************************************************************************** -->
  <!-- * Define queryLBL Method Parameters -->
  <!-- ********************************************************************************************** -->
  <xsd:complexType name="queryLBLmethodType">
    <xsd:all>
      <xsd:element name="Parameters" type="queryLBLparamsType" />
    </xsd:all>
    <xsd:attributeGroup ref="Usn_VersionAttrbGroup" />
  </xsd:complexType>
  <xsd:complexType name="queryLBLparamsType">
    <xsd:all>
      <xsd:element name="LBLname" type="NoSpaceNameType" minOccurs="0" />
      <xsd:element name="GWCname" type="GWCNameType" minOccurs="0" />
    </xsd:all>
    <xsd:choice minOccurs="0">
        <xsd:element name="PreferredMPGroup" type="NoSpaceNameType"/>
    </xsd:choice>
  </xsd:complexType>
</xsd:schema>
```

2.13 Appendix C for A00007217: Error codes and messages

Table 31 Return codes when command is unsuccessful

Cause of error	Return code	Example return messages
Incorrect command version in query	301	Unsupported version
Platform applications internal error: OSS Interface applications cannot connect to required server application	302	Interfacing error

Error codes have not yet been assigned. This section will need completing. before the feature completes.

2.13.1 Example Error Message

```
<?xml version='1.0'?>
    <CommandList>
       <Response>
         <Interface>ITransIf</Interface>
           <Methods>
              <queryNAT usn="1.0" version="1.0">
               <ReturnData>
                  <NATname>nat1111</NATname>
                   <ReturnCode value= "305" text="NAT not found"/>
               </ReturnData>
              </queryNAT usn="1.0">
```

```
        </Methods>
    </Response>
</CommandList>
```

2.14 Appendix D for A00007217: XML Commands: description of method parameters

2.14.1 Parameter definitions (new in SN09)

- **MPGroupName** - The unique name of the Media Proxy Group. TYPE *NoSpaceNameType*.
- **itransMPGroupName** - The same MPGroupName as defined above. This tag is used in the non-Itrans operations to give the context of Internet Transparency. TYPE *NoSpaceNameType*.
- **preferredMPGroup** - The id of the media Proxy Group.
- **vpnName** - The unique name of the VPN. TYPE *NoSpaceNameType*.

2.14.2 Method Parameters

Method parameters are defined below. Input data is mandatory except where indicated otherwise.

1. **addMPGroup** - Method to create a new Media Proxy Group. This method has the following parameters:

- Input data:
  - usn
  - version
  - MPGroupName. The unique name of the Media Proxy Group.
  - MPname. A list of between one and five Media Proxies which belong to the group that is being created.
- Output data:
  - usn (value should be the same as the input)
  - version (value should be the same as the input)
  - ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

2. **queryMPGroup** - A set of methods to query Media Proxy Groups. This method has the following parameters, one of the three optional parameters must be supplied:

- Input data:

– usn

– version

– MPGroupName (optional). Query to return the list of Media Proxies in a the group.

– MPname (optional). Query to list the Media Proxy Groups the Media Proxy belongs to.

– GWCName (optional). Query to list the Media Proxy Groups assigned against the Gateway controller.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– MPname (returned when the MPGroupName option is used)

– MPGroupName (returned when either the MPname or GWCName options are used)

– ReturnCode - indicates via an integer value if the command has been successful or, if not, the error type and includes a brief textual message with further information.

3. **changeMPGroup** - Method to change the list of Media Proxies assigned to a Media Proxy Group. This method has the following parameters:

• Input data:

– usn

– version

– MPGroupName. The unique name of the Media Proxy Group which must already exist.

– MPname. A list of between one and five Media Proxies which are now to be assigned to that group.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

4. **deleteMPGroup** - Method that deletes a Media Proxy Group. This method has the following parameters:

• Input data:

– usn

– version

– MPGroupName. The name of the existing Media Proxy Group that is to be deleted.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

5. **addVpn** - Method to Add a new VPN identifier. This method has the following parameters:

• Input data:

– usn

– version

– vpnName. The name of the VPN which is being created.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

6. **deleteVpn** - Method to delete an existing VPN identifier. This method has the following parameters:

• Input data:

– usn

– version

– vpnName. The name of the VPN which is being deleted.

• Output data:

– usn (value should be the same as the input)

– version (value should be the same as the input)

– ReturnCode

Product = CS 2000

A00007269--NGSS Backup and Restore

Functional Description

1: Applicable Solution(s)

PT-IP

1.1 Synopsis

This activity enhances the backup functionality provided by the NGSS Session Server for SN09. These enhancements include creating a new directory to store the backed up files, backup additional files not previously backed up, and provide a mechanism for the customer to change the backup time. It also documents a restore procedure for the various backed up components.

1.2 Background Information

1.2.1 NGSS Pre-SN09 Backup Capability

In SN07 and SN08 the NGSS Session Server performs a daily backup of the Solid database files into the following directory on each NGSS unit:

```
/opt/apps/database/solid/backup
```

The database backup is performed by an automatic timed command at 1 AM daily. The backup time can not be configured. A single copy of the database backup is stored on the NGSS.

1.2.2 NGSS SN09 Backup Capability

For SN09, this activity backs up the Solid database, certificates, commish, and web files on the NGSS Session Server.

All backed up files are placed in a TAR file on the following directory:

```
/data/bkresmgr/backup
```

The backup mechanism is controlled by a cron job running on the NGSS. The backup time can be configured by the customer. The backup cron job is set to run at 1 AM as a default setting.

Customers need to ensure that NGSS backup times are synchronized with the times set for IEMS backups.

It is strongly recommended that customers transfer the backups to an external server or location daily to protect against system or office outages.

NOTE: In SN09, both units will be backed up. As some files are different between them, customers are recommended to store the backups taken from both units.

1.3 Description

1.3.1 NGSS Back up Directory

Backup files are stored locally on the NGSS. A new directory is created to store the backed up files. A directory is created for this purpose is:

`/data/bkresmgr/backup`[3]

All backed up files are placed in a TAR file in the backup directory. The name of the backup file is in the following format:

`<hostname>.backupfile.date_time.tgz`

For example:

`vm0.backupfile.2005-03-14_09-47.tgz`

1.3.2 NGSS Backed up Files

The following files are backed up on the NGSS for SN09:

- Solid Database files
  - /opt/apps/database/solid/backup/solid.db
  - /opt/apps/database/solid/backup/solid.ini
  - /opt/apps/database/solid/backup/solmsg.out
- certificate files
  - /opt/base/share/ssl/gen_cert.txt
  - /opt/base/share/ssl/server.crt
  - /opt/base/share/ssl/trusted.crt
- commish files[4]
  - etc/hosts[5]
  - etc/ntp.conf
  - etc/sysconfig/network-scripts/ifcfg-eth0[6]
  - etc/sysconfig/netnodes
  - etc/group

3. This backup directory naming convention was introduced by the A00006979 Synchronized Backup and Restore activity for Succession products.
4. Note: files in the etc/ directory are identical to those in the /persist directory. They can be backed up from either directory.
5. This is unit specific data.
6. This is unit specific data.

— etc/passwd

— etc/shadow

— /opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key.pub

— /opt/base/synch_local/common/etc/ssh/ssh_host_key.pub

— /opt/base/synch_local/common/etc/ssh/ssh_rsa_key.pub

- web files

  — /opt/apps/webint/jakarta-tomcat-4.1.30/conf/server.xml

  — /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/jsp/redirect.jsp

  — /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/jsp/redirect_SSPFS.jsp

  — /opt/apps/webint/jakarta-tomcat-4.1.30/webapps/prov/jsp/redirect_no-SSPFS.jsp

  — /usr/local/apache/htdocs/redirect_apps.php

All backed up files are placed in a tar file on the following directory:

```
/data/bkresmgr/backup
```

1.3.3 Restoring NGSS Backed up Files

In general the backed up files simply need to be returned to their original directories as documented above “NGSS Backed up Files” on page 927. The files should be applied to their respective directories after the commish and SIPGW installation steps have been completed and prior to unsuspending the SIPGW application.

Perform these initial steps to start the restore process.

1. Log into NGSS as root.
2. Transfer backup TGZ file to /data/bkresmgr/restore
3. If image is stored locally, copy it from /data/bkresmgr/backup

   ```
   cp /data/bkresmgr/data/backupfile.tgz
   /data/bkresmgr/restore
   ```

4. If image is stored externally, use NFS, SFTP, SCP, or read it from a CD/DVD/tape drive.
5. Go to restore dir

   ```
   cd /data/bkresmgr/restore
   ```

6. Un-compress the backup image into the current dir.

   ```
   tar -xzvf backupfile.tgz
   ```

The following sections provide a detailed procedure on how to restore files for each component that was backed up. Determine which components need to be restored. Follow the restore steps for that component if they are relevant to what needs to be restored. For instance, if the keys do not need to be restored, skip that step.

1.3.1.1 Restoring database from a backup copy

The following procedure is used to restore the database from the backup copy. The database is restored to its state when the backup was made. In general this procedure should only be followed when database corruption has occurred on both units of the NGSS. The database must be restored on the **active unit** of the NGSS.

1. Jam the Active Unit.
2. Suspend Call Processing
3. Copy over the database files[7]

```
cp -i solid.db
/opt/apps/database/solid/backup/solid.db

cp -i solid.ini
/opt/apps/database/solid/backup/solid.ini

cp -i solmsg.out
/opt/apps/database/solid/backup/solmsg.out
```

4. Set permissions on the files accordingly

```
chmod 700
/opt/apps/database/solid/backup/solid.db

chmod 700
/opt/apps/database/solid/backup/solid.ini

chmod 700
/opt/apps/database/solid/backup/solmsg.out
```

5. Run the restorebackup script as shown from the following directory:

```
cd /opt/apps/database/solid_install/

./restorebackup.sh
```

6. Unsuspend Call Processing
7. UnJam the Active Unit

Jamming the active unit is necessary to prevent the database from switching activity while its being restored. The database must be restored on the active unit. No action is needed to restore the database on the inactive unit. The

7. For each copy the system asks for confirmation. Please ensure the copy is correct before typing yes.

database on the inactive unit is automatically updated by the active unit. Call processing should be suspended since the database will not be available.

1.3.1.1 Restoring certificate

Stop the services which use the certificates and copy over the existing ones.

1. Restore **all** files

```
cp -i gen_cert.txt /opt/base/share/ssl/
cp -i server.crt /opt/base/share/ssl/
cp -i trusted.crt /opt/base/share/ssl/
cp -i server.xml /opt/apps/webint/jakarta-tomcat-4.1.30/conf/
```

2. Set the permissions on the files accordingly

```
chmod 644 /opt/base/share/ssl/server.crt
chmod 644 /opt/base/share/ssl/gen_cert.txt
chmod 644 /opt/base/share/ssl/trusted.crt
```

3. suspend the application
4. /opt/apps/webint/tomcatd stop
5. /usr/local/apache/bin/apachect1 stop
6. /usr/local/apache/bin/apachect1 start
7. /opt/apps/webint/tomcatd start
8. unsuspend the application

1.3.1.1 Restoring system data

Copy over and set permissions on the files that need to be restored.

1. Copy over the following files as needed

```
cp -i hosts /etc/
cp -i passwd /etc/
cp -i group /etc/
cp -i ntp.conf /etc/
cp -i shadow /etc/
cp -i ifcfg-eth0 /etc/sysconfig/network-scripts/
cp -i netnodes /etc/sysconfig
cp -i ssh_host_dsa_key.pub /opt/base/synch_local/common/etc/ssh/
```

```
cp -i ssh_host_key.pub
/opt/base/synch_local/common/etc/ssh/

cp -i ssh_rsa_key.pub
/opt/base/synch_local/common/etc/ssh/
```

2. Set the permissions on the restored files accordingly

```
chmod 755 /etc/hosts

chmod 755 /etc/passwd

chmod 755 /etc/shadow

chmod 755 /etc/group

chmod 755 /etc/sysconfig/netnodes

chmod 755 /etc/sysconfig/network-scripts/ifcfg-
eth0

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_key
.pub

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_host_dsa
_key.pub

chmod 644
/opt/base/synch_local/common/etc/ssh/ssh_rsa_key.
pub
```

1.3.1.1 Restoring web files

1. Copy over the following files

```
cp -i redirect*.jsp /opt/apps/webint/jakarta-
tomcat-4.1.30/webapps/prov/jsp/

cp -i redirect_apps.php /usr/local/apache/htdocs/
```

Note: If additional web files need be restored then do a reinstall.

1.3.4 Configuring the backup time on the NGSS

The backup utility is run as a cron job. Cron is the name of a program that enables users to execute commands or scripts at specific times and dates. It is recommended that the backup utility be run daily on the NGSS during off peak hours. As a default setting the backup utility on the NGSS is scheduled to run at 1 AM daily.

Changing the scheduled time of the NGSS backup involves changing the cron programs configuration file: *crontab*. An entry in the crontab file is made

up of a series of fields with each separated by a space. An example crontab entry follows:

0 1 * * * /opt/apps/database/solid_install/bkup_solprov.sh

A list of the fields follows:

minute hour day month weekday user cmd

minute: the minute of the hour the command will run on, range 0 to 59.

hour: thehour of the day the command will run on as specified on a 24 hour clock, range 0 to 23, where 0 is midnight.

day: the day of the month the command will run, e.g. to run a command on the 19th of each month, the day would be 19.

month: the month of the year the command will run on, range 0 to 12.

weekday: the day of the week the command will run, range 0 to 7.

cmd: the command/program to run.

To run a program daily set the minute and hour fields and place a * in the remaining fields (day, month, and weekday). In the previous example the bkup_solprov.sh program gets run at 1 AM daily.

Notes: Place a * in any unused fields. More than one value may be put into a field by separating the values with commas.

1.4 Hardware Requirements or Dependencies

N/A.

1.5 Software Requirements or Dependencies

N/A.

1.6 Limitations and restrictions

For security reasons *.key and *.keystore files are not backed up by this feature:

/opt/base/share/ssl/certificate.keystore
/opt/base/share/ssl/server.key
/opt/base/synch_local/common/etc/ssh/ssh_host_dsa_key
/opt/base/synch_local/common/etc/ssh/ssh_host_key
/opt/base/synch_local/common/etc/ssh/ssh_rsa_key

1.7 Interactions

N/A.

1.8 Glossary

Term	Description
CLI	Command Line Interface
CRONTAB	Cron Table
DB	Database
NGSS	Next Generation Session Server

1.9 References

A00006979 *Synchronized Backup and Restore Manager*
A00009266 *Siren[8] HLD Backup and Restore Framework*

8. The NGSS may transition to the Siren platform at some future release.

Product = CS 2000

A00007544--NCAS Link and SIP NMS Support based on RFC 3842

Functional Description

1: Applicable Solution(s)

PT-IP, CHS, Int'l PT-IP

1.1 Description

This development includes following two separate but interdependent design:

- Non-Call Associated Signaling (NCAS) link development.
- Session Initiation Protocol (SIP) based network message waiting service (NMS) support based on RFC 3842.

1.1.1 NCAS Link Development

The NCAS Link provides a light weight switching control point (SCP) like functionality. The NCAS link provides a non-call associated link between the Communication Server 2000 (CS2K) Session Server (SS) (formerly known as Next Gen Session Server (NGSS)) and the CS2K Core (Brisc/88K, XA-Core and Compact/3PC). The NCAS link is used by the SIP NMS support based on RFC 3842.

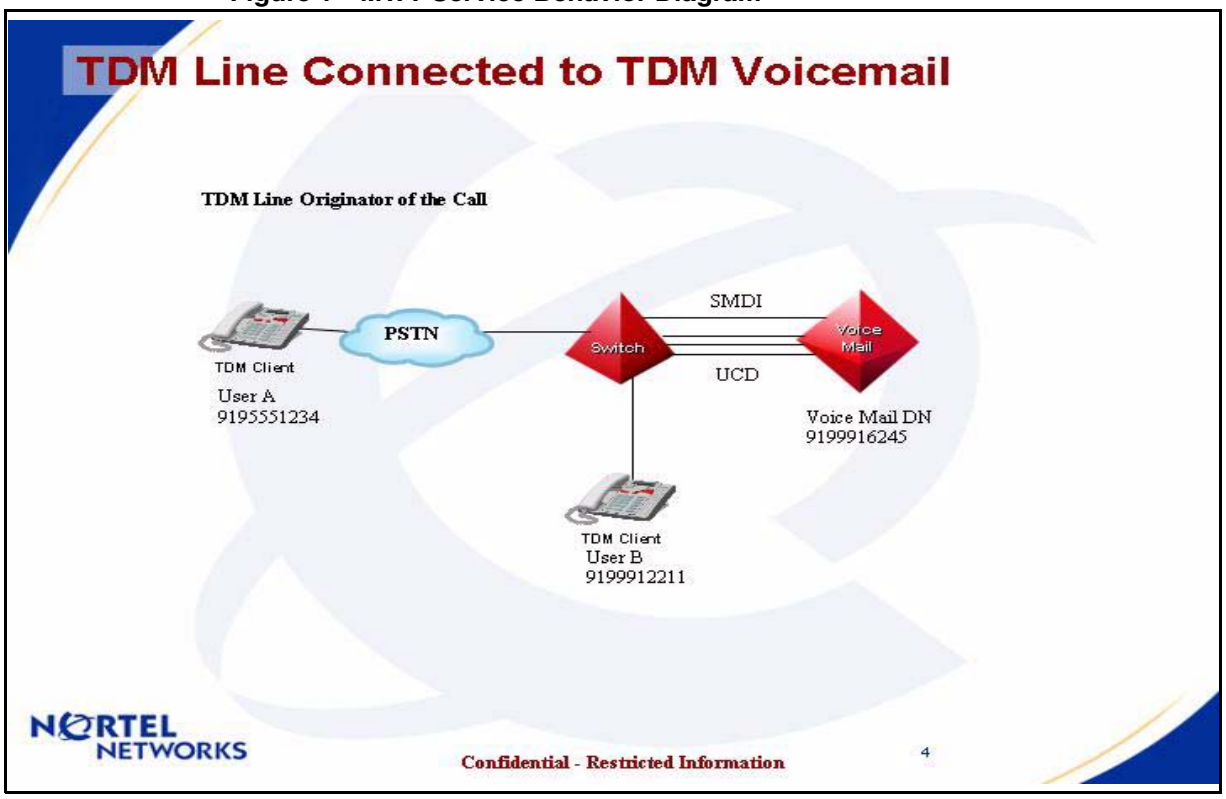
In the CS2K Core, NCAS link development is done under activity A00004500 in SN07. However, this development did not consider some internal drawback associated with Intelligent Network Access Point (INAP) signalling. Therefore, under this activity, the INAP drawback has been removed.

1.1.2 SIP NMS Support based on RFC 3842

The Message Waiting (MWT) service is a CS2K Core based service. The complete MWT service, includes Voicemail system (VM) to record voice messages and retrieve voice messages, communication link between CS2K Core and VM, the MWT service control in the CS2K Core, end user devices to provide MWT Indication (MWI) and CS2K Core based Redirection Services, such as Call Forward Do not Answer (CFD/CFDA) etc.

The following figure provides a pictorial view of how MWT service is provided to an end user and how an end user uses the service in traditional switching environment.

Figure 1 MWT Service Behavior Diagram



The following steps describe the functionality shown in Figure 1 above:

1. User A (In PSTN network) is calling User B (On serving End Office (EO))
2. User B does not answer (User B's CFDA is set to go to DN of VM). Call Forwarding happens and Call terminates to DN of VM.
3. VM answers the call and prompts user A for message. Message is recorded by User A. User A exits and call clears.
4. VM sends a turn on notification to EO for providing MWT functionality to User B.
5. EO sends appropriate message to User B's device to turn on the MWT Indication (MWI).
6. User B finds MWI, initiates call request for retrieval (CRR) functionality. The call terminates to DN of VM.
7. VM answers the call and prompts User B for User ID and Password for authentication. User B enters appropriate details. The VM play the message from User A to User B. User B can continue to interact with VM.
8. VM sends a turn off notification to EO for providing MWT functionality to User B.
9. EO sends appropriate message to User B's device to turn off the MWI.

The above functionality provides support for the traditional MWT service along with a traditional Voice Mail system. Increasingly, number of customers are deploying the VM connection with the CS2K Core or equivalent class 5 switches in a network mode. In this case, the customers have to maintain only one VM for mutiple customers servred via different class 5 switches (including CS2K). The existing software in CS2K Core already provide this service using NMS based on GR-866_core using SS7 network.

Due to advancement of Unified Messaging (UM) which combines all type of mail messages (e.g. Voice Message, E-mail, Paging etc.) and Voice over Internet Protocol (VoIP), an increasing emphasis to provide same functionality using SIP based on RFC 3842.

The MWT functionality to CS2K Core based SIP lines is developed under SIP lines development plan (Please refer to actid A0000 - for CS2K Core design, actid A0000 - for CS2K GWC design and actid A0000 - for CS2K SS design). The communication between CS2K SS and SIP Line is based on the RFC 3842.

Deployment of the SS7 network is expensive proposition in the VoIP network. While SIP based on RFC 3842 can provide similar network capability using SIP messages between two CS2K or a CS2K and SIP compliant remote node (e.g. MCS). This feature develop necessary software in CS2K SS to support RFC 3842 based message waiting SIP messages and expands existing NMS software in CS2K Core to use the SIP network to provide network message waiting service to/from remote CS2K or SIP compliant remote node.

This feature does not cover development needed in SIP clients, SIP compliant remote node and SIP compliant VM.

Based on the converged network needs and support for multiple interfaces following end user devices are supported:

- Traditional Phones (e.g POTS, RES, IBN, KSET etc.)
- CICM IP sets
- Traditional Lines off of a remote switch
- Traditional Lines off of a remote SIP domain
- Traditional Lines off of a PBX
- SIP lines served by MCP 5100/5200.

Also, following interfaces to a message server (Voicemail) system are supported:

- Traditional SMDI and UCD/HUNT group to VM.
- Traditional VM using public SS7 network for NMS.
- Traditional VM using SIP NMS based on RFC 3842.
- SIP NMS based on RFC 3842 for MCP 5100/5200 platform.

The combination of above user devices and VM interfaces are supported with following interoperatibility limitations.

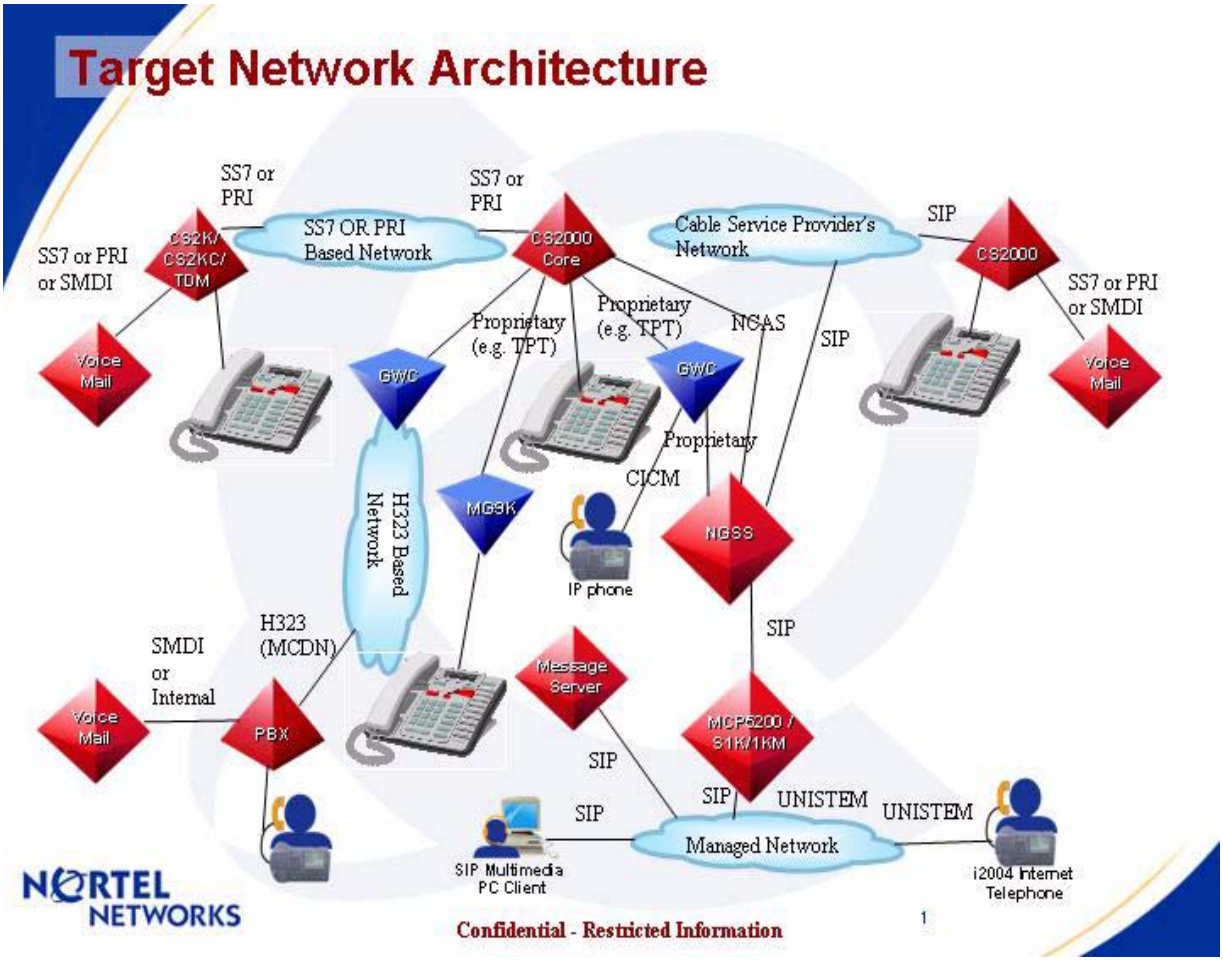
The design is generic and based on RFC 3842 standards, we are unable to test every possible interoperatibility using different handware and different vendor equipments. Therefore, we can only be able to claim the support for the tested networks. In order to make other hardware and different vendor equipment supported, proper interoperatibility testing must be done in Nortel approved interoperatibility lab. After the complete testing, appropriate support will be provided for them.

For Cable network support we need a design lab with appropriate Media Terminal Adaptors (MTAs). For design testing, no such lab identified yet. Without this testing, we can not claim the compatibility with cable specification for this feature.

1.1.3 Target Network Architecture

The feature develops a converge network architecture. In this architecture of the Message Waiting the VM or Message Server (MsgSrv) can resides any network and the user device can resides in any network. The communication required for MWT service is supported by this architecture. The following figure is pictorial representation of the target architecture.

Figure 2 Target Architecture



With this development, MWT is provided across the different type of networks within Service Provider's network. The following are the advantages to the service provider:

- Support of MWI on user's choice of device
- Consolidation of the VM system in service provider's network
- Converged network support
- MWI to SIP clients or S1K/1KM

Other topologies and how MWT service provided are described in "Supported Configurations" on page 940.

1.1.4 Supported Configurations

The connection and communication bases the supported configurations are separated in two catagories. 1) Configurations of Voicemail or MsgSrv systems and 2) Configurations of Lines or clients.

The configurations described here are specific to MWT service and VM communications for MWT service. These configurations assumes that the call related communications and signalling are provoided prior to the MWT service and exists in the given configuration.

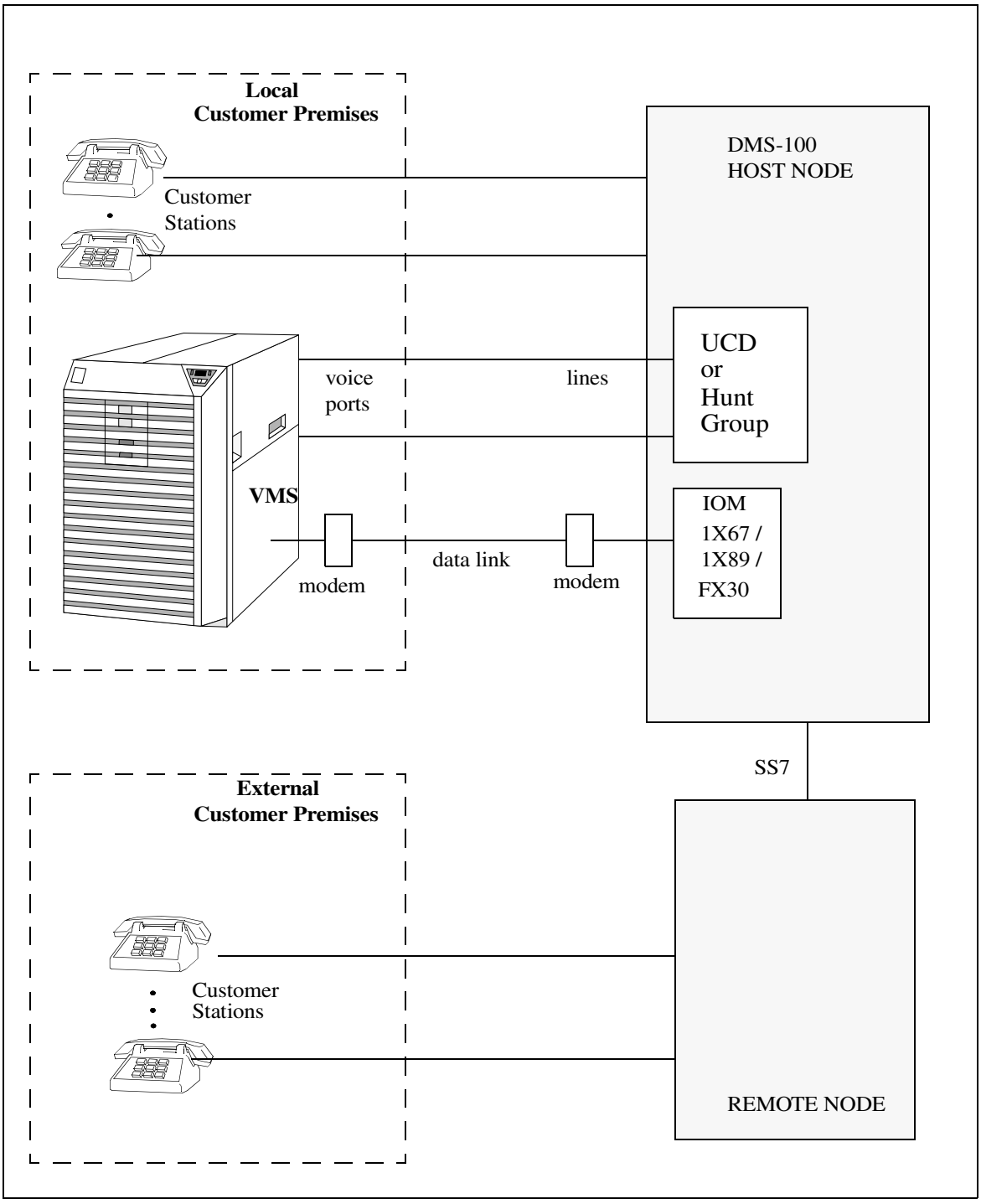
1.1.4.1 Configurations of Voicemail or MsgSrv Systems

The following configurations are separated by the protocol used for communication between CS2K and VM system:

1.1.4.1.1 Traditional VM communication using UCD/HUNT group and SMDI link

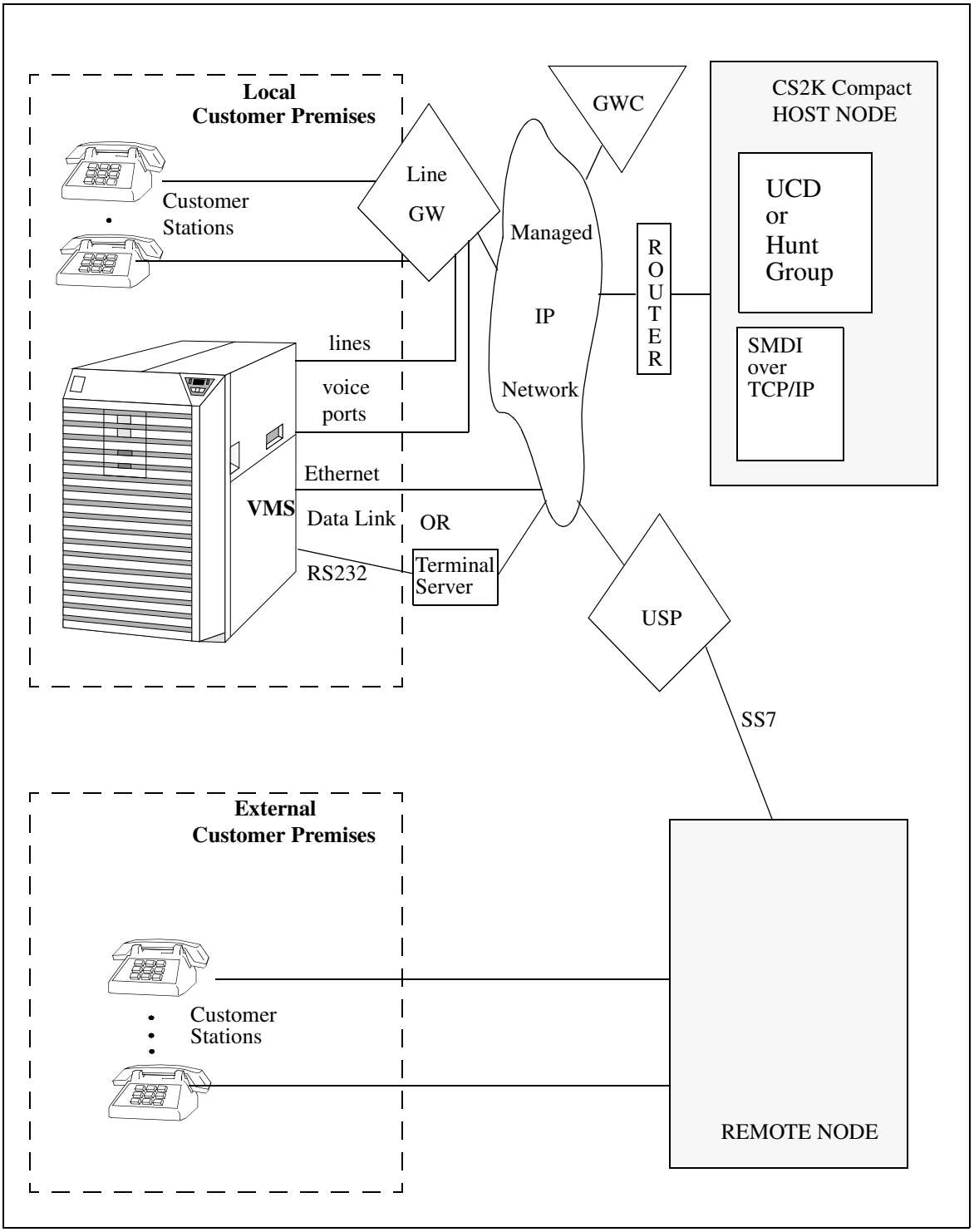
This is an existing and supported configuration in CS2K/DMS. For details on this configuration, please look in the NTP 297-2051-104- SMDI Setup and Operation. The following figure is a generic view of this configuration in DMS:

Figure 3 Simple VM Configuration in DMS



The data link in above Figure 3 is based on SMDI specifications described in the GR-283-Core. The following figure provides simple VM configuration in the CS2K Compact:

Figure 4 Simple VM Configuration is CS2K Compact



In Figure 4 , the communication between the CS2K Compact and VM is SMDI based on GR-283-Core. However, the transport medium is TCP/IP. The

details of this configuration can also be found in the NTP 297-2051-104 - SMDI Setup and Operation.

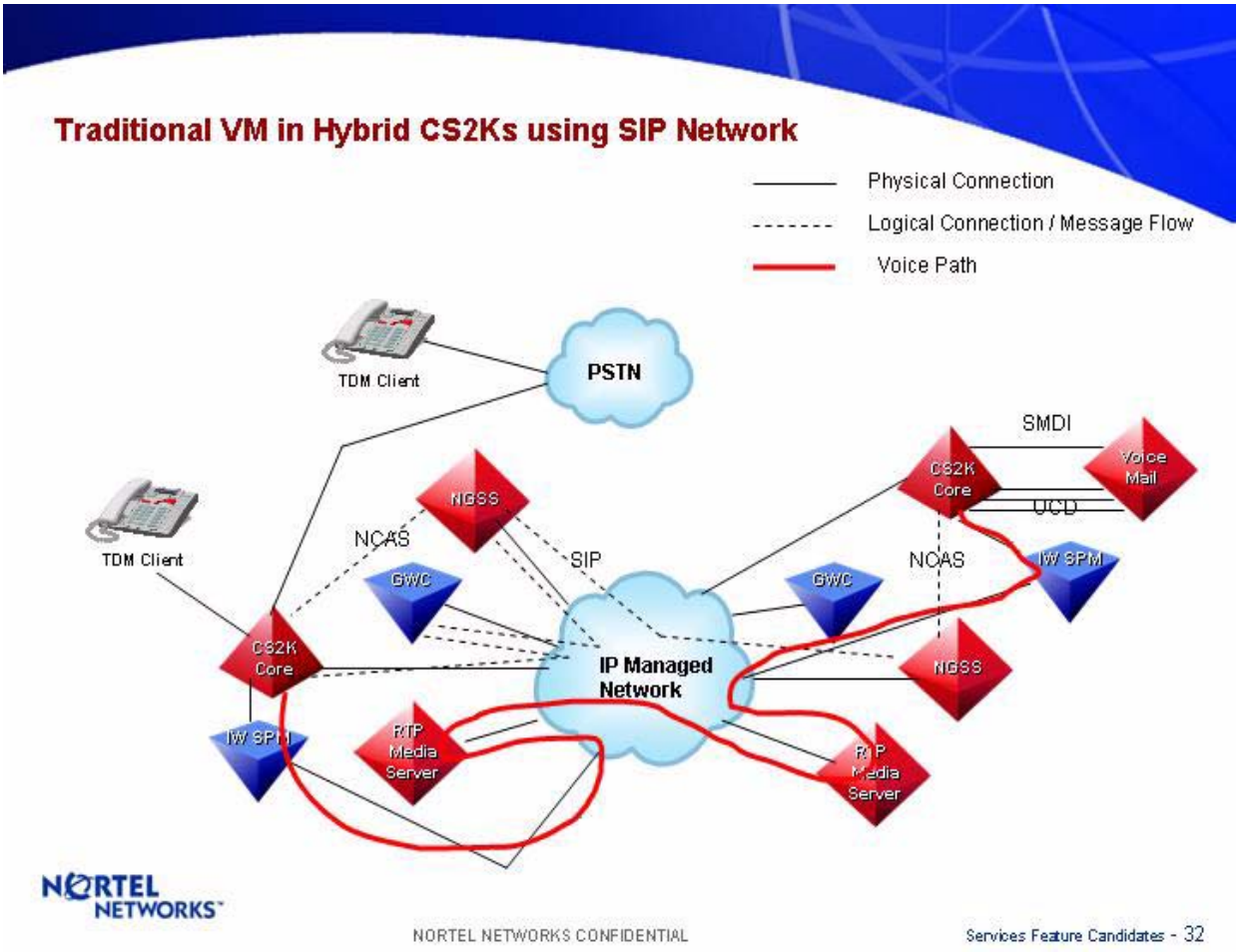
1.1.4.1.2 Network VM communication using SS7 network

Figure 3 and Figure 4 also describe the configuration of the VM communication using SS7 network between host node and remore node. For details, please see NTP 297-2051-104 - SMDI Setup and Operation; and NTP 297-8021-350v13 - North American Translation Guide Volume 13 of 25.

1.1.4.1.3 Traditional VM communication using SIP network

This configuration, the VM is a traditional VM connected to one CS2K via SMDI and UCD/HUNT group. The line is on another CS2K. The RFC 3842 based SIP messages are used between two CS2K to pass MWI information for NMS.

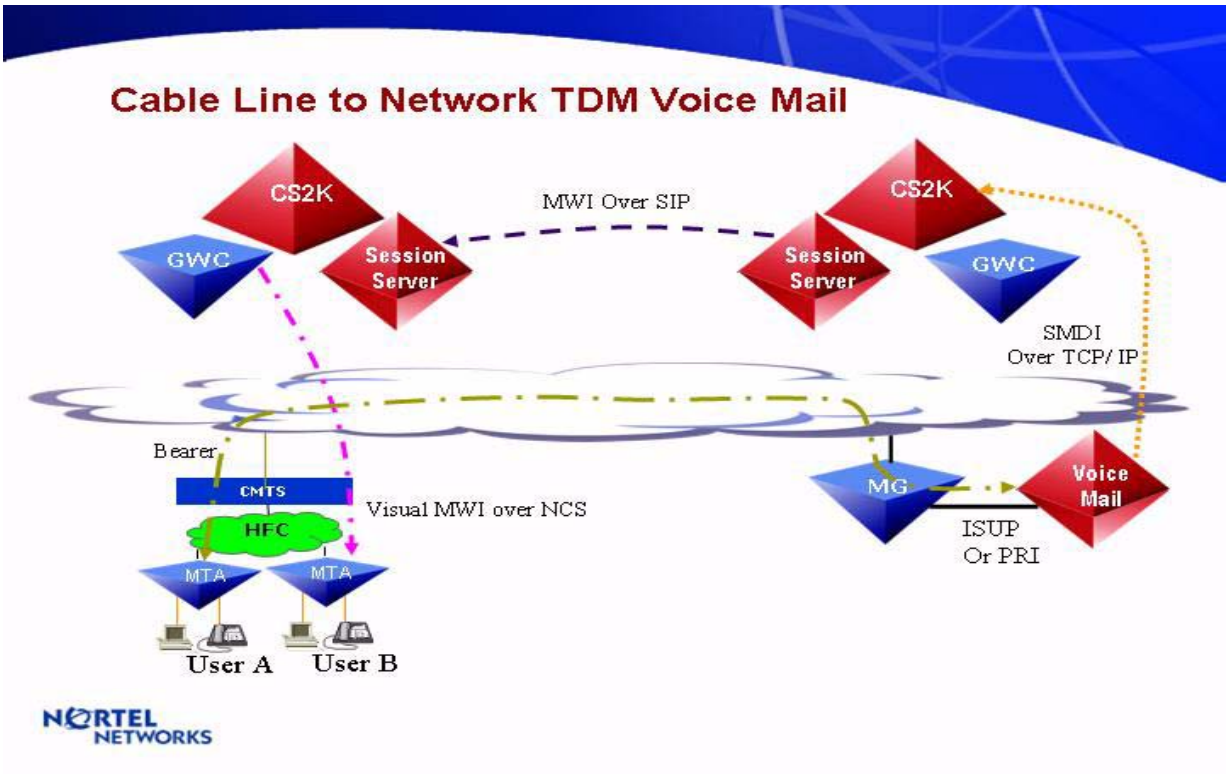
Figure 5 Traditional VM communication using SIP network



1.1.4.1.4 Network VM communication using SIP for Cable Service Providers

In cable service provider network, the VM is connected to a CS2K compact as described in previous section. However, the communication between two CS2K Compact is based on the managed IP network using SIP signalling.

Figure 6 VM in Cable Network

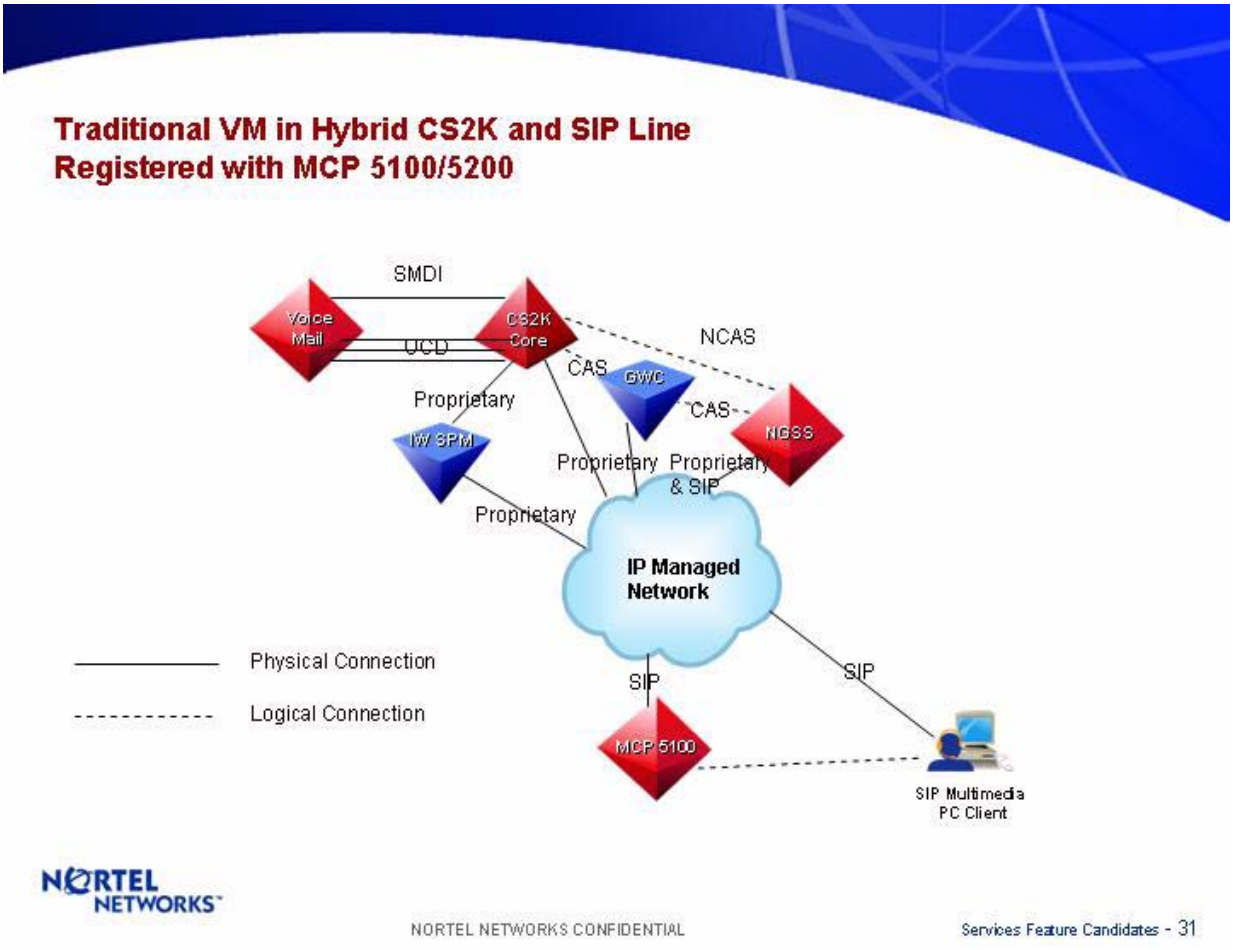


Note: The complete interoperatibility and compliance depends on the availability of the design lab. This configuration is quite similar to configuration describe by Figure 5 in previous section. The only major difference is the usage of MTA and conformance testing for cablelab specifications.

1.1.4.1.5 VM support for MCP 5100/5200 Platform using SIP network

This configuration, the VM is a traditional VM connected to one CS2K via SMDI and UCD/HUNT group. The SIP line is registered with the MCP 5100/5200 platform and SIP line is served by the traditional VM. The CS2K is sending RFC 3842 defined SIP messages to MCP 5100/5200 platform to provide network based MWI service.

Figure 7 VM support for MCP 5100/5200 using SIP network



1.1.4.2 Configurations of Lines or clients

The details of these configurations (datafill and setup) are described in the CN section of the feature. The following configurations are separated by the protocol used for communication between CS2K and line/client:

1.1.4.2.1 Lines connected via LCM/XPM

The phone line which is connected via LCM/XPM using PSTN network to the host node are supported today. In case of the SIP VM, these type of lines are considered as non-SIP lines and appropriate additional configuration is required in the Session Server.

1.1.4.2.2 Lines connected via Gateways

The phone lines which are connected via a MG9000 behave the same as traditional line connected to the CS2K via LCM/XPM. There is no change anticipated in this configuration. The CICM lines which are connected via an IP gateway behave the same. There is no imapct to thier setup and operation. In case of the SIP VM, these type of lines are considered as non-SIP lines and appropriate additional configuration is required in the Session Server.

1.1.4.2.3 Lines connected to a remote node

The lines connected to a remote node (e.g. PBX, another switch, MCP etc.) are considered as networked lines. For these lines network message waiting (NMS) service is provided. The CS2K does not store any data associated with these remote lines.

1.1.4.2.4 Media Terminal Adaptor

The media terminal adaptor is used in the cable network to provide media (voice) services. From the CS2K perspective, the media terminal adaptor is same as a line in the CS2K supported via gateways and gateway controller. The MWT service is provided to the Media Terminal Adaptor same way as it is provided to lines connected via gateways.

> Note: The complete interoperatibility and compliance depends on the availability of the design lab. The availability of MTA will allow us to perform this cable network requirement. However, it will not be tested, if no lab or MTA available. If we assume that the MTA cable line is another line in the CS2K and behave same way as any other line with MWT service assignment, than this design will support the MTA.

1.1.4.2.5 Single Physical Line with Multiple VM Access

Current design of MWT service in the CS2K does not restrict a single physical line to have access to multiple VM systems. With this design, there is no change to such support. The support is provided using the datafill of the Call Forwarding on the single physical line. The following example explains how this works:

Line B is a KSET line with two different DN keys and has MWT service assigned to it.

The first key's DN is datafilled with call forwarding busy (CFB) and call forwarding do not answer (CFD) and call forwarding number to DN of VM 1.

The second key's DN is datafilled with call forwarding busy (CFB) and call forwarding do not answer (CFD) and call forwarding number to DN of VM 2.

Now let's say first call to DN Key 1 encounters busy condition and forwards to the VM 1. The VM 1 records the message and send a message to CS2K to turn MWT light on for the DN Key 1. The MWT light is now lit for the first message from VM 1.

During the first call, a second call come to the DN key 2 and encounters no answer condition and forwards to the VM 2. The VM 2 records the message and send a message to CS2K to turn MWT light on for the DN Key 2. The request is now enqueued for the VM 2.

When user of Line B retrives the message from the VM 1, the MWT light will remain lit for the second message.

Please note that the MWT request from each VM will be treated as two separate requests in the MWT service.

1.1.4.2.6 Multiple Lines with Single VM Access

The multiple lines in a given CS2K are supported by a single VM. In this case the VM has each line provisioned as individual user. This is already supported functionality. This functionality is not changed by this feature.

If VM is capable to provide multiple MWT messages for multiple lines in a single mail box than it is also suppored because for each line CS2K receive a MWT message.

1.1.4.2.7 Multiple Lines with Multiple VM Access

This configuration is also supported in current design. The following example describes how this is supported.

Line A is a RES line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 1. The VM 1 is on a remote node.

Line B is an IBN line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 2. The VM 2 is on host node.

Line C is a SIP Line with MWT service and datafilled with CFB and CFD forwarding to DN of VM 3. The VM 3 is a SIP VM. The Line C is not registered.

Originator A calls Line A and Line A is busy. The call forwards to VM 1 on remote node. The VM 1 records the message from Originator A. The remote node sends a MWT message to the host node. The request of network MWT is now queued to Line A from VM 1.

Originator B calls Line B and Line B is busy. The call forwards to VM 2. The VM 2 records the message from Originator B. TheVM 2 sends a MWT message to the host node. The request of local MWT is now queued to Line B from VM 2.

Originator C calls SIP Line C and SIP Line C is not registered. The call forwards to VM 3. The VM 3 records the message from Originator C. TheVM 3 sends a MWT message to the host node. The request of network MWT is now queued to Line C from VM 3. The MWT notification is not sent to the Line C because it is not register. When the user of Line C sends a subscribe message for MWT after registration, the CS2K sends the current status of the MWT service in the CS2K to the line C.

1.1.5 Sample Message Details for SIP

The message details are based on the SIP Line configuration described above.

Step 1: The SIP Line SUBSCRIBE for MWT service.

Figure 8 SIP Line Register with CS2K - SUBSCRIBE Message

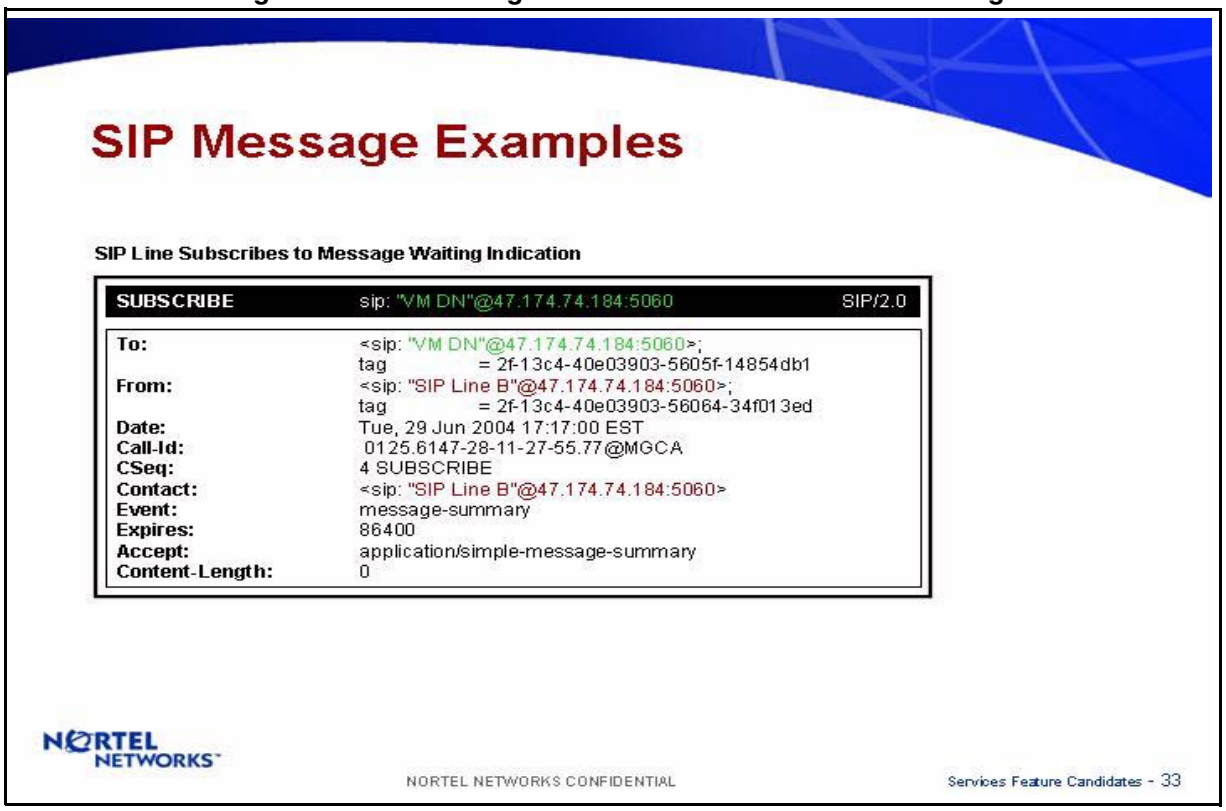


Figure 9 SIP Line Register with CS2K - OK Response

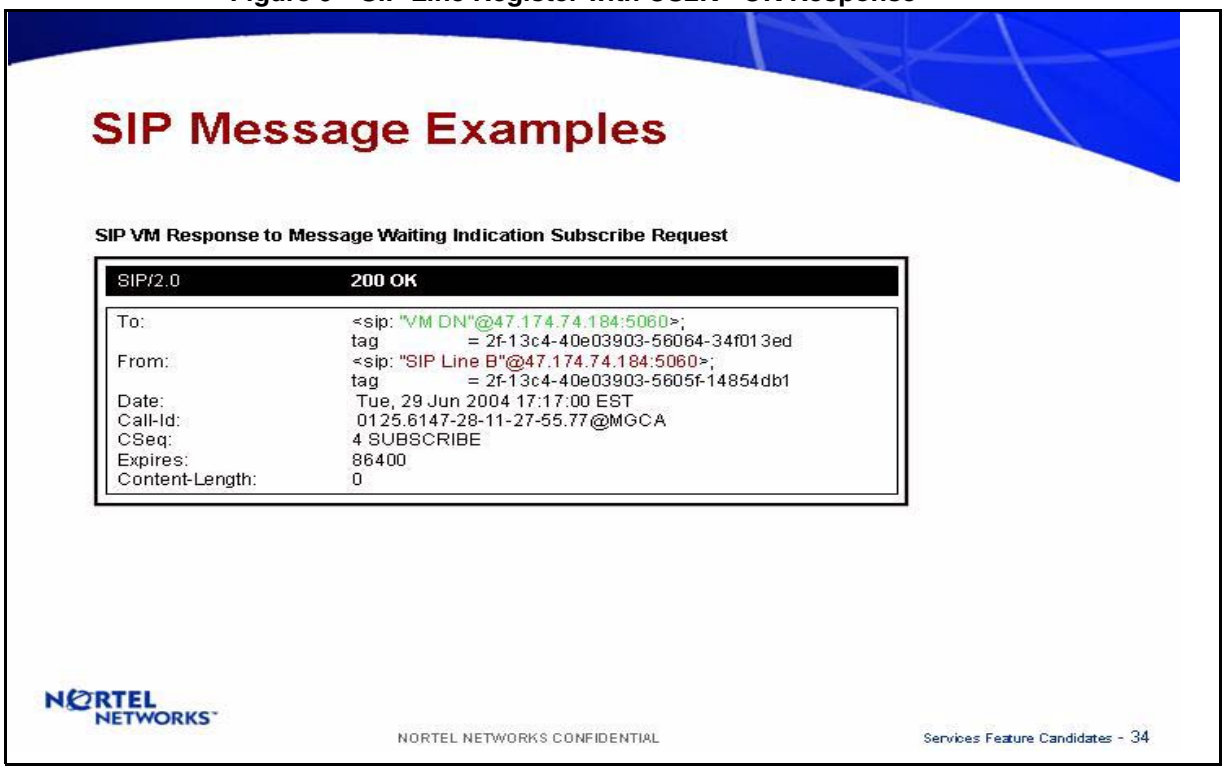


Figure 10 SIP Line Register with CS2K - NOTIFY Message

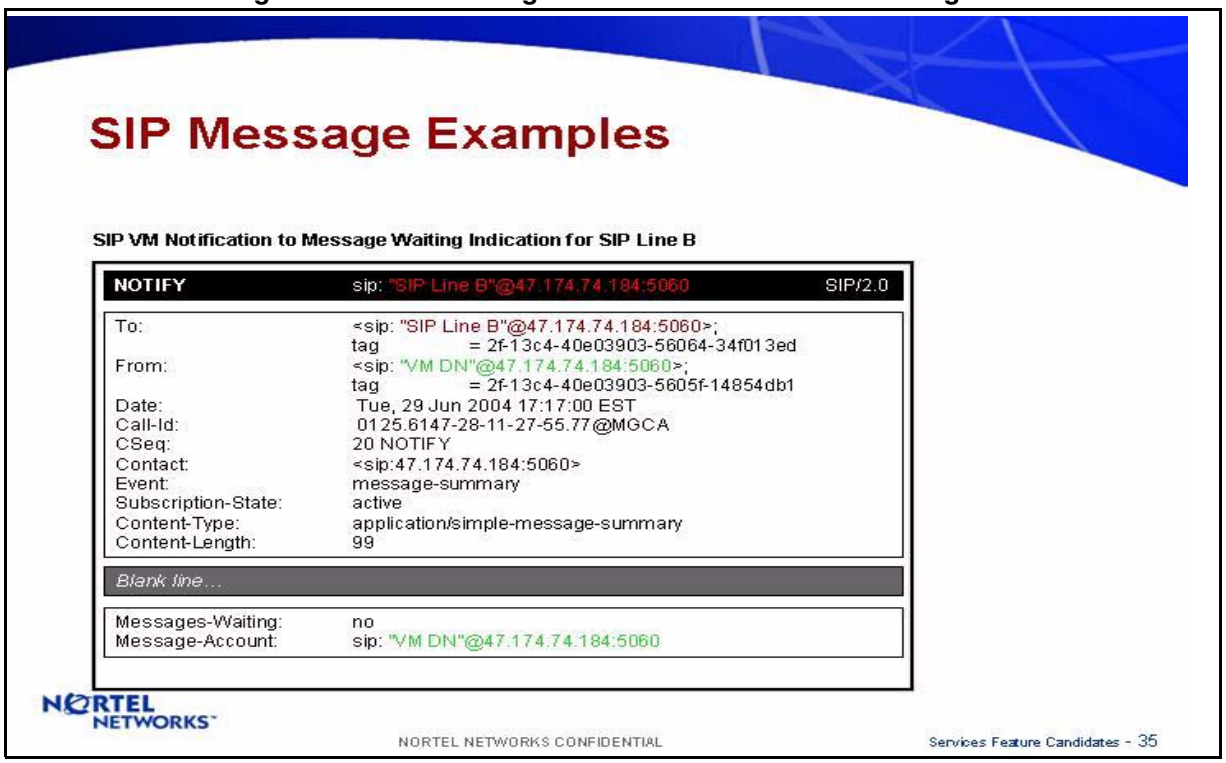
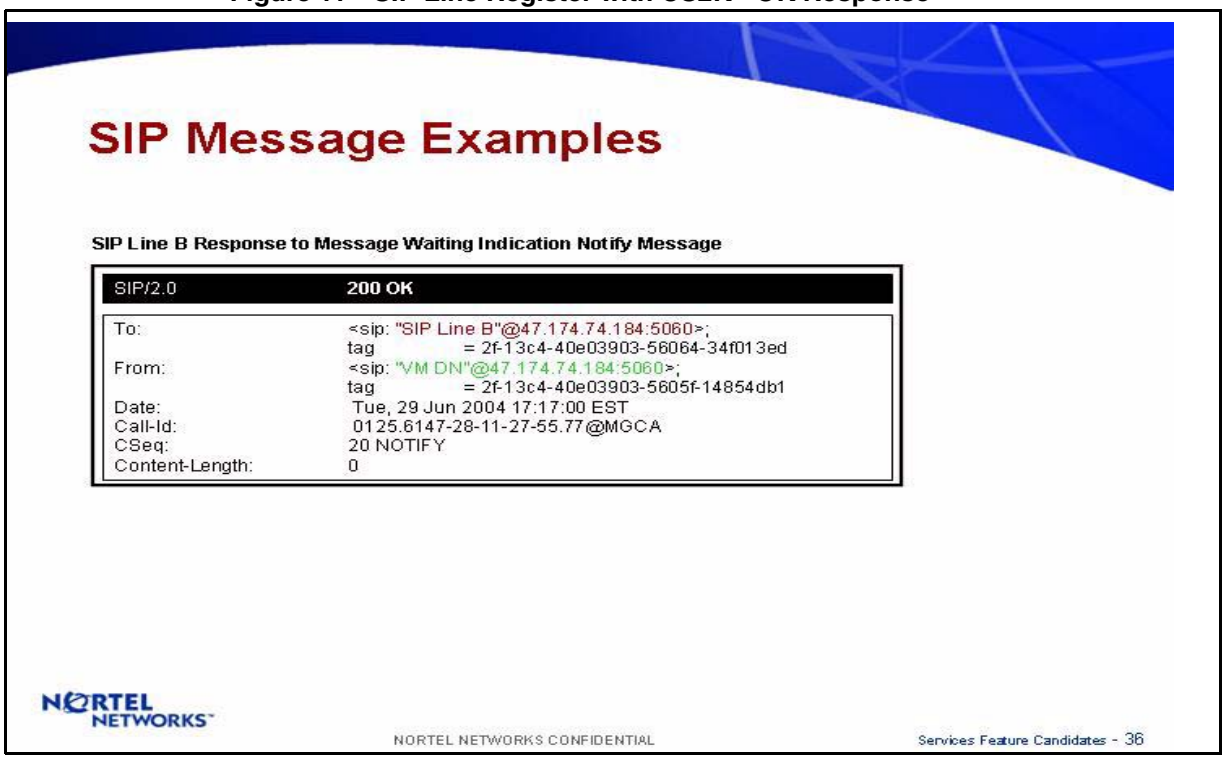


Figure 11 SIP Line Register with CS2K - OK Response



Step 2: Line A Calling SIP Line B and Forwarded to VM using SIP network

Figure 12 Call Termination to SIP VM DN - INVITE Message

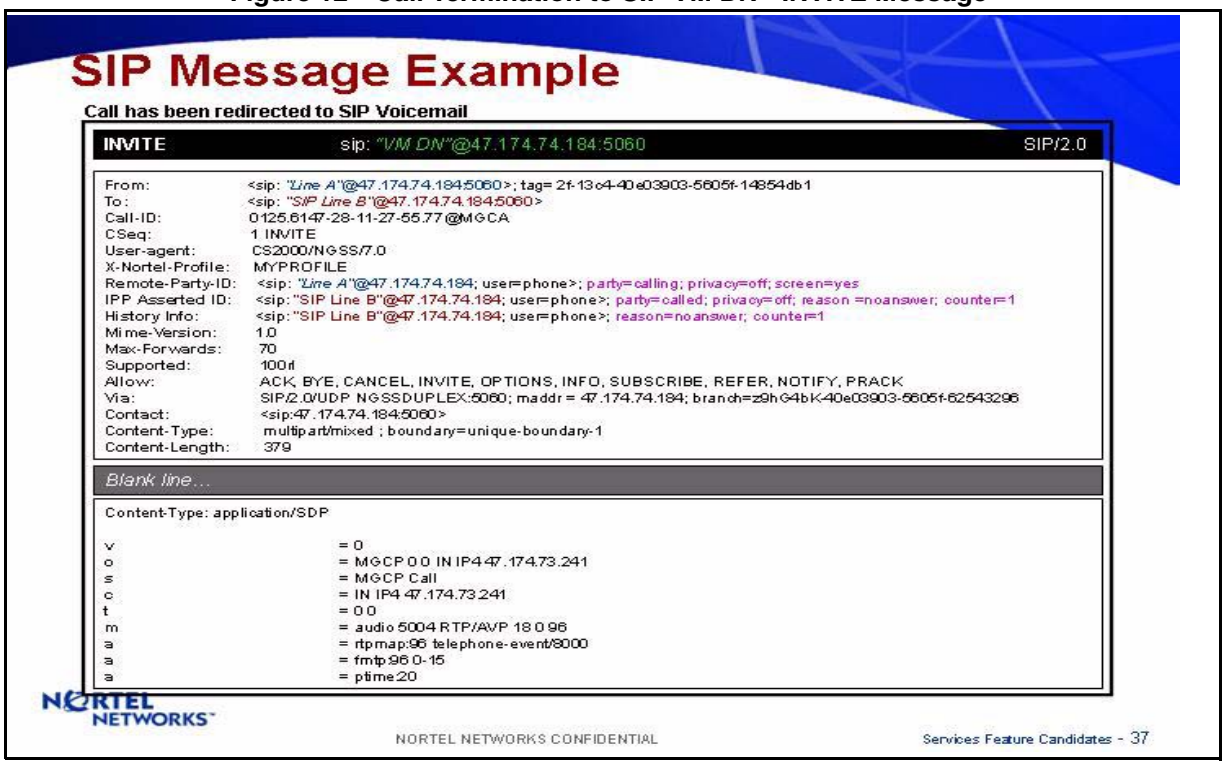


Figure 13 Call Termination to VM DN - 100 Trying Response

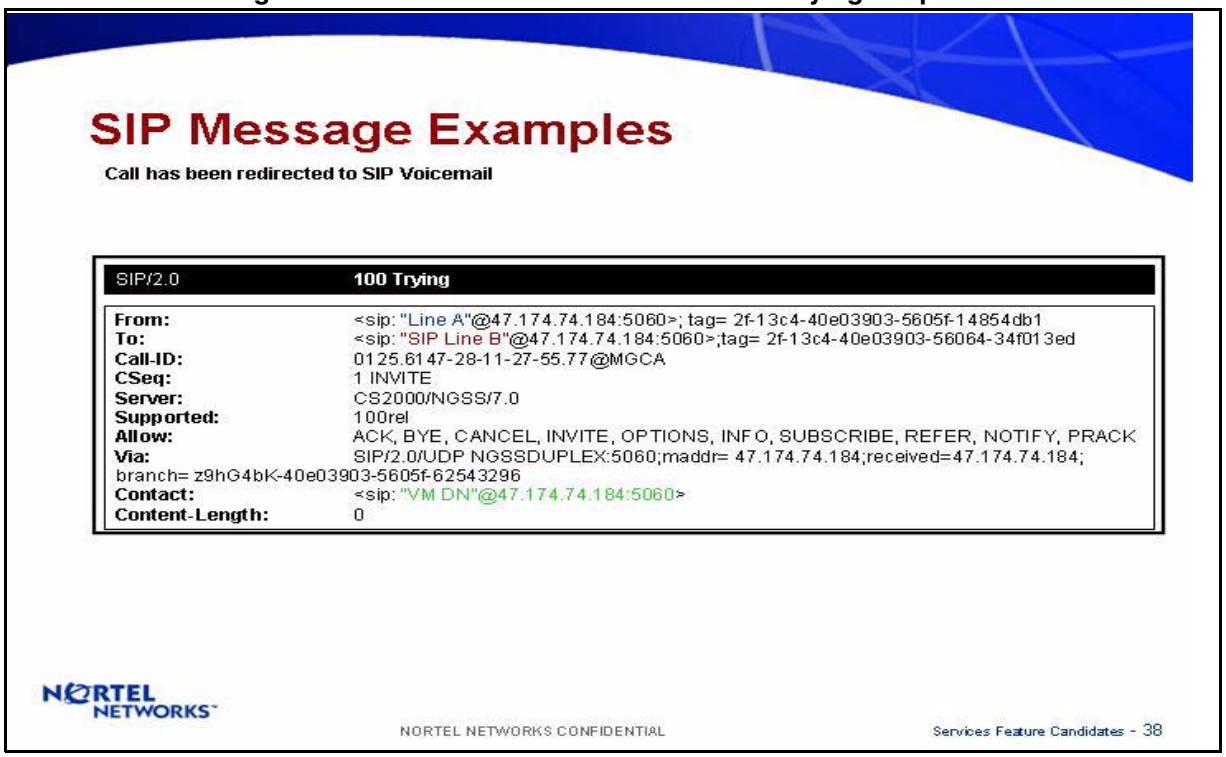


Figure 14 Call Termination to VM DN - 180 Ringing Response

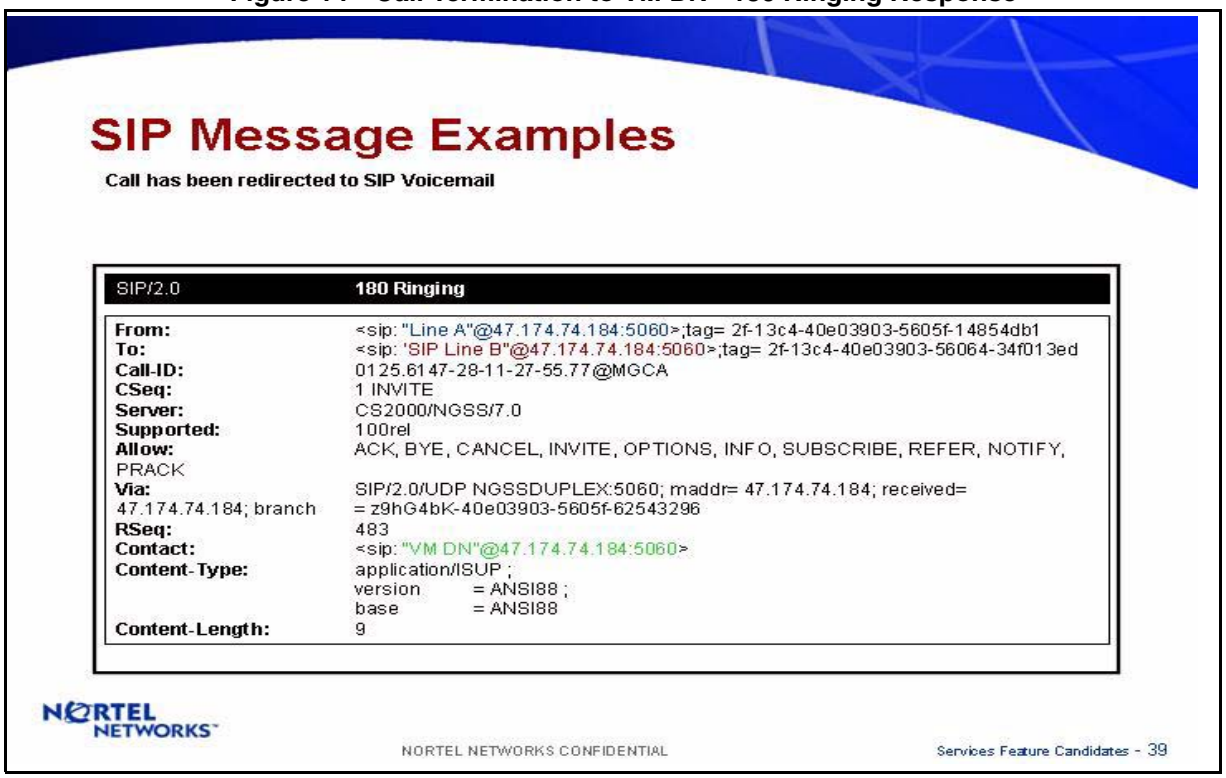


Figure 15 Call Termination to VM DN - 200 OK Response

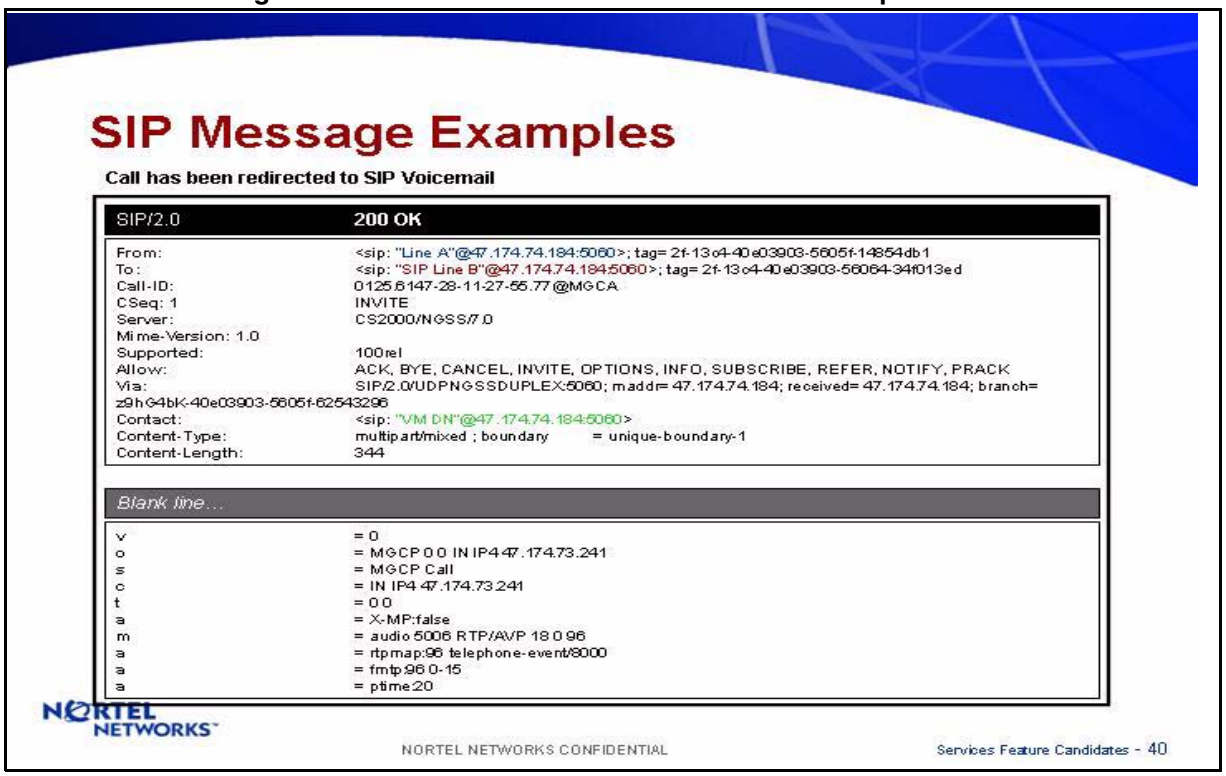
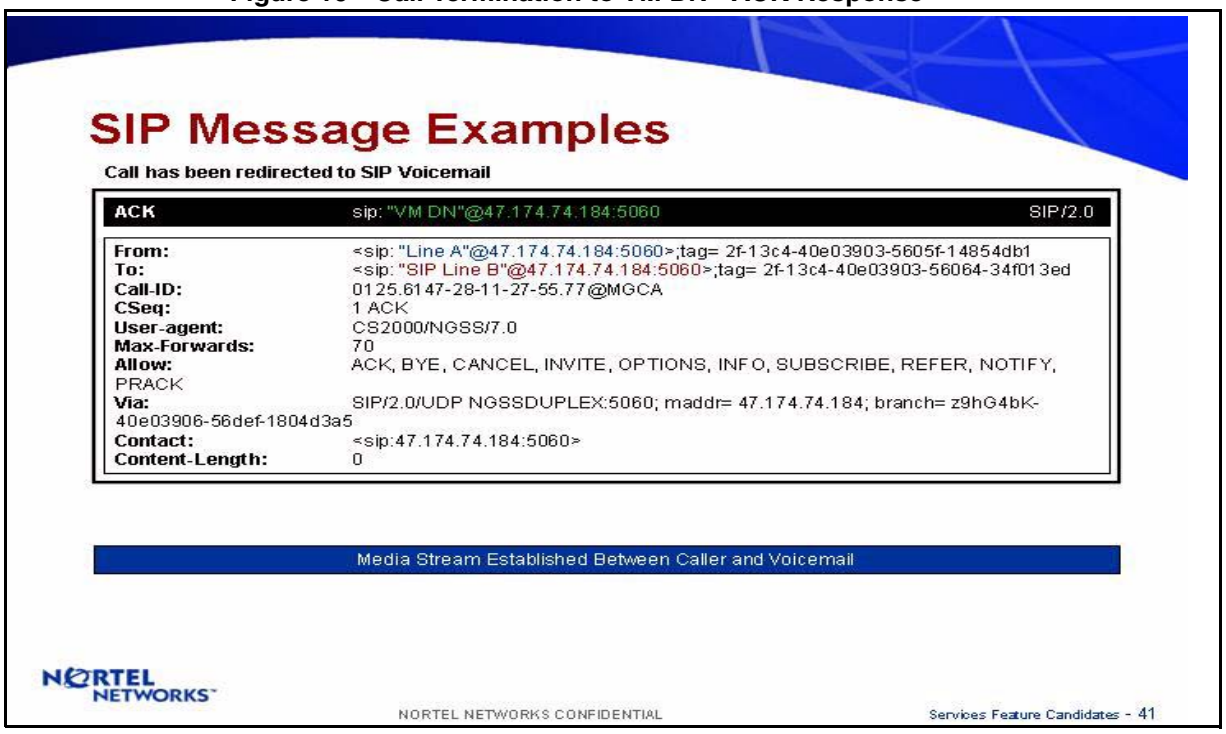


Figure 16 Call Termination to VM DN - ACK Response



Step 3: Caller Records Message and hang-up

Figure 17 Call Release from Caller - BYE Message

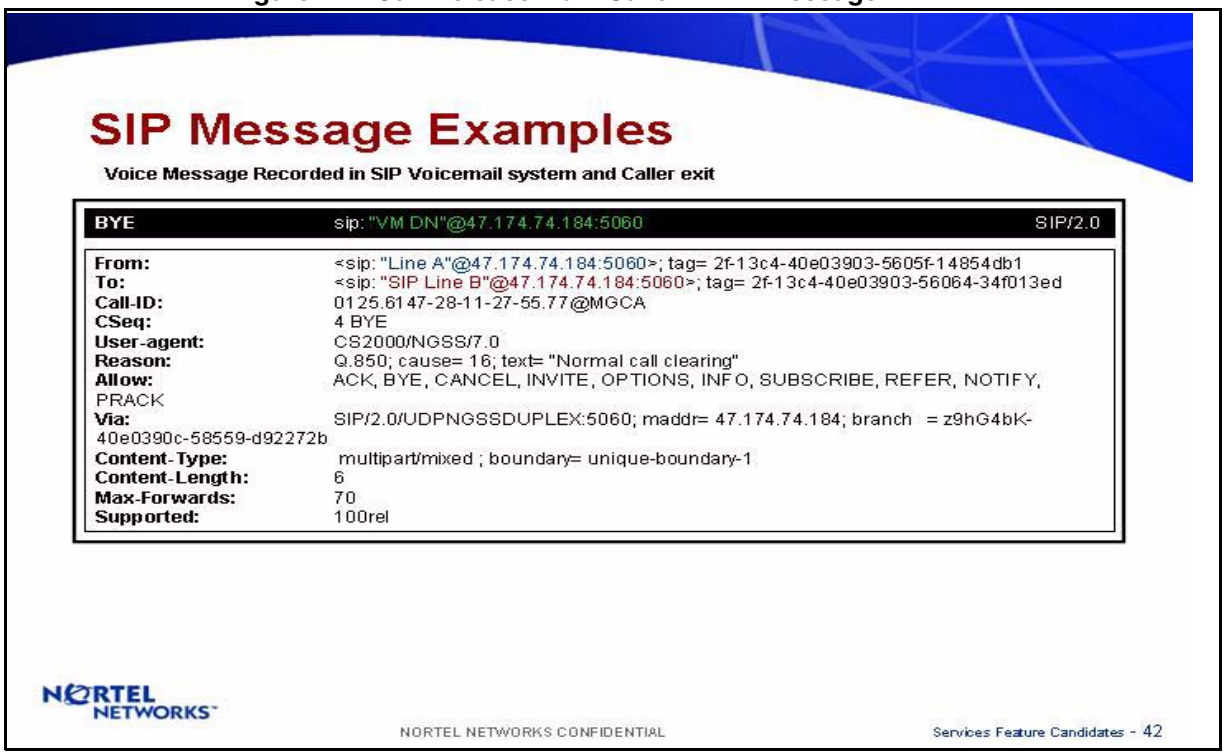
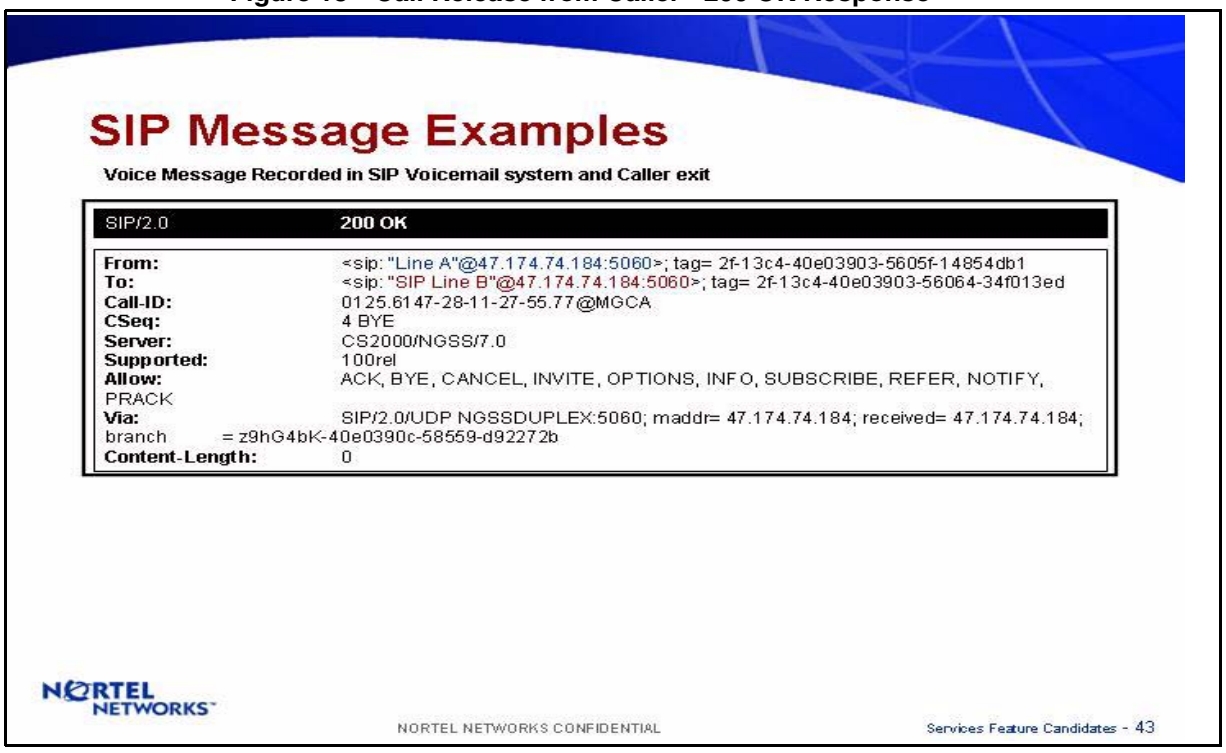


Figure 18 Call Release from Caller - 200 OK Response



Step 4: CS2K sends a NOTIFY Message

Figure 19 CS2K sends NOTIFY Message

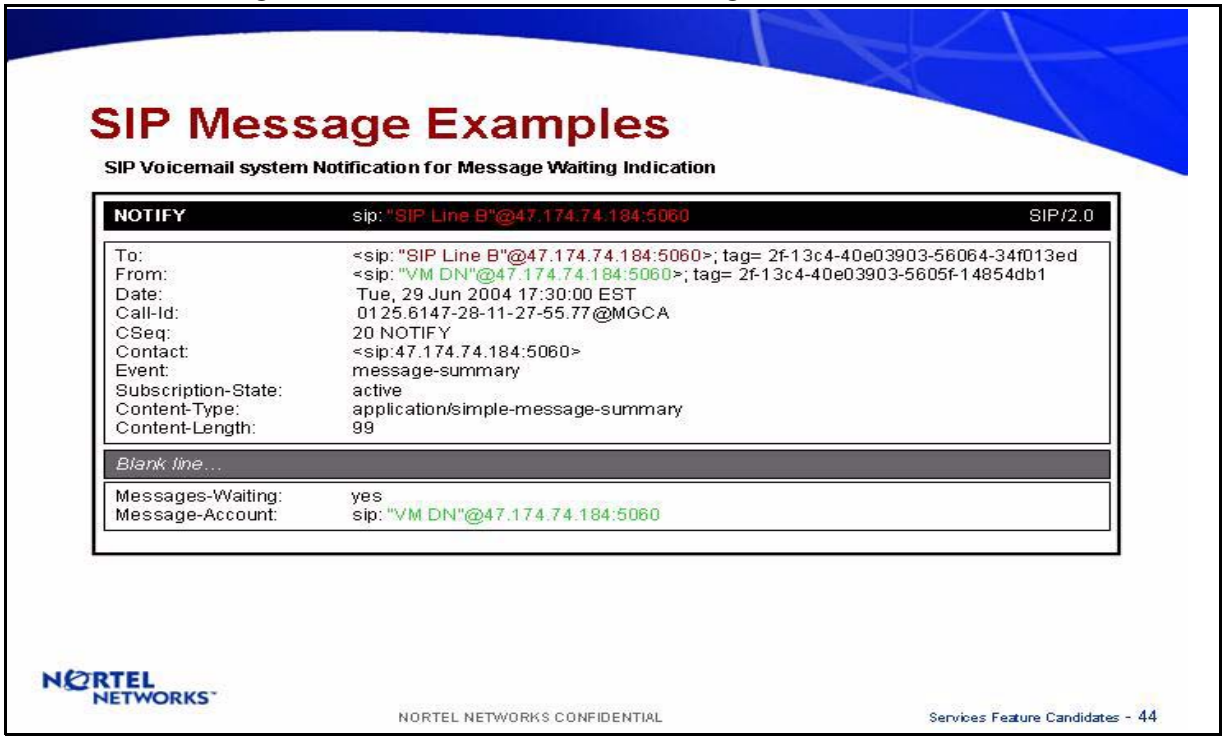
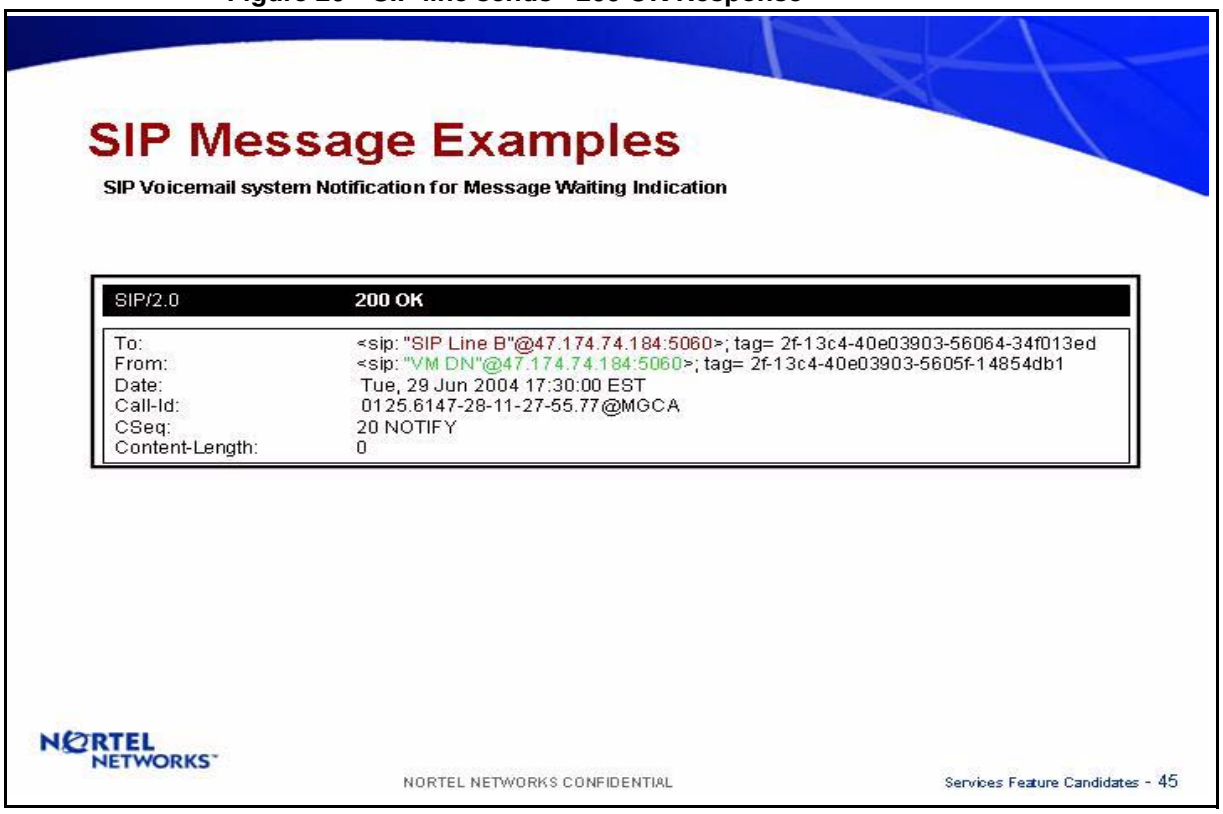


Figure 20 SIP line sends - 200 OK Response



Step 5: SIP Line retrieves the Messages from the VM using SIP network

Note: The SIP messages are related to basic SIP call.

Figure 21 SIP Line B Calling VM DN - INVITE Message

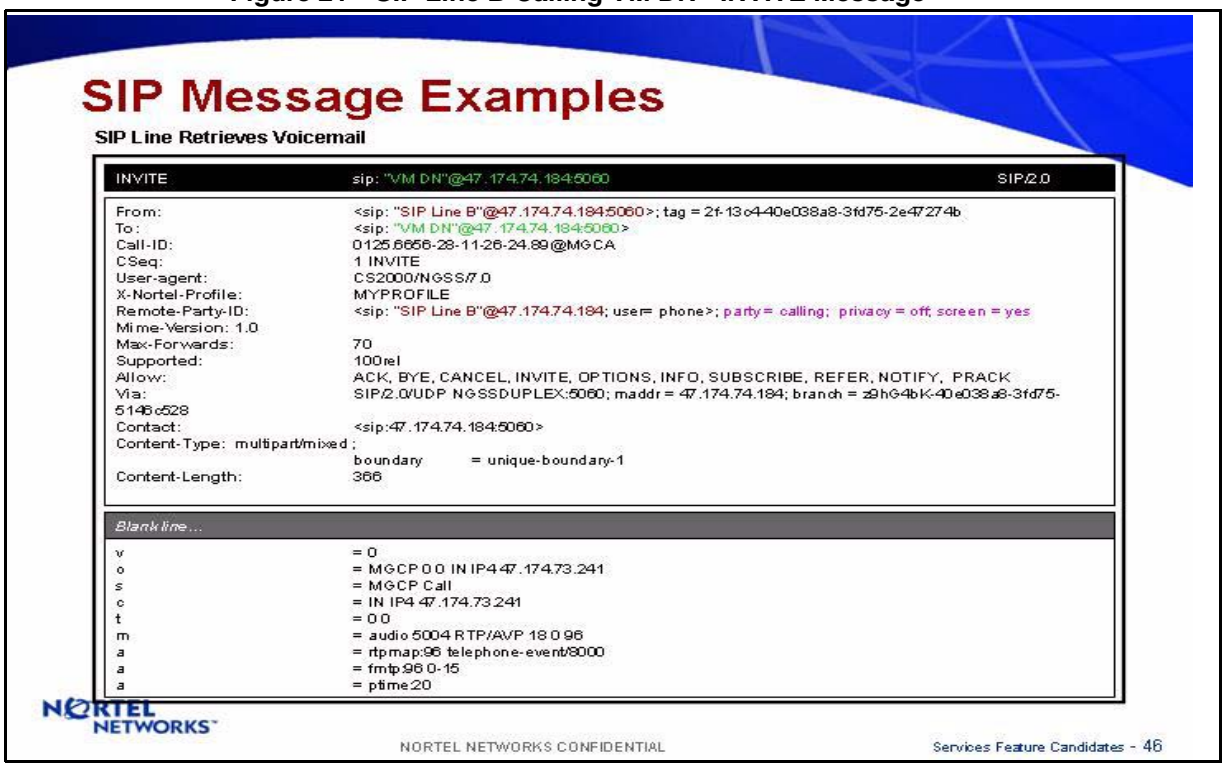


Figure 22 SIP Line B Calling VM DN - TRYING Message

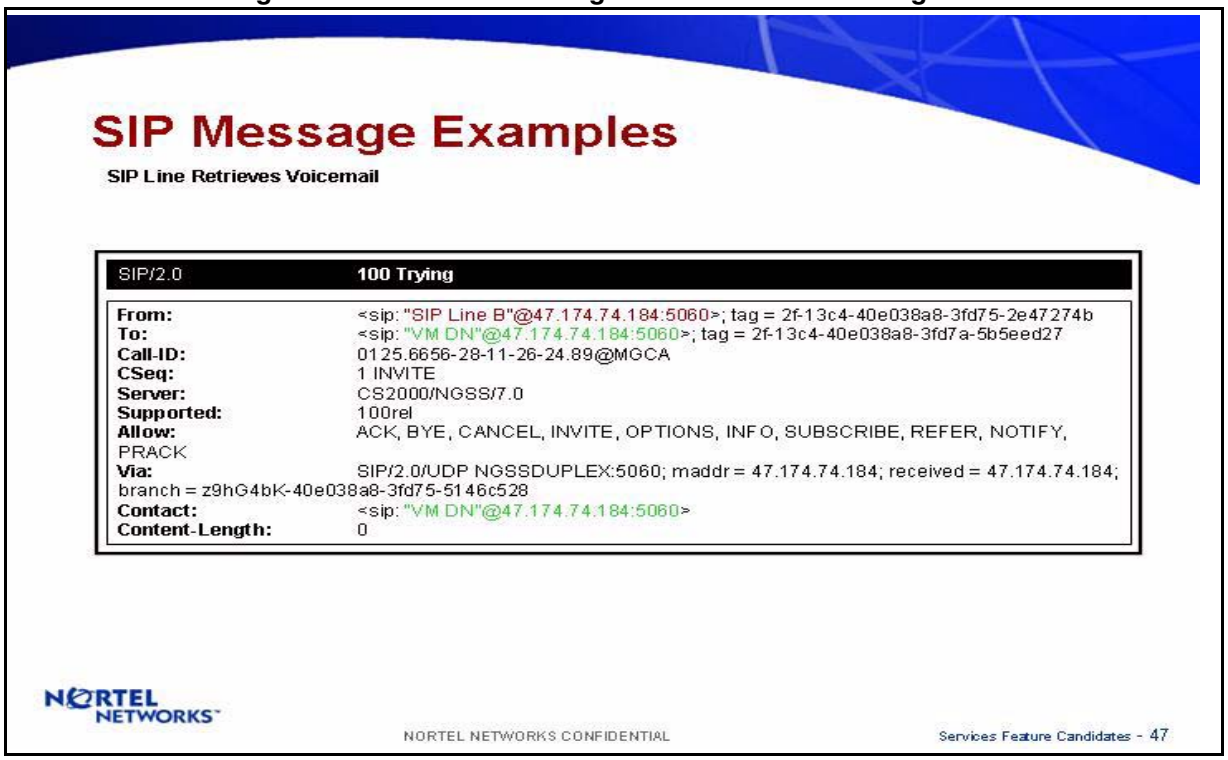


Figure 23 SIP Line B Calling VM DN - RINGING Message

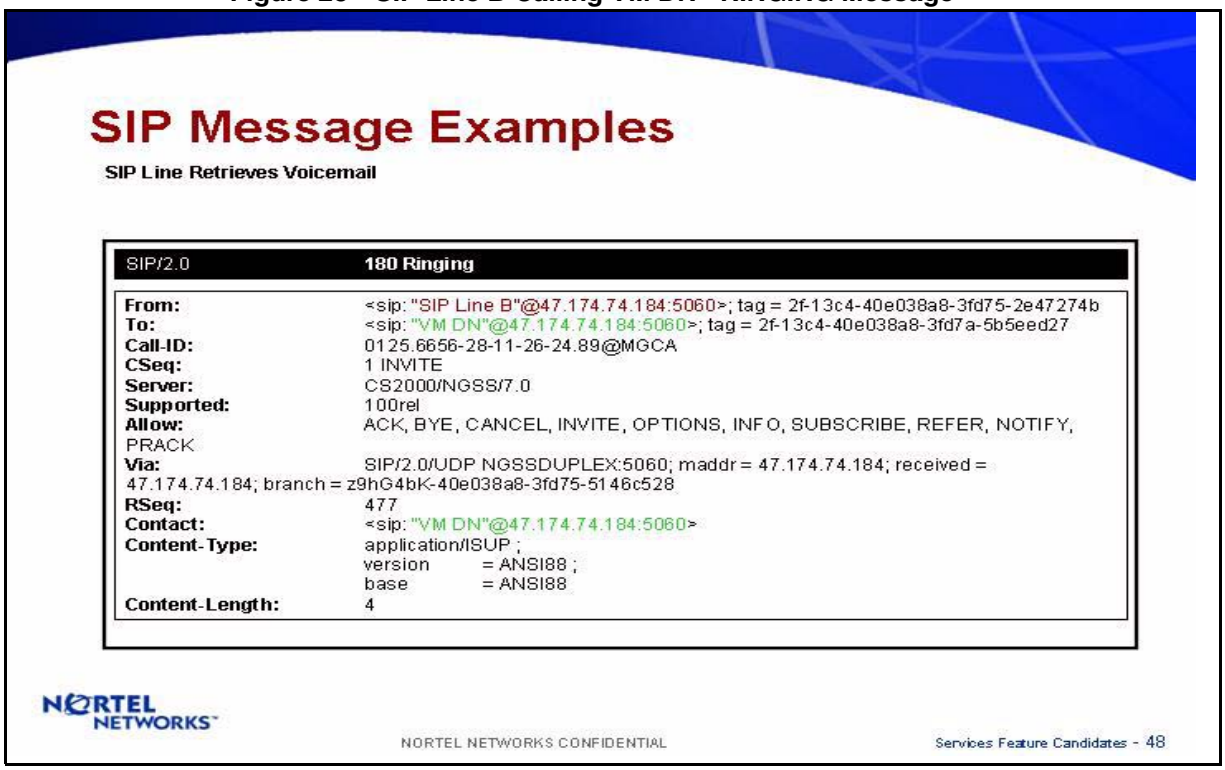


Figure 24 VM Answers - CS2K sends OK Response Message

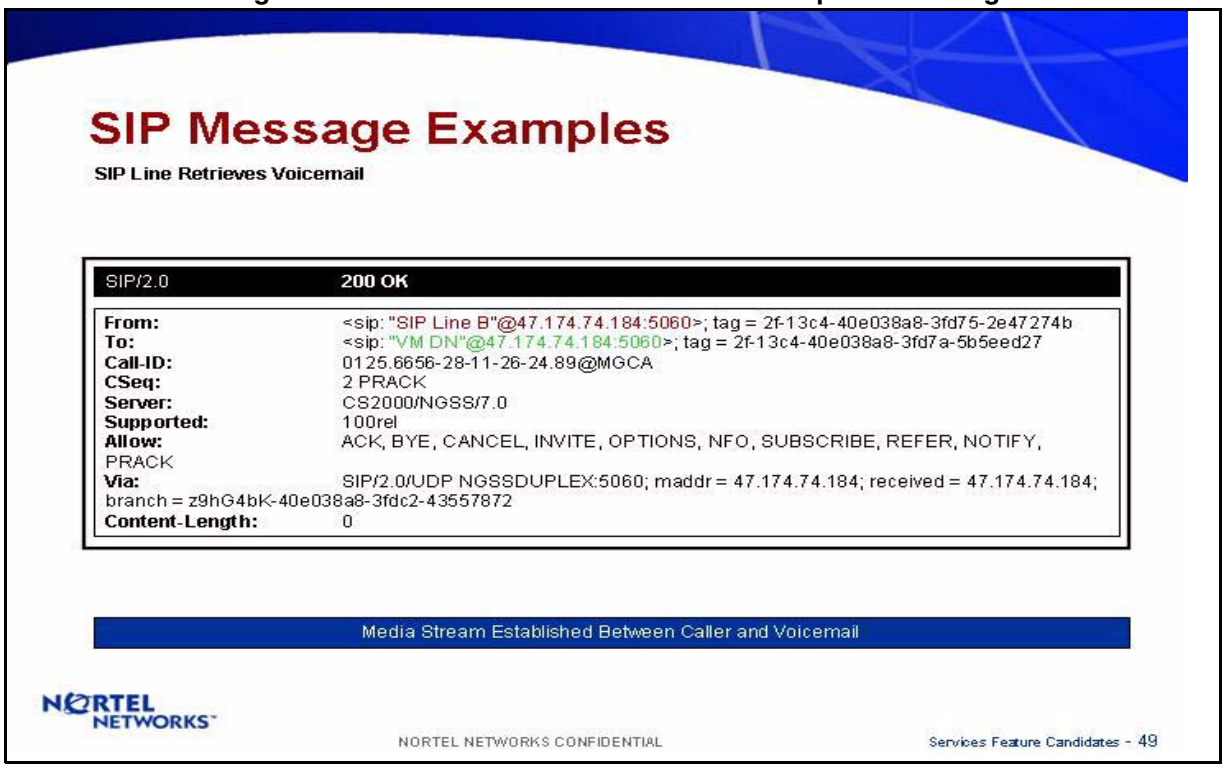


Figure 25 SIP Line B Accepts - ACK Response Message

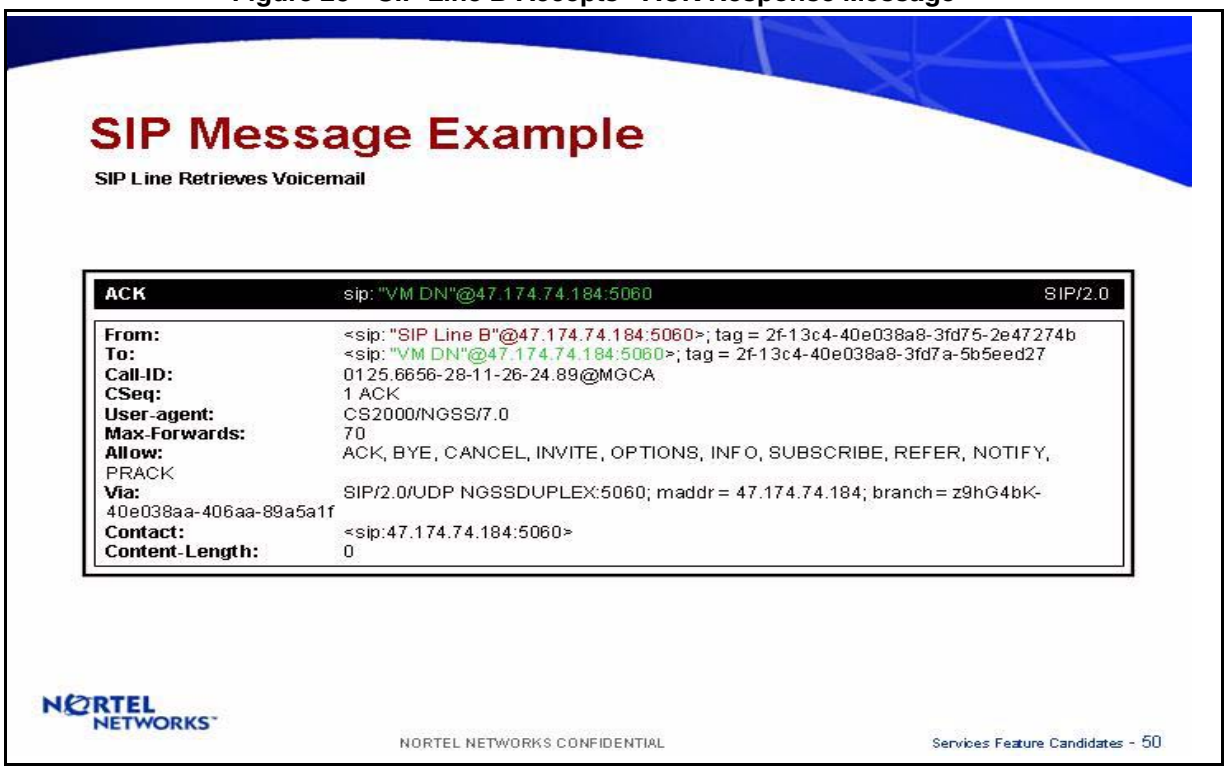


Figure 26 SIP Line B Exit from the Call - BYE Message

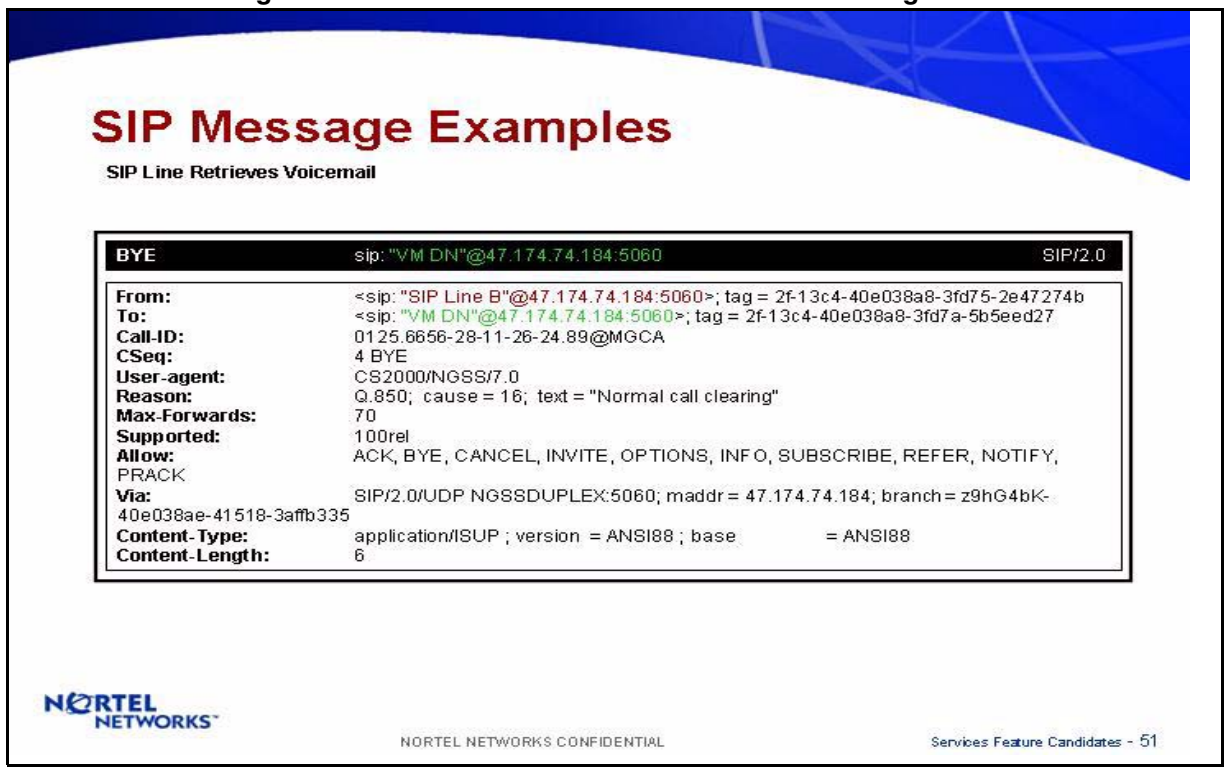
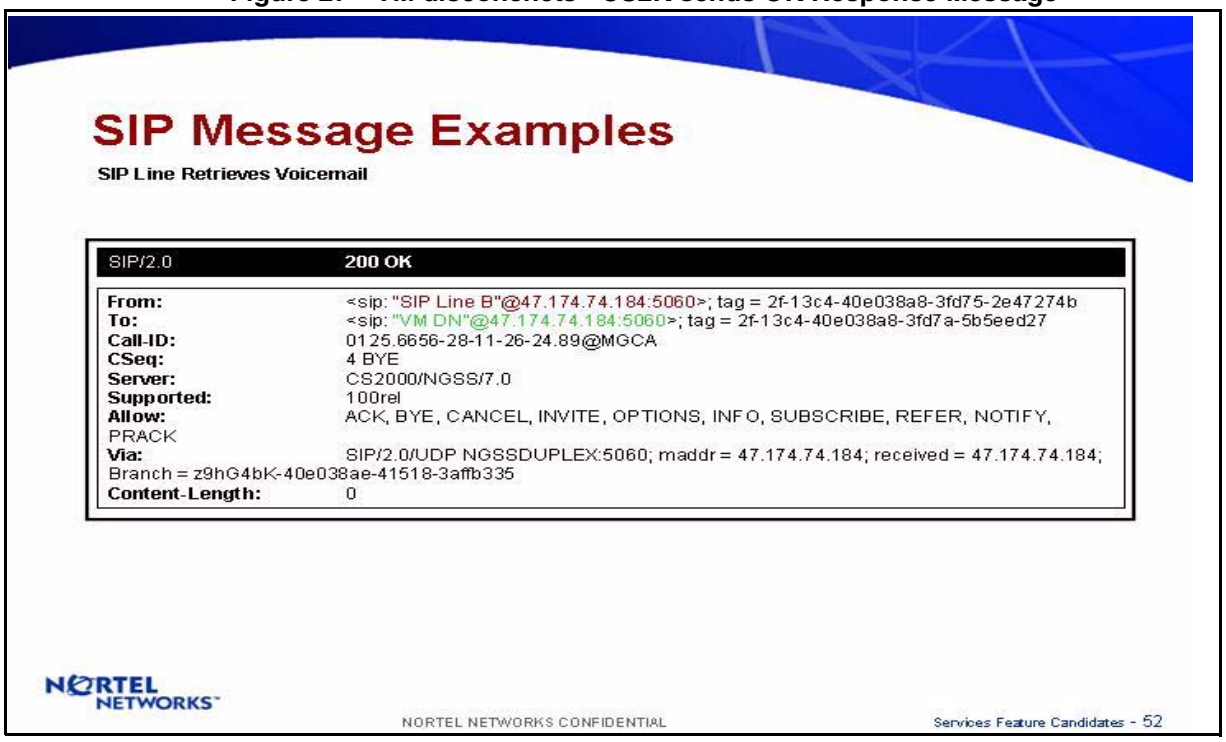


Figure 27 VM disconencts - CS2K sends OK Response Message



Step 6: CS2K sends NOTIFY message.

Figure 28 CS2K sends NOTIFY Message

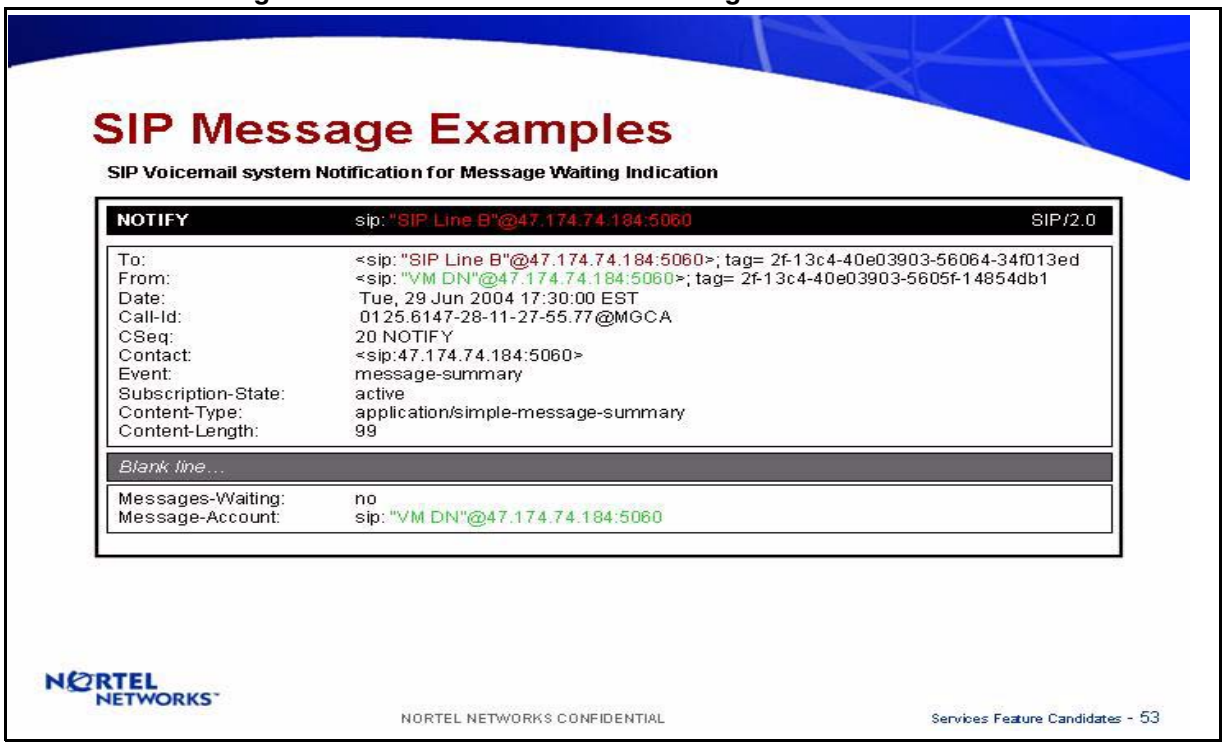
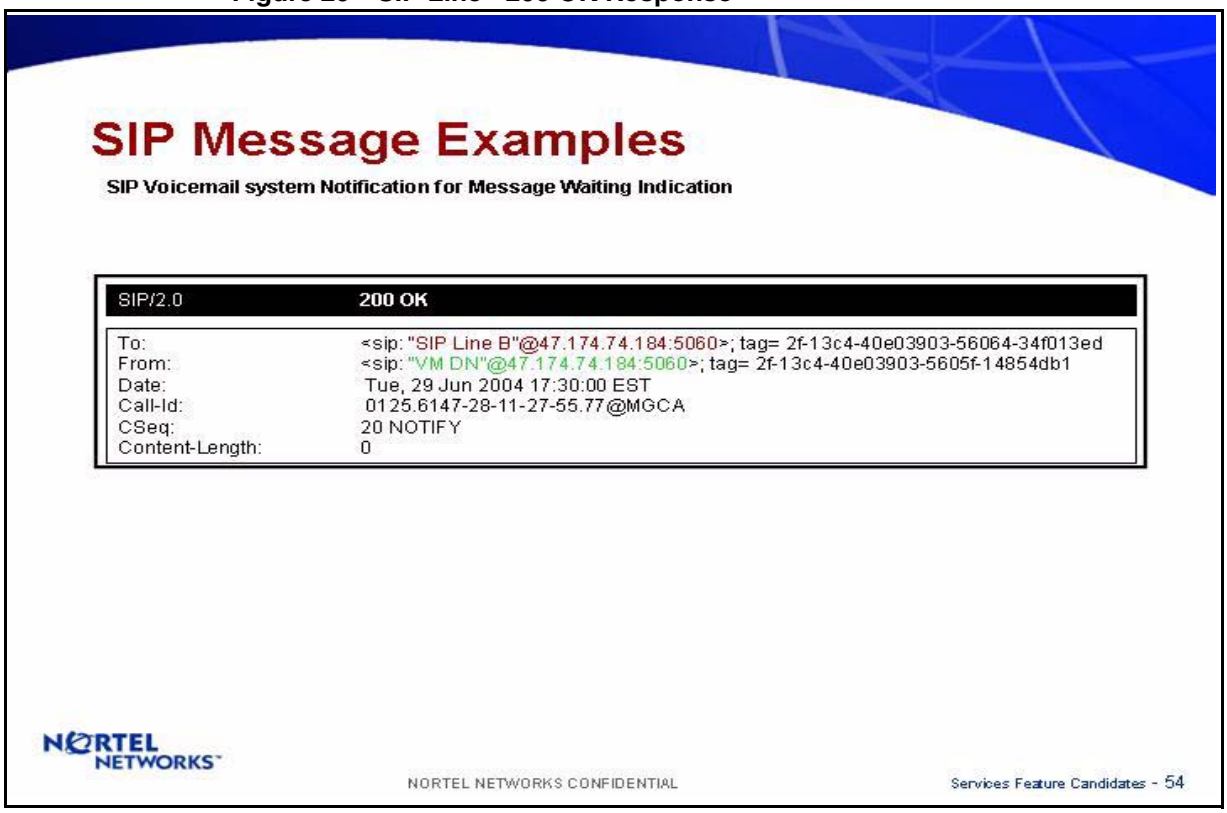


Figure 29 SIP Line - 200 OK Response



1.1.6 SOC Control

The new functionality is controlled by a SOC. This is a state controlled SOC. The following SOC is developed for this feature:

MDC00078 - NMS Over IP (SCTP)

1.2 Hardware Requirements or Dependencies

This feature uses the existing hardware of CS2K Core and Session Server. The Session Server provides standardized interface to SIP. Therefore, all 3rd party hardware and Voicemails are directly supported.

There is no new hardware dependency or requirement for this feature.

1.3 Software Requirements or Dependencies

The development depends on following 3rd party software currently exists in respective platform:

- SIP Stack from RADVISION in Session Server

1.4 Limitations and restrictions

The following limitations and restrictions apply to the feature:

- The NMS service sends MWI ON/OFF for the remote lines. It is assumed that the remote node or SIP Client will provide appropriate indication to end user for the MWI. The MWI indication can not be enforced.
- The Call Request Retrieval (CRR) functionality can not be invoked as second leg of Three way call (TWC). This limitation is for fraud prevention.
- The Call Request Retrieval (CRR) functionality can not be invoked as second or subsequent leg of a conference (CNF) call. This limitation is for fraud prevension.
- The MWT functionality is only provided to multiple appearance directory number (MADN) primary member.
- The MWT functionality is only provided to HUNT group primary member only.
- All existing MWT and NMS service limitations apply to this feature.
- The optional data defined in the RFC 3842 are not supported by this feature due to limited design scope. The support for the optional data can be developed in future releases.
- The direct SIP VM communication is not tested. Therefore, support for non-SIP lines using SIP VM can not be verified nor tested.
- In cases where a Line connected to a CS2K, the VM connected to a remote node (e.g. MCS) via SIP network and if G729 compatible codec is used for interconnect voice paths than remote node or device must support RFC 2833 for out of band DTMF signalling.
- When the line is connected to a remote node (e.g. MCS) via SIP network, VM is connected to a CS2K and if G729 compatible codec is used for interconnect voice paths than remote node or device must support RFC 2833 for out of band DTMF signalling.
- The design is generic and based on RFC 3842 standards. Testing limitations does not allow to test every possible interoperatibility using different handware and different vendor equipments in a network. Therefore, only tested network configurations are supported. In order to make other hardware and different vendor equipment supported, proper interoperatibility testing must be done in Nortel approved interoperatibility lab. After the complete testing, appropriate support will be provided.
- The design supports maximum of 10 digit DN in form of North American and Universal DN.
- The IP device supported in Table IPAPPL for SOC MDC00078 - NMS over SCTP are EIU and HIOP only.
- The SETPRIME and MULTIHOMING options in Table IPAPPL are allowed to add in Table IPAPPL. However, their usage is ignored.

- The MODE option in Table IPAPPL is always SERVER. If not added by the crafts person, it will be added automatically.
- The option NEWTOR in table MSGRTE is not supported.
- For international markets, only ETSI ISUP interworking is allowed. The DPNSS based interworking is not supported.

1.5 Interactions

The service is controlled by the CS2K Core. The Session Server and GWC only provides access to various networks and protocol conversions. Therefore, CS2K Core interactions are applicable to this service.

The existing MWT and NMS service software is used for the development. Therefore, all existing interactions are apply to this expansion of service. There is no new interaction anticipated at the time of this writing.

1.6 Glossary

Term	Description
CFB	Call Forward Busy
CFD/CFDA	Call Forward Do Not Answer
CFU	Call Forwarding Unconditional / Call Forwarding Universal
CICM	Centrex IP Line
CRR	Call Request Retrieval
CS2K	Communication Server 2000
DMS	Digital Multiplex Switch
DN	Directory Number
EO	End Office
ETSI	European Telecommunications Standards Institute
GCP	Generic Call Protocol
GW	Gateway
GWC	Gateway Controller
IAD	IP Analog Gateway
IBN	Integrated Business Line
IP	Internet Protocol
ISDN	Integrated Services Digital Network

Term	Description
KSET	Key Set Line
MCDN	Meridian Customer Defined Networking
MG9K	Media Gateway 9000
MS	Message Switch
MsgSrv	Message Server
MWI	Message Waiting Indication
MWT	Message Waiting
NCAS	Non-Call-Associated Signaling
NGSS	Session Server
NMS	Network Message Waiting
PBX	Private Branch Exchange
PC	Personal Computer
POTS	Plain Old Telephone Service
PSTN	Public Switched Telephony Network
PVG	Packet Voice Gateway
RES	Residential Line
S1K/1KM	Type of IP PBX
SCTP	Session Control Transport Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SMDI	Simplified Message Desk Interface
SOC	Software Optionality Control
SS7	Signaling System No. 7
TCAP	Transaction Capabilities Application Part
TDM	Time Division Multiplexing
TEL URI	Telephony URI
TPT	Terminal Processing Task
UCD	Uniform Call Distribution
UM	Unified Messaging
URI	Uniform Resource Identifiers
VM	Voicemail System

Term	Description
VoIP	Voice over Internet Protocol

2: Fault Management for A00007544

2.1 Fault management strategy

The fault management information is provided using LOGs. The LOGUTIL CI provide the access to the LOGs generated by MWT and NMS software. The LOG are generated based on LOG framework. This feature uses the existing framework to add new LOGs in MWT and NMS software.

2.2 Fault management tools and utilities

2.2.1 Faults, Alarms and Logs

The LOGUTIL CI command is used as tools in the CS2K Core software. All existing tools and utilities are applicable in case of CS2K Core software.

The LOG generated in the GWC are passed to the CS2K Core via maintenance logs. Therefore, they are also available as part of the CS2K Core tools and utilities.
The Session Server (NGSS) LOGs are independent and uses the new mechanism to pass the LOG information to the remote system. The existing LOG tools and utilities are used in the NGSS.

2.3 Logs (For CS2K only)

The following Logs are aded in DMS/C22K Core as part of this activity:

- NMSS115: It is generated if an error occurs while sending NMS TCAP messages to SCTP
- NMSS116: It is generated if an error occurs while receiving NMS TCAP messages from SCTP
- NMSS117: It is generated if an error occurs while sending NMS REJ messages to SCTP
- NMSS118: It is generated if an error occurs while receiving NMS REJ messages from SCTP.

2.4 Log Title/Log ID: NMSS115

2.4.1 Formats

<Switch ID> NMSS115 <DATE> <TIME> INFO
SCTPNMS_ERR_SNT_REPORT

Error occurred while sending NMS messages over SCTP.

Example:

RSNN08AZ NMSS115 NOV25 09:40:46 0800 INFO SCTPNMS_ERR_SNT_REPORT

Error occured while sending NMS messages over SCTP.

2.4.1.1 NTSTD
Not Applicable

2.4.1.2 SCC2
Not Applicable

2.4.1.3 Syslog
Not Applicable

2.4.1.4 SNMP
Not Applicable

2.4.2 Explanation
Description: This log is generated in association with a OM PEG. It provides information regarding a problem in sending Non-CallP messages to the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the SCTP.

2.4.3 Field descriptions
There are no fileds in the log. The string is self explanatory.

2.4.4 Action

2.4.5 Associated Operational Measurements or Performance Measurements
This log is generated when the SCTPNMSS OM is not pegged.

2.4.6 Additional information
N/A

2.5 Log Title/Log ID: NMSS116

2.5.1 Formats

<Switch ID> NMSS116 <DATE> <TIME> INFO SCTPNMS_ERR_RCV_REPORT

Error occurred while receiving NMS messages over SCTP.

Example:

RSNN08AZ NMSS116 NOV25 09:41:25 0800 INFO SCTPNMS_ERR_RCV_REPORT

Error occurred while receiving NMS messages over SCTP.

2.5.1.1 NTSTD
Not Applicable

2.5.1.2 SCC2
Not Applicable

2.5.1.3 Syslog
Not Applicable

2.5.1.4 SNMP
Not Applicable

2.5.2 Explanation
Description: This log is generated in association with a OM PEG. It provides information regarding a problem in receiving Non-CallP messages from the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the CS2K. The NMS TCAP message received is corrupted.

2.5.3 Field descriptions
There are no fileds in the log. The string is self explanatory.

2.5.4 Action

2.5.5 Associated Operational Measurements or Performance Measurements
This log is generated when the SCTPNMSR OM is not pegged.

2.5.6 Additional information
N/A

2.6 Log Title/Log ID: NMSS117

2.6.1 Formats

<Switch ID> NMSS117 <DATE> <TIME> INFO SCTPREJ_ERR_SNT_REPORT

Error occured while sending REJ messages over SCTP.

Example:

RSNN08AZ NMSS117 NOV25 09:45:23 0800 INFO SCTPREJ_ERR_SNT_REPORT

Error occured while sending REJ messages over SCTP.

2.6.1.1 NTSTD
Not Applicable

2.6.1.2 SCC2
Not Applicable

2.6.1.3 Syslog
Not Applicable

2.6.1.4 SNMP
Not Applicable

2.6.2 Explanation
Description: This log is generated in association with a OM PEG. It provides information regarding a problem in sending Non-CallP messages to the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the SCTP.

2.6.3 Field descriptions
There are no fileds in the log. The string is self explanatory.

2.6.4 Action

2.6.5 Associated Operational Measurements or Performance Measurements
This log is generated when the SCTPREJS OM is not pegged.

2.6.6 Additional information
N/A

2.7 Log Title/Log ID: NMSS118

2.7.1 Formats

<Switch ID> NMSS118 <DATE> <TIME> INFO SCTPREJ_ERR_RCV_REPORT

Error occured while sending NMS messages over SCTP.

Example:

RSNN08AZ NMSS118 NOV25 09:47:26 0800 INFO SCTPREJ_ERR_RCV_REPORT

Error occured while receiving REJ messages over SCTP.

2.7.1.1 NTSTD
Not Applicable

2.7.1.2 SCC2
Not Applicable

2.7.1.3 Syslog
Not Applicable

2.7.1.4 SNMP
Not Applicable

2.7.2 Explanation
Description: This log is generated in association with a OM PEG. It provides information regarding a problem in sending Non-CallP messages to the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the CS2K.The REJECT message received is corrupted.

2.7.3 Field descriptions
There are no fileds in the log. The string is self explanatory.

2.7.4 Action

2.7.5 Associated Operational Measurements or Performance Measurements
This log is generated when the SCTPREJR OM is not pegged.

2.7.6 Additional information
N/A

2.7.7 Explanation
Description: This log is generated in association with a OM PEG. It provides information regarding a problem in sending Non-CallP messages to the SCTP. When this log is generated, it indicates that the MWI service is broken for a subscriber in the the CS2K. The REJECT message received is corrupted.

2.7.8 Field descriptions
There are no fileds in the log. The string is self explanatory.

2.7.9 Action

2.7.10 Associated Operational Measurements or Performance Measurements
This log is generated when the SCTPREJR OM is not pegged.

2.7.11 Additional information
N/A

2.8 Logs (For NGSS only)

The following logs are added on NGSS as a part of this activity. These logs can be viewed using the NGSS web interface.

1 NCAS601 : This log is raised when a new NCAS Link is created.

2. NCAS325 : This log is generated when an alarm is generated when the NCAS Link goes down.It is also generated when the alarm is cleared when the NCAS Link comes up.

2.9 Log Title/Log ID: NCAS601

2.9.1 Formats

<MMM dd hh:mm:ss> <device name> <prog name>: <Log Name> <alarm value> <event type><label><text format>

<MMM dd hh:mm:ss> : Current date and time.

<device name> : The name assigned to the session server.

<prog name> : The name of the program that generates the log.

<Log Name> : Log Name - NCAS601

<alarm value> : None

<event type> : INFO

<label> : NCAS Link created

<text format> : A new SCTP connection -LINK1 has been established between SCPLite and the core

Here LINK1 is the name given to the new NCAS Link created.

Example:
Feb 7 08:54:56 rtptngss0-1 a.out: NCAS601 NONE INFO NCAS Link Created A new SCTP connection -LINK1 has been established between SCPLite and the core

2.9.1.1 NTSTD

Not Applicable

2.9.1.2 SCC2

Not Applicable

2.9.1.3 Syslog

Not Applicable

2.9.1.4 SNMP

Not Applicable

2.9.2 Explanation

Description:This log is generated when a new NCAS Link is created.

2.9.3 Field descriptions

There are no fileds in the log. The string is self explanatory.

2.9.4 Action

None.

2.9.5 Associated Operational Measurements or Performance Measurements

N/A.

2.9.6 Additional information

N/A

2.10 Alarms

The new alarms will be added in the NGSS for the SCTP link between NGSS and CM. The alarm NCAS325 is raised when the NCAS Link connection is lost. .

2.10.1 Integrated Element Manager GUI Fields

Table 1: IEMS Alarm GUI Field descriptions

Field	Value
Severity	CRIT
Category	Communications
LogName	NCAS
LogNumber	325
EventType	TBL
EventLabel	NCAS Link Down
ProbableCause	outOfService
SpecificProblem	NCAS Link Connection between the core and Scplite is lost

Table 1: IEMS Alarm GUI Field descriptions

Field	Value
BodyText	SCTP connection -LinkName between SCPLite and the core is lost

2.10.2 Explanation

Description: NCAS325 Alarm is raised when the SCTP connection between the SCPLite and the core is lost.. When the alarm is raised an NCAS325 log is generated and can be found in the customer logs. Severity: Critical

2.10.3 Action

The SCTP Connection between the SCPLite and the core has to be restored.

2.10.4 Corresponding Clear Log

Log Title: NCAS325 - SCTP Connection Restored.

This log is generated when the NCAS Link down trouble alarm is lowered.

2.10.4.1 Format

<Date> <Time> <DeviceName> alarmd: NCAS325 <AlarmSeverity> TBL NCAS Link Down: <DeviceInfo> <AlarmRaiseLowerText>

<Date> : Current Date

<Time> : Current Time

<DeviceName> : The name assigned to the session server.

<AlarmSeverity>: The current severity of the alarm.

CRIT

NONE

<DeviceInfo> : Info which specifies the device to which the alarm pertains

<AlarmRaiseLowerText> :

SCTP Connection between SCPLite and core is lost

SCTP Connection between SCPLite and core is lost - Alarm Cleared

Feb 7 08:55:06 rtptngss0-1 alarmd: NCAS206 NONE TBL NCAS Link NCGL=rtptngss0-1;Unit=1;SCTP Connection Link1 between the SCPLite and core is lost - Alarm cleared

2.10.4.2 NTSTD

2.10.4.3 SCC2

2.10.4.4 Syslog

2.10.4.5 SNMP

Table 2: NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label		*NCAS Link Down*				
Equipment ID						

Table 3: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Location:				
Notification Id:				
State:				
Category:		*Communication*		
Cause:		*outOfService*		
Time:				
Component Id:		*NCAS*		
Specific Problem:		*NCAS Link Connection between the core and Scplite is lost*		

Table 3: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Description:		*SCTP Connection Link1 between the SCPLite and core is lost - Alarm cleared*		
Fabric				
Frame Location				

2.11 Related documentation

Appropriate NTP contains the details of various existing logs.

3: Configuration for A00007544

3.1 Hardware and Software Requirements

The design depends on the RADVISION stack in Session Server (NGSS) for SIP. There is no additional hardware or software requirements.

If the remote node/system/VM/switching entity complies with the standard protocols supported by this design, then it will be able to interwork with the CS2K. Appropriate changes should be developed in the remote systems and this design have no specific information on configurations of the remote systems.

3.2 Initial Configuration

By default the SOC for the design are at idle state. Therefore, no service will be provided by this design. At initial configurations, it is assumed that standard datafill exists in the DMS/CS2K, GWC and NGSS. The new configurations associated with this feature do not exist.

For supported configurations, please see “Configuration Walkthrough” on page 989.

3.3 Office/Subnet parameters (OP/SP) (CM & SESM)

This design does not require any office parameter or subnet parameter. However, it does requires definition of appropriate IP address, Port number and application name for the NCAS link. For details, please See “Data schema (DS) (CM, MIBS, RDB)” on page 974. No details are added here.

3.3.1 New/modified office/subnet parameters

Not Applicable

3.4 Upgrade Considerations

Not Applicable.

3.5 Data schema (DS) (CM, MIBS, RDB)

3.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/ OLD/UNCHANGED)
IPAPPL	CHANGED	UNCHANGED
MSGRTE	CHANGED	UNCHANGED

3.5.2 Table/MIB/Remote Database Schema information

3.5.2.1 Name: IPAPPL

IP APPLICATION TABLE

3.5.2.1.1 Functional description

This table contains information about the IP addresses and Port numbers of remote system needed for the SCTP communication. This table also contains information about what application this tuple is datafilled.

3.5.2.1.2 Usage sequence and implications (CM Only)

This table should be datafilled first to create a NCAS link.

3.5.2.1.3 Size

Not changed.

3.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for IPAPPL.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPT	Changed	SERVICE	NMS	New added service

3.5.2.1.5 Datafill example

The following example shows sample datafill for table IPAPPL.

2 NCAS SCTP EIU (IPV4 47 142 160 171) (IPV4 47 142 160 172) $ 4990

(APPLICATION NMS) $

3.5.2.1.6 Table release history update
The NMS is added in this release. The Table was created in SN07 release.

3.5.2.1.7 Supplementary information
None.

3.5.2.1.8 Translation verification and other tools
The Table IPAPPL does not use translation verification tools.

3.5.2.2 Name: MSGRTE
MESSAGE ROUTING TABLE

3.5.2.2.1 Functional description
This table provides the routing of the message based on the selector in the table.

3.5.2.2.2 Usage sequence and implications (CM Only)
The datafill for the NCAS link should be done in Table IPAPPL prior to datafilling this table.

3.5.2.2.3 Size
Not changed.

3.5.2.2.4 Fields/OIDs
The following table lists fields/OIDs for MSGRTE

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MSGRTRES	Changed	MSGRTE_SEL	SCTP <Instance number>	New selector SCTP is added.

3.5.2.2.5 Datafill example
The following example shows sample datafill for table MSGRTE:

PUBLIC 6137221440 6137221540 (SCTP 2) $

3.5.2.2.6 Table release history update
New selectors are added.

3.5.2.2.7 Supplementary information
None

3.5.2.2.8 Translation verification and other tools

Not Applicable

3.6 Service Orders (SO) (CM & SESM)

Not Applicable.

3.7 Software optionality control (SOC)

Based on PLM input this section will be updated.

Table 4 SOC

SOC option name:	MDC00078
SOC option title:	NMS Over IP (SCTP)
SOC option control type:	State
New SOC option?	Yes
SOC option order code	00041296
Option defined in DRU:	CCM
Affected products:	All

3.8 Element Management

3.8.1 New/modified GUIs

Table 5 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Remote SIP Server	Changed
Config Data	Changed
Add NCAS Link	New
List NCAS Link	New
NCAS Link	New
Add VM Profile	New
List VM Profile	New

3.8.2 GUI information

3.8.2.1 GUI name: Remote SIP Server

Remote SIP Server

3.8.2.1.1 Functional description

A remote SIP Server is a remote SIP device that the Session Server Manager communicates with via the session initiation protocol. Two examples are other Call Server 2000s or a Multimedia Communication Server (MCS).

3.8.2.1.2 GUI usage and implications

SIP Gateway remote SIP server provisioning is performed by opening the "Remote SIP Server" folder in the left menu. Once there, the following may be performed:

- Remote SIP Server datafill may be added by clicking on the "Add Server" link.
- Remote SIP Servers may also be listed by clicking on "List Servers".
- After listing the Remote SIP servers, the user may choose to delete a particular remote SIP server or modify the data for a particular SIP server.

3.8.2.1.3 GUI size

Not Applicable.

3.8.2.1.4 GUI fields

Table 6 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Server Type	New		- Session Server - VRDN - Message Server - Select the Server Type	If the Server Type = Message Server, a SUBSCRIBE message will be sent out to the Remote Server.	
Auto Subscribe	New		Yes / No	If the Auto-Subscribe = 'Y', the Remote Server will be subscribed for accepting MWT notification.	

3.8.2.1.5 Usage example

Figure 1 Provisioning of Server Type on Remote SIP Server

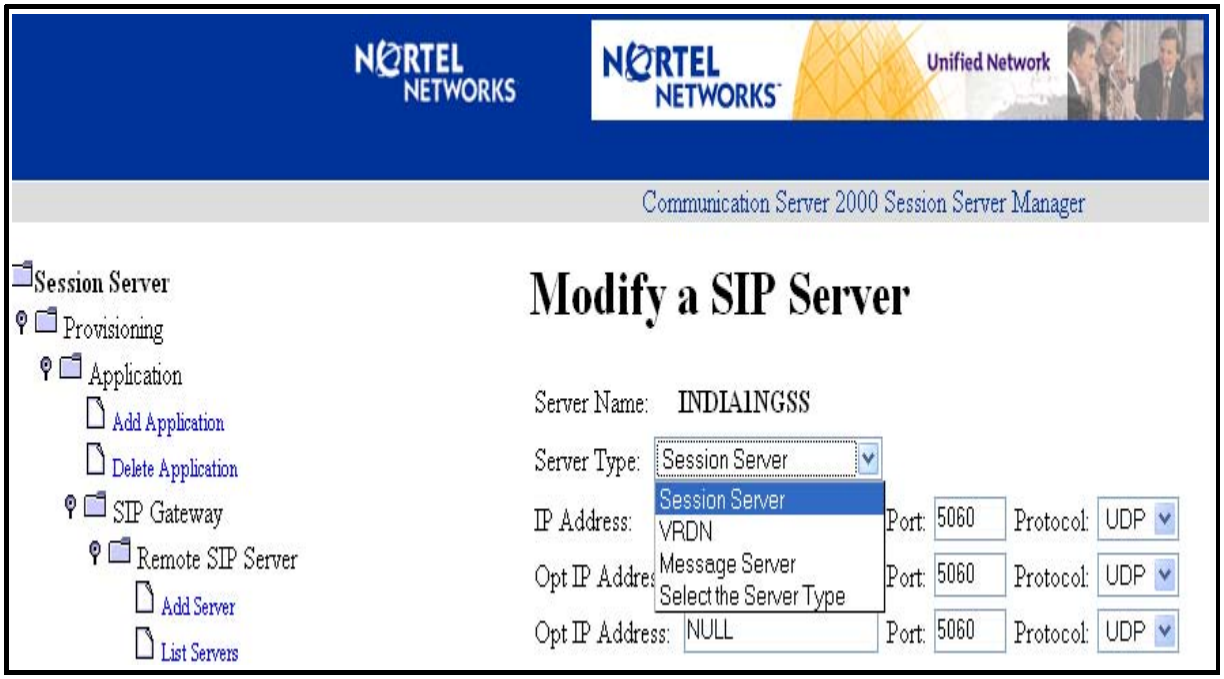
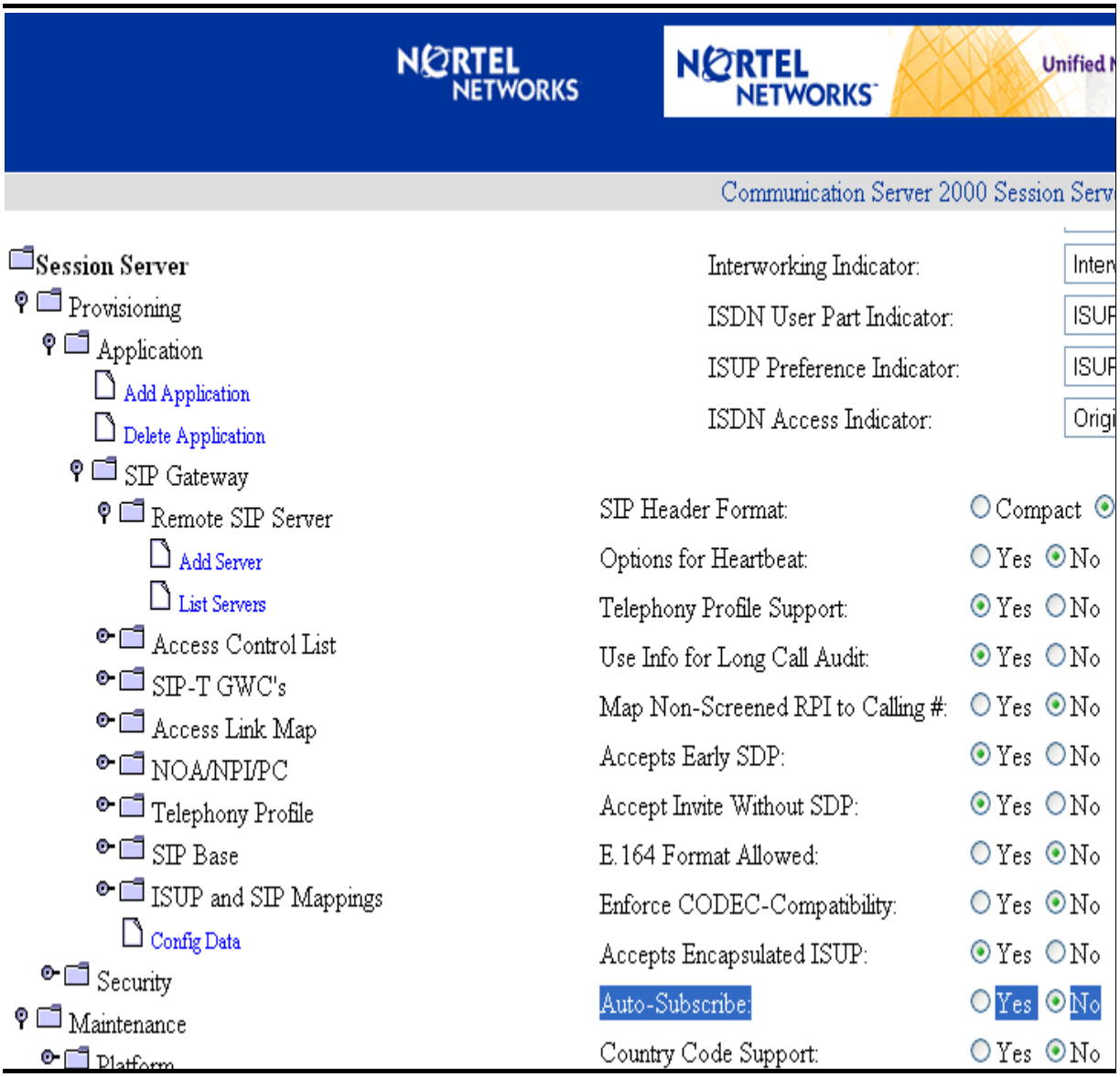


Figure 2 Provisioning of Auto-Subscribe on Remote SIP Server



3.8.2.1.6 GUI release history update

Not Applicable.

3.8.2.1.7 Context sensitive launching information

Not Applicable.

3.8.2.1.8 Supplementary information

Not Applicable.

3.8.2.2 GUI name: Config Data

Configurable Parameter

3.8.2.2.1 Functional description

Before the SIP Gateway application is brought into service, base configuration parameters should be modified to appropriate values.

While many parameters exist on the “Config Data” page, **care** must be taken when changing any of them.

3.8.2.2.2 GUI usage and implications

All the configurable parameters are found on the **Configurable Parameters** page. That page is reached from the Session Server Manager main page via:

- Click on the Provisioning folder
- Click on the Application folder
- Click on the SIP Gateway folder
- Click on **Config Data**

3.8.2.2.3 GUI size

Not Applicable.

3.8.2.2.4 GUI fields

Table 7 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
subsRetryTmr	New		Range 0 - 50000 milliseconds	If subsRetryTmr = 0, SUBSCRIBE will not be retried.	

3.8.2.2.5 Usage example

Figure 3 Provisioning of SubsRetryTimer on Session Server

3.8.2.2.6 GUI release history update

Not Applicable.

3.8.2.2.7 Context sensitive launching information

Not Applicable.

3.8.2.2.8 Supplementary information

Not Applicable.

3.8.2.3 GUI name: Add NCAS Link

Add NCAS Link

3.8.2.3.1 Functional description

This GUI allows the craft person to add NCAS link datafill for each application such as Message Waiting.

3.8.2.3.2 GUI usage and implications

This GUI is under provisioning, Application, NCAS Link. This GUI provide an interface to input appropriate IP Address and Port Number for each application such that the NGSS software can communicate with the CS2K Core software as a client.

3.8.2.3.3 GUI size
Not Applicable.

3.8.2.3.4 GUI fields

Table 8 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Application Name	New	Name of Supported Applications	Selection an Application	This field is for the application name associated with the NCAS Link. For the Message Waiting application, the name should be "Message Waiting" selected from drop down menu.	-
IP Address	New	None	NULL	This field is for the IP Address of the Core HIOP. This field takes the value of xx.xx.xx.xx. The example is "47.142.97.120".	-
Port Number	New	None	NULL	This field is for the Port number defined in Table IPAPPL in the Core. The port number should match, otherwise the link do not work.	-

3.8.2.3.5 Usage example

3.8.2.3.6 GUI release history update
Not Applicable.

3.8.2.3.7 Context sensitive launching information
Not Applicable.

3.8.2.3.8 Supplementary information
Not Applicable.

3.8.2.4 GUI name: List NCAS Link
List NCAS Link

3.8.2.4.1 Functional description

This GUI display currently datafilled NCAS Links on the NGSS.

3.8.2.4.2 GUI usage and implications

This GUI allows the query and display type functionality for the crafts person. It displays all the NCAS Link datafilled.

3.8.2.4.3 GUI size

Not Applicable.

3.8.2.4.4 GUI fields

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
IP Address	New	None	Datafilled IP Address	This field is the IP Address datafilled during the Add NCAS Link operation.	-
Port Number	New	None	Datafilled Port Number.	This field is the Port Number datafilled during the Add NCAS Link operation.	-
Link Name	New	None	Datafilled Application Name	This field is the Link Name. This field is the same value datafilled as Application Name in the Add NCAS Link operation.	-

Table 9 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
status	New	None	Current Status of the link	This field is the status of the link. There are three values: Stopped - The link is not connected and no communication exists. TryingToConnect - The link is not connected. The connection attempts are in progress. This state only come in following conditions: a) When link is datafilled in NGSS but not datafilled in the Table IPAPPL in CS2K Core. b) Maintenance activity is going on in the CS2K Core. c) The communication route has trouble such that no data can be passed between the NGSS and CS2K Core. Connected - The link is connected and the communication exists.	-

3.8.2.4.5 Usage example

3.8.2.4.6 GUI release history update

Not Applicable.

3.8.2.4.7 Context sensitive launching information

Not Applicable.

3.8.2.4.8 Supplementary information

Not Applicable.

3.8.2.5 GUI name: NCAS Link

NCAS Link

3.8.2.5.1 Functional description

3.8.2.5.2 GUI usage and implications

3.8.2.5.3 GUI size

Not Applicable.

3.8.2.5.4 GUI fields

Table 10 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
IP Address	New	None	Datafilled IP Address	This field is the IP Address datafilled during the Add NCAS Link operation.	-
Port Number	New	None	Datafilled Port Number.	This field is the Port Number datafilled during the Add NCAS Link operation.	-
Link Name	New	None	Datafilled Application Name	This field is the Link Name. This field is the same value datafilled as Application Name in the Add NCAS Link operation.	-

Table 10 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
status	New	None	Current Status of the link	This field is the status of the link. There are three values: Stopped - The link is not connected and no communication exists. TryingToConnect - The link is not connected. The connection attempts are in progress. This state only come in following conditions: a) When link is datafilled in NGSS but not datafilled in the Table IPAPPL in CS2K Core. b) Maintenance activity is going on in the CS2K Core. c) The communication route has trouble such that no data can be passed between the NGSS and CS2K Core. Connected - The link is connected and the communication exists.	-

Table 10 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
allowed operations	New	None	Selection by user	The buttons are displayed based on current status of the link. Stop button - This is visible when the link is in connected or TryingToConnect state. Basically this button press will stop the link from communication. Delete button - This is visible when the link is in Stopped state. When this button is pressed, it deletes the link. All associated data is removed from the database as well.	-

3.8.2.5.5 Usage example

3.8.2.5.6 GUI release history update

Not Applicable.

3.8.2.5.7 Context sensitive launching information

Not Applicable.

3.8.2.5.8 Supplementary information

Not Applicable.

3.8.2.6 GUI name: Add VM Profile

Add VM Profile

3.8.2.6.1 Functional description

3.8.2.6.2 GUI usage and implications

3.8.2.6.3 GUI size
Not Applicable.

3.8.2.6.4 GUI fields

Table 11 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Remote SIP Server	New	None	Selection	The drop down menu will show only remote SIP servers which are datafilled in the NGSS. This is the remote end were the SIP messages communicated.	-
Starting DN	New	None	DN up to 10 digits	This field allow the first DN to be supported for the remote SIP Server.	-
Ending DN	New	None	DN upto 10 digits	This field allows the last DN to be supported for the remote SIP server.	-

3.8.2.6.5 Usage example

3.8.2.6.6 GUI release history update
Not Applicable.

3.8.2.6.7 Context sensitive launching information
Not Applicable.

3.8.2.6.8 Supplementary information
Not Applicable.

3.8.2.7 GUI name: List VM profile
List VM Profile

3.8.2.7.1 Functional description

3.8.2.7.2 GUI usage and implications

3.8.2.7.3 GUI size
Not Applicable.

3.8.2.7.4 GUI fields

Table 12 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Remote SIP Server	New	None	Selection	The drop down menu will show only remote SIP servers which are datafilled in the NGSS. This is the remote end were the SIP messages communicated.	-
Starting DN	New	None	DN up to 10 digits	This field allow the first DN to be supported for the remote SIP Server.	-
Ending DN	New	None	DN upto 10 digits	This field allows the last DN to be supported for the remote SIP server.	-

3.8.2.7.5 Usage example

3.8.2.7.6 GUI release history update
Not Applicable.

3.8.2.7.7 Context sensitive launching information
Not Applicable.

3.8.2.7.8 Supplementary information
Not Applicable.

3.8.3 CLUI Interface
Not Applicable.

3.9 User interface changes
Not Applicable.

3.10 OSSGate Interface Changes
Not Applicable.

3.11 Security
Not Applicable.

3.12 Configuration Walkthrough
TBA based on the FN sections.

4: Performance for A00007544

4.1 Performance management strategy

The Operational Measurements will be pegged to generate the performance history. The details of performance management will be then developed as per engineering rules.

4.2 Performance management tools and utilities

The OMSHOW command and EADAS will be used for the OM display and OM transfer to remote system.

4.3 Performance Measurements (PM), Operational Measurements (OM), and stats

This feature does not have any specific PM. However, this feature introduces new OM groups in the DMS/CS2K Core and in the Session Server (NGSS).

4.3.1 PM, OM, and stats format

The OM in the NGSS and CORE follow the previously defined OM strategy and framework. The new group and appropriate fields are added. An existing OM group INSCTP is also pegged whenever necessary. The following are the details of the new OM groups and fields in the NGSS and DMS/CS2K Core.

4.3.1.1 OM Group NCAS_LINK (NGSS)

The New OM group called NCAS_LINK is introduced to keep a record of the state changes of the NCAS Link and the number of messages sent and received over the NCAS link.

This OM group accurately tracks the messages send and received on the NCAS link between CS2K Core and Session Server. The OM pegging will provide information on the message traffic between CS2K Core and Session Server. It will also have a count of the number of times the NCAS Link has gone down and come up.

4.3.1.2 Release history update

Added new in this release.

4.3.1.3 Registers

The following table gives an overview of the registers associated with the NCAS_LINK OM group.

Table 1 OM Registers in the NCAS_LINK OM Group

OM field	Description
NUM_LINK_UP	Number of times the NCAS Link is brought up
NUM_LINK_DOWN	Number of times the link goes down

OM field	Description
NUM_MSG_SENT	Number of messages sent over the NCAS Link
NUM_MSG_RCVD	Number of times a response is received over the NCAS Link
NUM_MSG_SEND_FAIL	Number of times the message send fails
NUM_MSG_RCV_FAIL	Number of times the message receive fails.

The following figure will be updated during coding.

OM group registers displayed are as follows:

Figure 1 OM Group Display

<regName> <regName> <regName> <regName>

4.3.1.4 Group Structure

OM group provides one tuple for each NCAS selector datafilled in Table MSGRTE.
Key field: <KField><description> TBA

Info field: <IField><description> TBA

4.3.1.5 Associated OM groups

None

4.3.1.6 Associated functional groups

The following functional groups are associated with OM group: None

4.3.1.7 Associated functionality codes

Not Applicable

4.3.1.8 OM group registers logic flow chart

TBA

4.3.2 Register NUM_LINK_UP

4.3.2.1 Register description

This register represents how many times the NCAS Link has been brought up.

4.3.2.2 Register release history update
New in this release

4.3.2.3 Associated registers

4.3.2.4 Associated logs
TBA

4.3.3 Register NUM_LINK_DOWN

4.3.3.1 Register description
This register represents how many times the NCAS Link has gone down.

4.3.3.2 Register release history update
New in this release

4.3.3.3 Associated registers

4.3.3.4 Associated Logs
TBA

4.3.4 Register NUM_MSG_SENT

4.3.4.1 Register description
This register represents how many times the a message is successfully sent over the NCAS Link.

4.3.4.2 Register release history update
New in this release

4.3.4.3 Associated registers
None

4.3.4.4 Associated logs
None

4.3.5 Register NUM_MSG_RCVD

4.3.5.1 Register description
This register represents how many times responses are successfully received over the NCAS Link .

4.3.5.2 Register release history update
New in this release

4.3.5.3 Associated registers
None.

4.3.5.4 Associated logs
None.

4.3.6 Register NUM_MSG_SEND_FAIL

4.3.6.1 Register description
This register represents how many times the message sent over the NCAS Link has failed

4.3.6.2 Register release history update
New in this release

4.3.6.3 Associated registers
None.

4.3.6.4 Associated logs
None

4.3.7 Register NUM_MSG_RCV_FAIL

4.3.7.1 Register description
This register represents how many times the a message receive over an NCAS Link has failed.

4.3.7.2 Register release history update
New in this release

4.3.7.3 Associated registers
None.

4.3.7.4 Associated logs
None

4.3.8 Performance File (CSV, SSV, XML) Format
The NGSS performance file format is used.

4.3.9 OM Group NMSNCAS (For CS2K Core only)

4.3.9.1 OM description
The New OM group called NMSNCAS is introduced to keep a record of the NMS messages sent and received by the CS2K Core over NCAS link. This OM group accurately tracks the messages sent and received on the NCAS link between CS2K Core and Session Server. The OM pegging will provide information on the message traffic between CS2K Core and Session Server.

4.3.9.2 Release history update

Added new in this release.

4.3.9.3 Registers

The following table gives an overview of the registers associated with the NMSNCAS OM group.

Table 2 OM Registers in the NMSNCAS OM Group

OM field	Description
SCTPNMSS	NMS TCAP messages sent successfully over SCTP
SCTPNMSR	NMS TCAP messages received successfully over SCTP
SCTPREJS	NMS REJ messages sent successfully over SCTP
SCTPREJR	NMS REJ messages receievd successfully over SCTP

The following figure will be updated during coding.

OM group registers display on the MAP terminal as follows:

Figure 2 OM Group Display

<regName> <regName> <regName> <regName>

4.3.9.4 Group structure

OM group provides one tuple for each NCAS selector datafilled in Table MSGRTE.

Key field: <KField><description> TBA

Info field: <IField><description> TBA

4.3.9.5 Associated OM groups

None.

4.3.9.6 Associated functional groups

None

4.3.9.7 Associated functionality codes

Not Applicable

4.3.9.8 OM group registers logic flow chart

TBA

4.3.10 Register SCTPNMSS (applies only to DMS)

4.3.10.1 Register description

This register represents how many NMS TCAP messages are sent to SCTP in half hour time period. This will provide information of performance needs for the NCAS link.

4.3.10.2 Register release history update

New in this release

4.3.10.3 Associated registers

None.

4.3.10.4 Associated logs

NMSS115.

4.3.11 Register SCTPNMSR (applies only to DMS)

4.3.11.1 Register description

This register represents how many NMS TCAP messages are received from SCTP in half hour time period.This will provide information of performance needs for the NCAS link.

4.3.11.2 Register release history update

New in this release

4.3.11.3 Associated registers

None.

4.3.11.4 Associated logs

NMSS116

4.3.12 Register SCTPREJS (applies only to DMS)

4.3.12.1 Register description

This register represents how many NMS REJECT messages are sent to SCTP in half hour time period.

4.3.12.2 Register release history update

New in this release.

4.3.12.3 Associated registers

None

4.3.12.4 Associated logs
NMSS117

4.3.13 Register SCTPREJR (applies only to DMS)

4.3.13.1 Register description
This register represents how many NMS REJECT messages are received from SCTP in half hour time period.

4.3.13.2 Register release history update
New in this release.

4.3.13.3 Associated registers
None

4.3.13.4 Associated logs
NMS118

4.3.14 OM Group INSCTP (For CS2K Core only)
This is an existing OM Group defined for AIN Transports. The OMs pegged for this OM Group are as follows:

- **MSGOUT:** Pegs Outgoing IN messages using SCTP
- **MSGIN:** Pegs Incoming IN messages using SCTP
- **SDFAIL:** Pegs IN messages using SCTP for which send failed
- **DATAERR:** Pegs IN messaageswhich encounted errors at application data
- **MSG2BIG:** Pegs IN messages which failed due to message length
- **BMSOPFAIL:** Peg instances when buffer errors are encountered while sending IN messages over SCTP
- **DATARCVD:** Pegs for incoming IN message decoding
- **NOTREADY:** Pegs when SCTP layer indicates that it is not ready to process the message.

Please refer to A00004500 for further information.

Product = CS 2000

A00007547--SIP Lines Core Call Processing Support

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

This activity provides initial CS2K support for SIP (Session Initiation Protocol) lines basic call for SIP agents that interface to the CS2K via the GWC and Phoenix. This includes the following components:

- Support for multiple call appearances for DPL lines
- CS2K call processing support for SIP basic call including signalling interface with the TPT in the GWC.

1.1.1 Multiple Call Appearances

Support for multiple call appearances relies on a new pool of resources (virtual terminal identifiers). This new pool has OMs and logs associated with it.

The new OM group DPLOM, has registers:

- DPLFNVA, DPLFBAL, DPLFREB, DPLRLOS
- DPLRCAL, DPLUSE, DPLFRE, DPLNOA, DPLNOD

DPL logs: DPL100, DPL101

The remainder of this section explains the rationale for these items and how they will be used when multiple call appearances are supported for SIP lines on the CS2K.

SIP allows devices to make multiple simultaneous call attempts, and actively engage in multiple simultaneous calls. The maximum number of such calls will be limited on a per-line basis, as part of the DPL SERVORD option, as described in feature A00008556. In order for the CS2K to handle these lines in a manner that preserves the way various line options work (as much as possible) and that makes efficient use of CS2K resources, a new resource pool is created. This section describes the resource pool and how it is controlled and monitored.

The new resource pool consists of “virtual terminal identifiers” (VIDs). VIDs are an existing resource on the CS2K. One VID is required for each appearance of a SIP line in a CS2K call. The pool will be sized to the total of the maximum call appearances of all DPL lines (from the DPL SERVORD option) but

capped at twice the maximum number of simultaneous calls (existing office parameter NCCBS in OFCENG).

1.1.1.1 Resource pool monitoring

There is a new OM group (DPLOM) defined that contains pegs and usage measurements of the resource pool. The registers are:

- DPLUSE - usage register (100 sec sampling, with extension register) that tracks the number of VIDs in use by call processing
- DPLFRE - usage register (100 sec sampling, with extension register) that tracks the number of VIDs on the resource pool free list.
- DPLNOA - peg register (with extension) that indicates the number of allocations from the resource pool.
- DPLNOD - peg register (with extension) that indicates the number of deallocations to the resource pool.
- DPLFNVA - peg register that indicates the number of times that a failure to allocate a VID happened because the resource pool free list was empty.
- DPLFBAL - peg register that indicates the number of times that a failure to allocate a VID happened because the resource pool free list was unavailable due to rebalancing (part of the rebuild process).
- DPLFREB - peg register that indicates the number of times that a failure to deallocate a VID happened (resulting in a “lost” VID) because the resource pool free list was being rebuilt.
- DPLRLOS - peg register that indicates the number of “lost” VIDs that were recovered.
- DPLRCAL - peg register that indicates the number of VIDs that were in use by call processing, but were not returned to the resource pool free list.

1.1.1.2 Resource pool recovery

As with any resource pool, there are recovery mechanisms. There is an audit which will recover “stranded” VIDs, that is, VIDs which are no longer in use, but have not been returned to resource pool free list. There is also a mechanism which detects corruption in the resource pool free list, and reconstructs it. A log will be output at the beginning of that reconstruction, and another at the end (DPL100 and DPL101, respectively).

1.1.2 Call Processing

The call processing component of this feature has very little customer visible impact to functionality. From the CS2K’s perspective, calls to and from DPL lines will function in the same manner that calls to and from standard IBN or RES lines function. Other than the VID allocation described in the previous section, the CS2K will provide very little indication that the end user is in fact a SIP client.

The entire call progresses as a typical IBN or RES line call would progress. This will include any standard OMs and logs that apply to IBN and RES lines. Additional OMs and logs related to the DPL VIDs may be produced as described in the previous section.

The main exception to the IBN/RES call processing model is the fact that the DPL SIP line can have multiple call sessions active at any given time. This introduces 2 new concepts: 1) A maximum number of call appearances per DPL line can be defined, and 2) The presence of certain options on the line can dictate whether or not multiple terminations are allowed when the line is "busy".

1.1.2.1 Maximum Call Appearances

Each DPL SIP line defined in the core will be provisioned with a suboption called MAX_CALL_APPEARANCES. (See A00008556 for more information on provisioning the DPL line.) MAX_CALL_APPEARANCES will define the total number of VIDs that can be allocated for the line. Therefore, the total number of incoming and outgoing calls that involve the DPL line cannot exceed the value of MAX_CALL_APPEARANCES for that line.

Once the call appearance limit has been reached, any incoming call attempts will receive BUSY treatment, and any outgoing call attempts will receive NOSR (No Software Resources) treatment.

1.1.2.2 Allow Busy Terminations

The ability of a DPL line to have multiple active call sessions introduces some interaction problems with common CS2K features. For example, standard call waiting has no useful purpose if multiple calls can already be terminated on a DPL line.

To solve this problem, the concept of ALLOW_BUSY_TERMINATIONS is introduced. ALLOW_BUSY_TERMINATIONS is an internal bool that will be stored for every DPL line in the CS2K.

When the bool is set to N, incoming calls will not be presented to the DPL line if there is already at least one active call in progress. These calls will receive BUSY treatment instead. When the bool is set to Y, the only restriction on incoming calls being presented to the DPL line is the value of MAX_CALL_APPEARANCES.

Outgoing calls originated by the DPL line will not be restricted by the ALLOW_BUSY_TERMINATIONS bool at all.

ALLOW_BUSY_TERMINATIONS is not intended to be a provisionable value. It will be stored internally, and altered based on the addition or removal of certain options on the DPL line. For example: Initially the bool will be set

to N, meaning that if one call is active, all subsequent incoming calls will receive busy treatment. The addition of the CWT option on the DPL line will cause the system to flip the internal bool to Y, and thus additional call terminations will be allowed as per the CWT feature function.

1.2 Hardware Requirements or Dependencies

1.3 Software Requirements or Dependencies

1.4 Limitations and restrictions

The DPL option will only be assignable to IBN and RES LCCs.

1.5 Interactions

Keyset and ISDN lines also make use of VIDs, but do so strictly based on provisioning. VIDs used for keyset and ISDN lines are separate from VIDs used in the resource pool defined by this activity. Thus, provisioning of keyset and ISDN lines will decrease the number of VIDs available for the resource pool defined by this activity, and vice versa.

1.6 Glossary

Acronym	Description
ACD	Automatic Call Distribution
CS2K	Call Server 2000
DPL	Dynamic Packet Line
GWC	Gateway Controller
IBN	Integrated Business Network Line Type
ISDN	Integrated Services Digital Network
MADN	Multiple Appearance Directory Number
RES	Residential Line Type
SCMP	Series Completion
SIP	Session Initiation Protocol
VID	Virtual Identifier

1.7 Applicable customer facing sections.

Fault Management

Logs	__X__
Alarms	_N/A_

Configuration

Data Schema _N/A_

User Interface _N/A_

Element Management _N/A_

Security _N/A_

Service Order _N/A_

Office Parameters _N/A_

Accounting (includes AMA billing) _N/A_

Performance (includes operational measurements) __X__

2: Fault Management for A00007547

2.1 Fault management strategy

Logs are used for fault management.

2.2 Fault management tools and utilities

Not applicable

2.2.1 Faults, Alarms and Logs

2.2.2 Logs

DPL100

DPL101

2.2.3 Formats

2.2.3.1 NTSTD

Examples:

RTPF08BZ DPL100 SEP21 07:30:32 0301 INFO DPL FREE QUEUE REBUILD START

RTPF08BZ DPL101 SEP21 07:30:33 0302 INFO DPL FREE QUEUE REBUILD FINISH

There is no variable text in the log body in all these logs

2.2.3.2 SCC2

2.2.3.3 Syslog

2.2.3.4 SNMP

3: Performance Management for A00007547

3.1 Performance management strategy

3.2 Performance management tools and utilities

3.3 Performance Measurements (PM), Operational Measurements (OM), and stats

New OM group DPLOM.

Registers:

- DPLFNVA
- DPLFBAL
- DPLFREB
- DPLRLOS
- DPLRCAL
- DPLUSE
- DPLFRE
- DPLNOA
- DPLNOD

3.3.0.1 OM description

OM Group DPLOM - Dynamic Packet Line OM

3.3.0.2 Release history update

Creation of new group DPLOM

3.3.0.3 Registers

OM group registers display on the MAP terminal as follows:

Figure 1 OM Group Display

DPLFNVA	DPLFBAL	DPLFREB	DPLRLOS
DPLCAL	DPLUSE	DPLUSE2	DPLFRE
DPLFRE2	DPLNOA	DPLNOA2	DPLNOD
DPLNOD2			

3.3.0.4 Group structure

OM group provides 1 tuple for the CS2K.

Key field: None

Info field: None

3.3.0.5 Associated OM groups
<None>

3.3.0.6 Associated functional groups
<None>

3.3.0.7 OM group registers logic flow chart

3.3.1 Register DPLFNVA

3.3.1.1 Register description
Register DPLFNVA

Dynamic Packet Line Failed Allocation due to No VIDs Available.

DPLFNVA is a peg register. It records the number of times that a call failed to allocate a VID from the DPL VID resource because the free list was empty

3.3.1.2 Register release history update
Initial creation

3.3.1.3 Associated registers
<None>

3.3.1.4 Associated logs
<None>

3.3.2 Register DPLFBAL

3.3.2.1 Register description
Register DPLFBAL

Dynamic Packet Line Failed Allocation due to Queue Balancing

DPLFBAL is a peg register. It records the number of times that a call failed to allocate a VID from the DPL VID resource because the free list was being balanced

3.3.2.2 Register release history update
Initial creation

3.3.2.3 Associated registers
<None>

3.3.2.4 Associated logs
<None>

3.3.3 Register DPLFREB

3.3.3.1 Register description
Register DPLFREB

Dynamic Packet Line Failed Deallocation due to Queue Rebuilding.

DPLFREB is a peg register. It records the number of times that a call failed to return a VID to the DPL VID resource because the free list was being rebuilt.

3.3.3.2 Register release history update
Initial creation

3.3.3.3 Associated registers
<None>

3.3.3.4 Associated logs
<None>

3.3.4 Register DPLRLOS

3.3.4.1 Register description
Register DPLRLOS

Dynamic Packet Line Recover Lost

DPLRLOS is a peg register. It records the number of VIDs that were recovered and put back on the resource pool free list when a call failed to return a VID to the DPL VID resource pool free list because the free list was being rebuilt.

3.3.4.2 Register release history update
Initial creation

3.3.4.3 Associated registers
<None>

3.3.4.4 Associated logs
<None>

3.3.5 Register DPLRCAL

3.3.5.1 Register description
Register DPLRCAL

Dynamic Packet Line Recover Call VID.

DPLRCAL is a peg register. It records the number of VIDs that were recovered and put back on the resource pool free list when a call failed to return a VID to the DPL VID resource pool free list because the call terminated abnormally.

3.3.5.2 Register release history update
Initial creation

3.3.5.3 Associated registers
<None>

3.3.5.4 Associated logs
<None>

3.3.6 Register DPLUSE

3.3.6.1 Register description
Register DPLUSE

Dynamic Packet Line Usage.

DPLUSE is a usage register. The scan rate is slow: 100s. It records the number of VIDs allocated from the DPL VID resource pool.

3.3.6.2 Register release history update
Initial creation

3.3.6.3 Associated registers
<None>

3.3.6.4 Associated logs
<None>

3.3.7 Register DPLFRE

3.3.7.1 Register description
Register DPLFRE

Dynamic Packet Line Free.

DPLFRE is a usage register.The scan rate is slow: 100s. It records the size of the DPL VID resource pool free list.

3.3.7.2 Register release history update
Initial creation

3.3.7.3 Associated registers
<None>

3.3.7.4 Associated logs
<None>

3.3.8 Register DPLNOA

3.3.8.1 Register description
Register DPLNOA

Dynamic Packet Line Number Of Allocations.

DPLNOA is a peg register. It records the number of times that a call successful allocations from the DPL VID resource pool

3.3.8.2 Register release history update
Initial creation

3.3.8.3 Associated registers
<None>

3.3.8.4 Associated logs
<None>

3.3.9 Register DPLNOD

3.3.9.1 Register description
Register DPLNOD

Dynamic Packet Line Number Of Deallocations.

DPLNOD is a peg register. It records the number of times that a call successfully returned a VID to the DPL VID resource pool

3.3.9.2 Register release history update
Initial creation

3.3.9.3 Associated registers
<None>

3.3.9.4 Associated logs

<None>

Product = CS 2000

A00008043 -- CS2K Support for 64 Character FQDN

Functional Description

1: Applicable Solution(s)

IAC

1.1 Description

Please refer to the FN under actid A00009189: SESM Support for 64 Character FQDN under the CS 2000 Management Tools section of this document.

Product = CS 2000

A00008090 -- SBA: Alternate Scheduled Closure of Billing Files

Functional Description

1: Applicable Solution(s)

PT-AAL1

1.1 Description

This feature facilitates the closure of billing files at the scheduled Interval as specified in the Stream Configuration and provides an additional functionality of Resetting the DIRP Billing File sequence number at Midnight. This feature does not impact the existing functionality of file closure based on time and other mechanisms like file closure based on file size or number of records in a file.

With this feature, all the open billing files are rotated exactly at scheduled interval without any drift or delay. Irrespective of the opening time of the billing File, the closure will take place at the exact scheduled interval. For e.g. if the scheduled interval for the ‘ Scheduled File Closure time options’ is ‘6 Hour’ then for the time frame 00:00 to 06:00,all the billing files which are in the open state will get closed at 06:00. In the time frame 06:00 to 12:00, all the billing files which are in the open state will get closed at 12:00. Similarly next file closure will be at 18:00 and 00:00 respectively.

If the billing files are closed by any other criteria such as BSY of SBA or issue of 'closec', prior to the scheduled rotation then additional file rotation occurs without impacting the scheduled closure of the next file. In the above example suppose that a closec command is issued for the scheduled stream at 04:00, but still the next file closure will happen at 06:00, if any open file exists.

This feature is introducing a new option in the Stream Configuration to schedule closure of billing files without any drift or delay. This option is mutually exclusive with the option of 'Files Closure based on a time limit' which means users can only turn on either 'Files closed at scheduled intervals from midnight' or 'Files Closure based on a time limit', but not both.

The functionality of file closure at scheduled intervals from midnight can be enabled at the time of configuring a Stream or at the time of changing the configuration of an existing stream. In the latter case, the functionality will be activated only for the billing files which are opened after enabling the functionality. Bsy/Rts of SBA application is not required to activate this functionality.

Following are the Options for the file closure of billing files at scheduled intervals from midnight.

1) Close billing files every 24 hours

2) Close billing files every 12 hours

3) Close billing files every 6 hours

4) Close billing files every 2 hours

5) Close billing files every 1 hour (Default Schedule Time)

6) Close billing files every 30 minutes

7) Close billing files every 15 minutes

7) Close billing files every 10 minutes

8) Close billing files every 5 minutes

Reset DIRP Sequence Number at Midnight:
This feature provides a facility to reset the DIRP Billing File sequence number at midnight. The first DIRP billing file which is opened after midnight (00:00 Hr) will have a sequence number 00, if there is no other file exists with the same name. If the same filename exists then increment the sequence number and rename the file with that Sequence Number.

This is introducing a new option in the Stream Configuration to enable the functionality of 'Reset DIRP Sequence Number at Midnight'. This option is mutually exclusive with the option of 'Files renamed with close date' which means users can only turn on either 'Files renamed with close date' or 'Reset DIRP Sequence Number at Midnight', but not both.

1.1.1 Desired Behavior of 'file closure based at scheduled intervals from midnight' with Respect to the Daylight Saving Time:

Since the proposed design uses RWTime, the 'file closed based at scheduled intervals from midnight' behaves in the similar way which is explained below with the help of an example.

Note: In the below examples consider that files are not closed by any other criteria such as BSY of SBA or closing the file with the command 'closec' or any other criteria other than the scheduled rotation.

Considering the US/Eastern TimeZone .

CASE1: On 04 April 2004, when Time Changes from 01:59:59 -> 03:00 (Time changes from EST to EDT)

Scheduled Interval : 05:00 Mins

SBA closes the file at intervals 00:05 hr, 00:10 hr,...,01:50 hr,01:55 hr(EST),03:00 hr(EDT),03:05 hr(EDT),...,23:50 hr,23:55 hr,00:00 hr.

Scheduled Interval : 10:00 Mins

SBA closes the file at intervals 00:10 hr, 00:20 hr,...,01:40 hr,01:50 hr(EST),03:00 hr(EDT),03:10 hr(EDT),...,23:40 hr,23:50 hr,00:00 hr.

Scheduled Interval : 15:00 Mins

SBA closes the file at intervals 00:15 hr, 00:30 hr,...,01:30 hr,01:45 hr(EST),03:00 hr(EDT),03:15 hr(EDT),...,23:30 hr,23:45 hr,00:00 hr.

Scheduled Interval : 30:00 Mins

SBA closes the file at intervals 00:30 hr, 01:00 hr,01:30 hr (EST),03:00 hr(EDT),03:30 hr(EDT),...,23:00 hr,23:30 hr,00:00 hr.

Scheduled Interval : 01:00 Hrs

SBA closes the file at intervals 01:00 hr(EST),03:00 hr(EDT),04:00 hr(EDT),...,22:00 hr,23:00 hr,00:00 hr.

Scheduled Interval : 02:00 Hrs

SBA closes the file at regular intervals 03:00 hr (EDT), 04:00 hr (EDT),06:00 hr,...,20:00 hr,22:00 hr,00:00 hr.

Scheduled Interval : 06:00 Hrs

SBA closes the file at intervals 07:00 hr (EDT), 12:00 hr ,18:00 hr,00:00 hr

Scheduled Interval : 12:00 Hrs

SBA closes the file at intervals 13:00 hr (EDT) and 00:00 hr

Scheduled Interval : 24:00 Hrs

SBA closes the file on April 5 2004(next day) at 01:00 hr and 00:00 hr

CASE 2: On 31 October 2004, when Time Changes from 01:59:59 -> 01:00 (Time changes from EDT to EST)

Scheduled Interval : 05:00 Mins

SBA closes the file at intervals 00:05 hr, 00:10 hr,...,01:50 hr,01:55 hr(EDT),01:00 hr(EST),01:05 hr(EST),...,23:50 hr,23:55 hr,00:00 hr

Scheduled Interval : 10:00 Mins

SBA closes the file at intervals 00:10 hr, 00:20 hr,...,01:40 hr,01:50 hr(EDT),01:00 hr(EST),01:10 hr(EST),...,23:40 hr,23:50 hr,00:00 hr.

Scheduled Interval : 15:00 Mins

SBA closes the file at intervals 00:15 hr, 00:30 hr,...,01:30 hr,01:45 hr(EDT),01:00 hr(EST),01:15 hr(EST),...,23:30 hr,23:45 hr,00:00 hr.

Scheduled Interval : 30:00 Mins

SBA closes the file at intervals 00:30 hr, 01:00 hr,01:30 hr (EDT),01:00 hr(EST),01:30 hr(EST),...,23:00 hr,23:30 hr,00:00 hr.

Scheduled Interval : 01:00 Hrs

SBA closes the file at intervals 01:00 hr(EDT),01:00 hr(EST),02:00 hr(EST),...,22:00 hr,23:00 hr,00:00 hr.

Scheduled Interval : 02:00 Hrs

SBA closes the file at intervals 01:00 hr (EST), 02:00 hr (EST),04:00 hr,...,20:00 hr,22:00 hr,00:00 hr.

Scheduled Interval : 06:00 Hrs

SBA closes the file at intervals 05:00 hr (EST), 06:00 hr ,12:00 hr,18:00 hr,00:00 hr

Scheduled Interval : 12:00 Hrs

SBA closes the file at regular 11:00 hr (EST) 12:00 hr and 00:00 h**r**

Scheduled Interval : 24:00 Hrs

SBA closes the file on 31st October 2004 at 23:00 hr and 00:00 hr

1.1.2 Desired Behavior of 'Reset DIRP Sequence Number at Midnight' with Respect to the Daylight Saving Time:

The functionality 'Reset DIRP Sequence Number at Midnight' does not have any impact if the time changes is happening in the same day. But if the time changes happens across the day following is the behavior.

for e.g. consider

CASE1: On 04 April 2004, suppose Time Changes from 22:59:59 -> 00:00 (Time changes from EST to EDT)

The resetting of DIRP Sequence number will happen when the new billing file opens on April 05 2004 after 00:00 hr.

CASE 2: On 31 October 2004, suppose Time Changes from 00:29:59 -> 23:30 (Time changes from EDT to EST)

In this case, resetting of DIRP sequence number will not happen again when the time changes from Oct 30 midnight(23:59 EST) to (00:00)Oct 31 , since the previously set date in Mib was of October 31.

i.e. The reset of DIRP Sequence number will occur only if current Date is greater than the date which was set in the Mib.

1.2 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature

1.3 Software Requirements or Dependencies

None

1.4 Limitations and restrictions

- The option of 'Files closed at scheduled intervals from midnight' is mutually exclusive to the existing option of 'Files Closed based on a time limit'
- The Option of 'Reset DIRP Sequence Number at Midnight' is mutually exclusive to the existing option of 'Files renamed with close date'.
- This feature supports only Scheduled Rotation as '24 Hours','12 Hours','6 Hours','2 Hours','1 Hour','30 Minutes','15 Minutes', '10 Minutes' and'5 Minutes'
- If there are large numbers of billing files, then the file closure may get delayed since the OS not Real time
- File Closure may get delayed when SBAStreams is busy writing the billing records to the disk
- Billing File name does not guarantee that all the records are in line with the file closure time, in the event of any delay in transferring the call records from core to SBA
- During the event of BSY of SBA, prior to the scheduled closure of billing files all the open files will get closed.
- During Daylight Saving Time, the file closure does not happen at the exact schedule time.
- If the functionality is enabled by using Change command from CONFSTRM then the functionality will be activated only for the newly opened Files

1.5 Interactions

None

1.6 Glossary

Term	Description
SDM	Supernode Data Manager
CBM	Core & Billing Manager
SBA	SDM/CBM billing application
DIRP	Device Independent Recording Package (File format used by SBA to store billing records based on the DIRP billing file format on the DMS core)

Product = CS 2000

A00008556--SIP Lines Core OAMP Support

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

The provisioning of DPL agents affects three major network components, the CS2K core, GWC, and CS2K Session Server(CS2KSS). Each of these components have their own specific provisioning requirements and each are provisioned via the appropriate application within SESM. The relationships between these components and SESM are shown in Figure 1 DPL Provisioning Component Overview below.

As part of this overview, the basic steps required to provision DPLs across the different components is included below. These steps are included here for context and intended only as a guide.

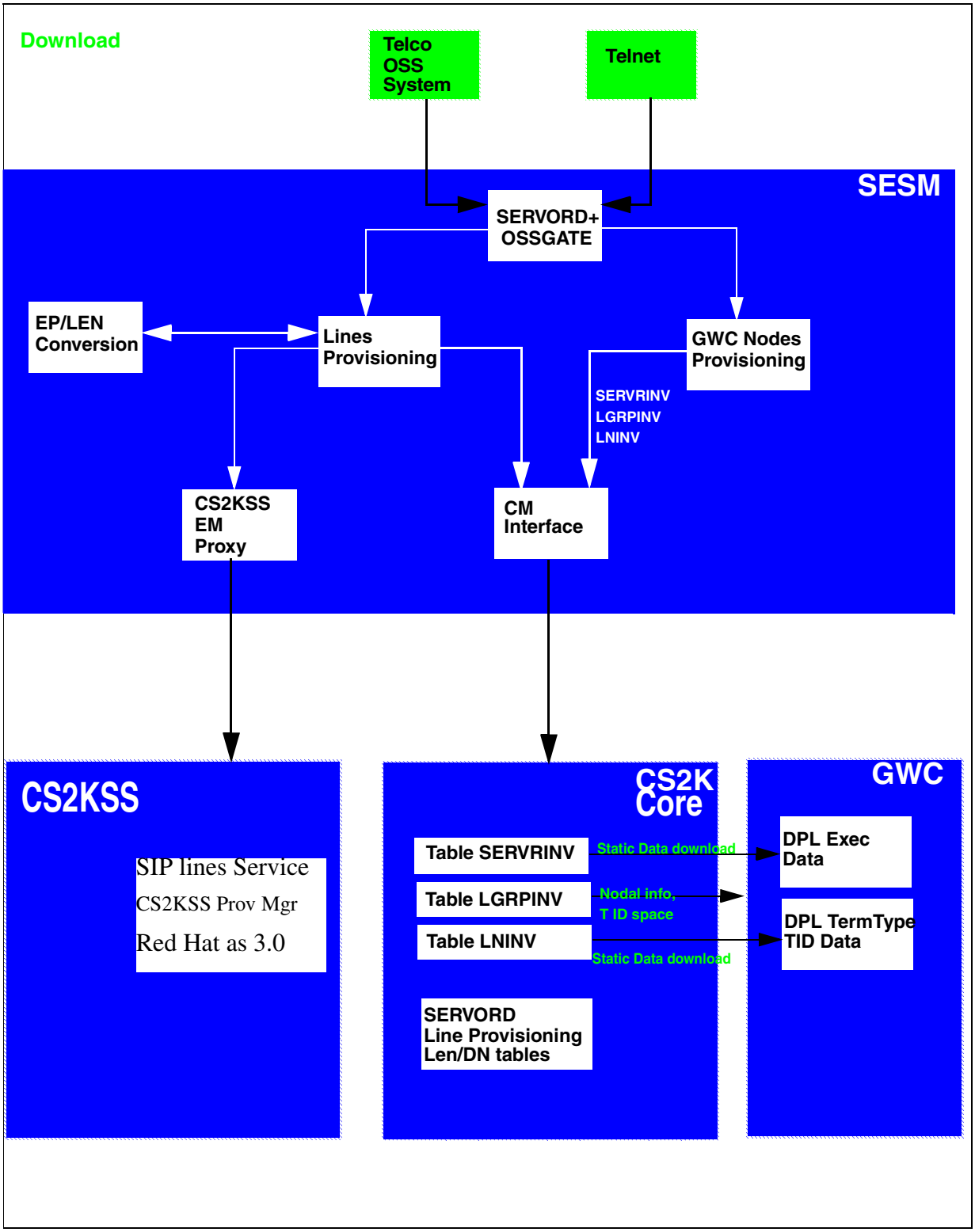
- Install the CS2KSS and activate DPL lines application CS2KSS.
- Configure commissioning data on CS2KSS using CS2KSS EM.
- Use SESM Provisioning GUI to “ADD GWC NODE” with the following details.
  - — Select the GWC profile ‘DPL’ signifying the GWC supporting DPL agents.
  - — Select Term type of DPL_TERM.
  - — Select Exec Data of DPLEX.
  - — The CM interface will subsequently add the GWC to table SERVRINV with DPLEX exec lineup and DPL_TERM term_type.
  - — Table SERVRINV ADD tuple will subsequently cause a static data download of DPLEX execs to the GWC.
  - — The GWC Configuration Manager will configure the GWC as a ‘DPL’ type GWC with DPLSupported GCM parameter set to TRUE.
- Use SESM Provisioning GUI to “ASSOCIATE Media Gateway”, the CS2KSS GW.
  - — Enter GW name, GW IP, and GWC to host GW.
  - — Select Gateway Profile Name of CS2KSS.
  - — Enter number of Reserved Terminations in multiples of 1023 up to a maximum value of 6138.

- Select the Gateway SITE name as previously provisioned in table SITE in the CS2K Core, and which must be unique for each CS2KSS GW added.
- Signalling protocol type will default to GCP.
- Enter protocol port and version.
- The CS2KSS EM proxy in SESM proxies this GW data to the CS2KSS which uses this data to identify new CS2KSS instances and provisions DPL agent data as required.
- The CM interface in SESM will cause provisioning to occur in the CS2K core table LGRPINV and table LNINV. An LGRP will be created for each increment of 1023 reserved terminations. 1023 tuples will be added to table LNINV for each LGRP added in LGRPINV.
- When the DPL line tuples are added to LNINV, static data is downloaded to the GWC for each terminal including the term type of DPL per TID.
- The GWC EM in SESM will cause the CS2KSS gateway to be registered as a ‘D’ type GW in the GWC with an CS2KSS lines profile name and a protocol of GCP.
- The GWC EM in SESM will cause the addition of endpoint groups for each 1023 endpoints on the CS2KSS GW in the GWC.
- The GWNAME will consist of up to 32 chars.
- The EPids added will have the format of SITE_Name/<0-511></0-9>/<0000-1022> E.g SIPVMG1.tampa.vz.com TMP1/000/2/0478

• Use Telco OSS or Telnet to perform SERVORD+ line provisioning via SESM.

- CS2KSS EM within SESM will proxy CS2KSS to provision user data in CS2KSS system.
- CM Interface within SESM will proxy the CS2K core to perform Servord line provisioning.
- Either LEN format or Gateway name and EPid combination will be accepted.

Figure 1 DPL Provisioning Component Overview



This activity focuses on the CORE OAMP(Operation, Administration, Maintenance & Provisioning) portion of the overall SIP feature. The components in this activity are as follows:

- GWC Provisioning.
- CS2KSS-GWC Association.
- DPL Lines Provisioning.
- Journal File.
- NCAS Link Provisioning.
- Core Maintenance support.
- Tool support
- SOC support (Refer to the CN section).
- NCAS Link Logs (Refer to the FM section).

1.1.1 GWC provisioning:

The GWC is commissioned through the SESM. The core stores information about this commissioned GWC in the table SERVRINV. The SIP feature deals with supporting new type of agent called dynamic packet line on the GWC.

- A new term_type DPL_TERM and a new exec_lineup called DPLEX are defined for supporting the DPL agents on the GWC. The new definitions DPL_TERM and DPLEX are passed onto the core along with the GWC information when the GWC is commissioned.
- On the core side, the table SERVRINV is enhanced so that it can accept these new definitions. When the GWC is commissioned, a tuple similar to the below one is expected to be datafilled in the table SERVRINV automatically:

Table SERVRINV:

SRVRNAME SRVRADDR **SRVREXEC** SRVRTONE BEARNETS SRVROPTS
GWC 0 IP 45 46 47 48 **(DPL_TERM DPLEX)**$ NORTHAA (NET_IP Y)$ $

This table is supposed to be provisioned via SESM and not manually. The field in bold is updated to support a new entry DPL_TERM DPLEX.

1.1.2 CS2KSS-GWC Association:

Currently, a gateway controller can be associated with a maximum of 6 gateways (LGRP nodes) in CS2KSS. After the GWC is commissioned, a logical association is created in the core between the GWC and the gateways in the CS2KSS.

- The table LGRPINV stores the information about the LGRP node and the GWC which it is associated with. After the GWC information is provisioned in the table SERVRINV, the LGRP node information for corresponding LGRP nodes are datafilled in the table LGRPINV. The table LGRPINV is enhanced so that a new lgrp_type 'SSDPL' is supported. This new lgrp_type signifies that this LGRP node is associated with DPL lines.

- Currently, each LGRP node can support 1023 lines and this size will not change as a part of this feature. The information on these lines for each of the LGRP node is stored in the table LNINV. Table LNINV does not require any enhancements to support this functionality.

- A tuple with following structure is expected after the table LGRPINV is provisioned:

Table LGRPINV:

LGRP_NO SRVR_NAME **GRPTYPE** LGRPOPTS
LG 1 1 GWC 5 **SSDPL** $

This table will be provisioned via SESM and is not supposed to be datafilled manually. As shown above, a new lgrp_type 'SSDPL' is supported now for table LGRPINV.

When 1 LGRP is provisioned, corresponding 1023 lines subtending from that lgrp will be datafilled in table LNINV. As a part of this feature, the table LNINV is enhanced so that it can support only RDTLSG(North American market) and GWLPOT(International Market) cardcode for SSDPL lgrp_type. Also, the restriction has been applied to the cardcodes valid for the other lgrp_types. A sample tuple:

Table LNINV:
LEN CARDCODE PADGRP STATUS GND BNV MNO CARDINFO CS2KSS 1 1 10 13 RDTLSG PKLNL HASU N NL Y NIL

As a part of this feature the following valid cardcodes apply for different lgrp_types:

LGRP_TYPE	List of Valid Cardcodes
SSDPL	RDTLSG, GWLPOT
S	RDTLSG, RDTCON, GWLPOT, RDTEBS,GWLEBS

LGRP_TYPE	List of Valid Cardcodes
M	RDTEBS, GWLEBS
C	RDTLSG, RDTCON, GWLPOT
LL_3RDPTY	RDTLSG, RDTCON, GWLPOT, RDTEBS, GWLEBS
CALIX_C7	RDTLSG, RDTCON, GWLPOT, RDTEBS, GWLEBS

The table LNINV will be provisioned via SESM and is not supposed to be datafilled manually.

1.1.3 DPL Lines Provisioning:

The DPL line is differentiated from other lines by adding DPL option on that line. The table IBNFEAT is enhanced to support a new data_feature DPL. The DPL option can be added only to IBN/RES lines. Also, SERVORD+ is enhanced for accepting new DPL related options and should be used for datafilling the DPL option.

1.1.3.1 The new DPL option

As a part of supporting new DPL option, table IBNFEAT, LCCOPT and OPTOPT are enhanced.

- The table IBNFEAT have been enhanced to support the DPL data_feature. The DPL line option will have a SIP sub option. The SIP sub option of DPL will itself have a sub option of MAX_NUM_CALLS(10).
- The table control editor commands, ADD,DEL and CHA are disabled for the DPL option in table IBNFEAT much in the same manner of the PDO option.

Table IBNFEAT:

LEN DNNO DF FEATURE DATA
LG 01 1 00 14 0 **DPL DPL Y 10**

This table will be provisioned via SESM.

- DPL option can only be added via Servord and not Table Control.
- The options incompatible with the DPL option can be datafilled in the table OPTOPT. A sample tuple:

Table OPTOPT:

DPL (BC) (CSDO) (EOF) (FIG) (FTS) (LDTPSAP) (LNPTST) (MAN) (MPB) (NDC) (NOH) (VOWDN) $

You can add options in this tuple which you want to make incompatible with option DPL. This is just a sample tuple. To see the list of supported options with DPL, please refer the interactions section of FN.

- The LCC's supporting the DPL option can be modified through the table LCCOPT. Currently, only IBN and RES lines support the DPL option. Sample tuples are as belows for IBN and RES LCC's.

Table LCCOPT:

RES (ACB) (ACRJ) (ADSI) (ADSL) (AIN) (AINDENY) (AINDN) (AMATEST) (AMSG) **(DPL)**

IBN (ACB) (ACD) (ACDNR) (ACRJ) (ADSI) (AIN) (AINDN) (ALI) (AMATEST) (AMSG) **(DPL)**

1.1.3.2 SERVORD+ Enhancements:

SERVORD+ Enhancements have been made so that it will now accept three new options related to SIP lines provisioning: DPL, SIP_PASSWORD and SIP_DATA. DPL will be seen in the core whereas the options SIP_PASSWORD and SIP_DATA will be send to the CS2KSS.

- When provisioning a SIP line all three of the options described above must be present in the SERVORD+ NEW command.
- The above options can not be added later via ADO.
- ADO and DEO of options that are compatible with DPL will be permitted. But ADO/DEO can not be used with the DPL line option.
- Only NEW, OUT and CHF will support the DPL line option. It is possible to add a DPL compatible option that does not require the DPL option in the command (such as ADO PIC). CHF can be used to manipulate the MAX_NUM_CALLS value subfield of the DPL option. The line must not be in the CPB or call processing busy state or the change will be rejected. CHG can be used to change all but the LCC (line class code).
- DGT option is required. It will be automatically added if not present.
- Long SERVORD+ commands are supported by allowing commands to be continued on a second line by using a + sign.
- The SIP URI change will be reflected in the CS2KSS and not in the core.
- E.g. of the SERVORD+ command:

Servord+ NEW Command:

NEW $ 6212500 IBN BNR 0 0 613 NILLATA 0 LG 000 0 10 13 DPL Y 3 SIP_PASSWORD xx SIP_DATA bobby mb1

1.1.3.3 Journal File:

The Journal File (JF) subarea provides a facility for preserving Data Modification Orders (DMO) on tape so that data tables can be restored if the switch should fail. The Journal File is an optional feature of the DMS switch which preserves DMO on magnetic tape. If a switch failure occurs that requires a reload, this magnetic tape is loaded back into the machine and switch data is restored to its condition at the time of switch failure.

1.1.4 NCAS Link Provisioning:

The core communicates directly with the CS2KSS Provisioning Server through NCAS links. The CS2KSS Provisioning Server can return both static and dynamic call data stored in CS2KSS back to the core via the NCAS link

The NCAS link is going to be an instance of SCTP. The table IPAPPL provides SCTP instance for various connections in DMS. This table is enhanced to support a new application called SIPMTC (just like AIN, SMDI etc). The core can now communicate with CS2KSSs using this SCTP instance.

Table IPAPPL:

InstKey InstName Transport IPDevice IPaddrs port optlist
1 a sctp hiop 198 202 188 221 4982 (application **sipmtc**)
(setprime 1)

The NCAS link association is going to be used for the new QSIP command.

The SIPMTC application is supported over HIOP only.

The multihoming functionality is not supported in SIPMTC application.

The port number allocated for SIPMTC application is 4982.

Multiple instances for SIPMTC are not allowed i.e. in table IPAPPL, there can be only one instance datafilled for SIPMTC.

1.1.5 Core Maintenance Activities:

On the core side, maintenance actions can be performed on the DPL lines. The maintenance operations will keep the core, gwc and cs2kss informed about each other's activities.

1.1.5.1 MAP Commands and Line State Propagation:

The DPL line can be posted on mapci; lns; ltp level.

- The line states for DPL lines on the Core include: IDL, LMB, MB, INB, CPB, CPD, SB. After the line is posted, operations like BSY, RTS, FRLS, HOLD, NEXT can be performed on the posted line. When these operations are performed, the state change of the lines is propagated to the GWC which in turn notifies CS2KSS.
- There are plans to support DIAG in the second phase of this feature, but they will not be supported in the current release. When DIAG is run on the core side, a message will be displayed: “This command is not valid for posted line.”.
- At the map level, the base DPL tid will be posted. If there is any call active, then the information posted for base DPL tid will depend upon the number of call appearances active. If there is only call appearance active, then the linking information for that call appearance will be posted. However, for more than one call appearance, the linking information will not be displayed for all the call appearances. The maintenance operations on specific call appearances will be supported in later release.
- The DPL line can be posted at all the sub-levels of the LTP level: LTPLTA, IBNCON, LTPMAN, LTPDATA, LTPISDN, DCTLTP, DTPLTP. But no maintenance operations can be performed on posted DPL lines at any of these sub-levels.
- For the BSY command, the CS2KSS will be notified that this DPL client is not available for call processing. If there are no call appearances active, then the base TID will be put into MB state and no calls can be associated with this DPL agent. If there are any call appearances active, then the base TID will be put into CPD state. When all the calls are taken down, the base dpl TID will move from CPD to MB state. New calls cannot be originated/terminated on the DPL line that has been busied. The line has to be RTSed back for new calls to be originated/terminated.
- A FRLS on a DPL agent will clear all active calls for the line. If there are no active calls then the base TID, then the tid will be put to MB state. If there are active calls, a FRLS will terminate all the sessions. However, FRLS on a particular session will be supported in a later release.
- On RTS operation, the line will be put into IDL state. This operation cannot be performed when the calls are active on a DPL line.
- The maintenance operations BSY/RTS/FRLS at the MAP level are applicable for all the multiple call appearances. The Mtc operations are applied to all the VIDs.
- The HOLD command puts the posted DPL line in the hold position.
- The NEXT command moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in a

specified hold position. The NEXT command does not list the next provisioned DPL VID.

- The LGRP node can be posted at the PM level but maintenance operations cannot be performed on the entire LGRP. Thus, the state changes because of maintenance operations are propagated upwards to the core through the GWC.

Note: The maintenance operations are not supported for the SSDPL lgrp.

- When the BSY LGRP command is given for the SSDPL lgrp, the following error message is displayed:

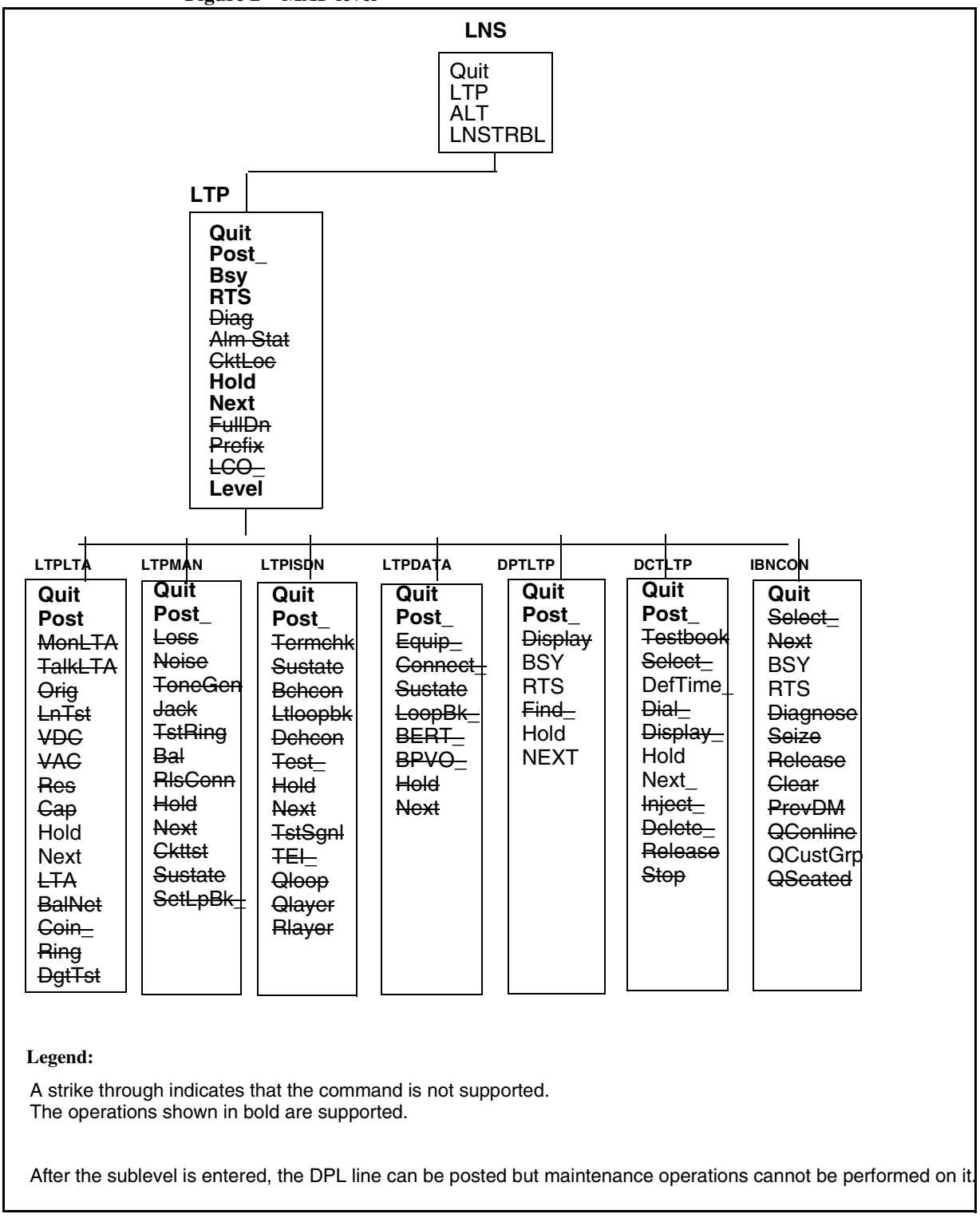
BSY COMMAND IS NOT SUPPORTED FOR THIS TYPE OF LGRP NODE.

- When the RTS command is given for the SSDPL lgrp, the following error message is given:

RTS CAN ONLY GO FROM MANB STATE.

Figure 2 Map Level below shows the MAP levels and operations which are supported and blocked for DPL lines.

Figure 2 MAP level



Legend:

A strike through indicates that the command is not supported.
The operations shown in bold are supported.

After the sublevel is entered, the DPL line can be posted but maintenance operations cannot be performed on it.

At the **LTPLTA** level, the error messages that will be seen for the unsupported maintenace commands are:

MonLTA, TalkLTA, Orig, LnTst, VDC, VAC: **This command is not valid for posted line.**
BalNet: **This command is not valid for Call Server LGRP lines.**
Coin, Ring, DgtTst: **No talk connection to posted line**

At the **LTPMAN** level, the error messages that will be seen for the unsupported maintenance commands are:

Loss, Noise, Tonegen, Jack, RlsConn : **This command is not valid for the posted line.**
Tstring: **To test the ringing function for Call Server LGRP lines, please run the DIAG command.**
Bal: **This command is not valid for Call Server LGRP lines.**
Ckttst: **CKTTST command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
SetLpBk_ : **SETLPBK command is not valid on POTS/COIN lines.**

At the **LTPISDN** level, the error messages that will be seen for the unsupported maintenance commands are:

TERMCHK: **TERMCHK command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
BchCon: **BCHCON command is not valid on POTS/COIN lines.**
LTLOOPBK: **LTLOOPBK command is not valid on POTS/COIN lines.**
DCHCON: **DCHCON command is not valid on POTS/COIN lines.**
TEST: **TEST command is not valid on POTS/COIN lines.**
TSTSGNL: **TSTSGNL command is not valid on POTS/COIN lines.**
TEI: **TEI command is not valid on POTS/COIN lines.**
QLOOP: **QLOOP command is not valid on POTS/COIN lines.**
QLAYER: **QLAYER command is not valid on POTS/COIN lines.**
RLAYER: **RLAYER command is not valid on POTS/COIN lines.**

At the **LTPDATA** level,

Equip, Loopbk_, BERT_, : **This command is not valid for Call Server LGRP lines.**
Connect: **CONNECT command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
BPVO: **BPVO command is not valid on POTS/COIN lines.**

At the **DPTLTP** level,

Find_ : **CLLI entered is not of a DPT trunk**
Display: **DN not involved in a call**

At the **DCTLTP** level,

Testbook: **No testbook is active.**
Select: **SELECT command not executed. No testbook is active.**
Dial: **DIAL command not executed. No testbook is active.**
Display: **DISPLAY command not executed. No testbook is active.**
Inject: **INJECT command not executed. No testbook is active.**
Delete: **DELETE command not executed. No testbook is active.**
Release: **RELEASE command not executed. No testbook is active.**
Stop: **STOP command not executed. No testbook is active.**

At the **IBNCON** level,

Select: **That line is not associated with a console.**
Next, Diagnose, Seize, Release, Clear, PrevDm, Qconline, Qseated: **Console not selected.**

1.1.5.2 Restart and Swact Recovery:

It is desired that when Core, GWC and CS2KSS undergo restart/swact, each of the component's view of line states are in sync.

When the core undergoes restart/swact it notifies the GWC about the type of restart/swact. The GWC performs the necessary operations and also notifies the CS2KSS regarding this. The heartbeat mechanism is used to notify each other of their availability.

When the core undergoes restarts/swacts, a message is sent to GWC about the type of restart/swact. The GWC has to take action upon the type of restart/swact that occurred.

Core Recovery:
The stable calls are the ones in the talking state. The unstable calls imply the ones not in the talking state.

- For core warm restart, GWC clears all unstable calls.
- For core cold restart, GWC clear all stable and unstable calls.
- For core warm SWACT, GWC clear unstable calls.
- For core cold SWACT, GWC clears all stable and unstable calls.
- For core reload restart, BSY GWC Node. When core recovers, RTS the GWC node.
- After the core restart is completed, a message is sent to the GWC that the core is in 'Running' state. If the GWC was BSYed, it will be RTSed. The core sends a SST320 message to RTS all the lines of an LGRP.

- If the CS2KSS is OOS before the restart, lines are put into LMB state. The availability of CS2KSS is tracked by the GWC by the heartbeat mechanism.
- Even if the line was manually BSYed before restart, the line is RTSed to IDL state after restart is over.
- When the core recovers, the endpoints appear as SB until the recovery process is complete, then they transition to IDL. However, the transition state SB cannot be tracked because by the time core recovers completely and we can post the line at the mapci level, the line would have been RTSed to IDL state.

GWC Recovery:

- When the GWC is busy, the state of the GWC in the core side will be ManB. If the GWC is OOS, the state of the GWC in the core would be SysB. When the GWC is not InSv, the LGRP will be in SysB state.
- When GWC goes down, a message is sent to the core to put the line in LMB state.
- When GWC recovers, message is sent to the core to put the line into IDL state. But since the connection between the GWC and CS2KSS is lost, the lines will be put into LMB state. When the discovery message from CS2KSS to GWC is sent, the lines of the corresponding lgrp are out into IDL state.

CS2KSS Recovery:

The maintenance operations are not supported on CS2KSS in this release. The line states are depedent upon whether CS2KSS is up or not.

- CS2KSS gateway is not provisioned on the GWC side.
  If the gateway is not provisioned on the GWC side, the lgrp state is SYSB the lines will be in INB state.

- CS2KSS gateway is provisioned but the gateway is OOS
  When the gateway is OOS, the lgrp is in SYSB state and the lines are in the LMB state. Only when the DISCOVERY message is sent to the GWC from the CS2KSS, the lines are put to IDL state.

1.1.6 Tools:

1.1.6.1 QSIP:

QSIP is a new query command at the CI level. It has been introduced as a part of this activity. QSIP would query the SIP Line data for a particular SIP Line.

The QSIP command will display the following information:

- SIP URI

- Registration State
- Allow Post Busy Termination
- Number of Contacts
- Contacts
- Service Package
- Services
- Endpt ID
- Virtual Media Gateway
- Middle Box ID List
- Client Type
- Static Client
- Node number and Terminal number of the VIDs of all the Active Call Appearances
- Number of Active Sessions in CS2000 Session Server

The QSIP command will launch a Query message to the CS2000 Session Server over the NCAS link. The CS2000 Session Server will launch a Response to the Core over the NCAS link. Upon receiving the Response from the CS2000 Session Server, the Core QSIP command will display the above SIP Lines information.

The response for the QSIP query sent is expected to arrive within a specific time interval. The default QSIP response time interval is 15 seconds. However, the timeout can be set from 1 to 30 seconds. If any value greater than 30 or lesser than 1 is given as the timeout value, the timeout value will be set to the default timeout value of 15. Timeout is an optional parameter in the QSIP command.

The QSIP command will only display the CS2000 Session Server services that are ENABLED. There could be services provisioned on the SIP line which are DISABLED which would not be shown. However, the QSIP will display the Service Package Name which would help if it is known which services are in a particular Service Package.

If a SIP line has contacts, only the URIs of the first three contacts will be shown.

If a SIP line has more than 3 middle box ids, only 3 middle box ids will be displayed.

If QSIP cannot display the SIP data from the CS2000 Session Server a message will be printed as follows:

SIP DATA CANNOT BE DISPLAYED DUE TO <REASON>

Where <REASON> could be one of the following

- RESPONSE TIMEOUT FROM CS2000 SESSION SERVER
- BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER
- QSIP SEND REQUEST FAILURE
- The QSIP Application Error String from the QSIPReportError message received from CS2000 Session Serve

If the response from the CS2000 Session Server does not have any data for any of the parameters then the following message is displayed:

- SIP DATA CANNOT BE DISPLAYED BECAUSE NO DATA RECEIVED FROM CS2000 SESSON

If the CS2000 Session Server responds with partial data , before the SIP data portion of the QSIP display begins there will be a message:
"PARTIAL DATA RECEIVED FROM THE CS2000 SESSION SERVER."
Then, the QSIP will display whatever data it can and leave the other fields blank.

If the total number of parameters, including main parameters and their sub-parameters, received in the response message from CS2000 Session Server is greater then 19 then it would be considered as an error scenarior and the following message would be displayed:

SIP DATA CANNOT BE DISPLAYED DUE TO BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER

The Allow Post Busy Termination and Node numbers and Terminal numbers of the VIDs active on the call are displayed only if some data is received in the response message from the CS2000 Session Server.

QSIP will work for all the LENs that work fine with QLEN. However, to get data the LEN should correspond to a SIP Line.

If QSIP is used with a non-SIP DN then the following message will be displayed:
QSIP SHOULD BE GIVEN FOR SIP LINES ONLY

If a non-existent DN is specified for QSIP then the following message will be displayed:
INVALID DN SPECIFIED FOR THE QSIP COMMAND

If a non-existent LEN is specified for QSIP then the following message will be displayed:
INVALID LEN SPECIFIED FOR THE QSIP COMMAND

The QSIP command’s CI format is shown below:

>q qsip

DISPLAY SIP LINE INFORMATION
Command Format: QSIP <DR_LEN_TYPE>
Parms: [<TIMEOUT> {1 TO 30}]

- Example for QSIP (DN as a parameter)

> qsip 6138675309
SIP USER DATA
==========
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12
CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061
6138675309@1.2.3.4:5062
SERVICE PACKAGE: DEFAULT_PKG
SERVICES: ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
==========
ENDPT ID: PHX/003/0/1000
VMG: VMG.1
MIDDLE BOX ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
==========
ACTIVE CALL APPEARANCES:
NODENO TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12

- Example #2 for QSIP (LEN as a parameter)

> qsip 6138675309
SIP USER DATA
==========
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12

CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061
6138675309@1.2.3.4:5062
SERVICE PACKAGE: DEFAULT_PKG
SERVICES: ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
==========
ENDPT ID: PHX/003/0/1000
VMG: vmg
MIDDLE BOX ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
==========
ACTIVE CALL APPEARANCES:
NODENO TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12

1.1.6.2 QDN/QLEN/DISPCALL/PMIST/CALLTRAK:

The QDN, QLEN, DISPCALL, PMIST, and CALLTRAK tools will be supported for DPL Lines, and they will retain their same functionality and same command interfaces. There will be no impact to these tools by this activity. However, tools like CALLTRAK are tid-based, and thus when tracing on a DPL line with multiple active calls, trace data for ALL of the active calls with be captured.

1.1.6.3 DISPCALL:

DISPCALL is a tool which is used to capture the call data associated with the agent.The agent can be selected to capture the call information using following commands.They are SAVETID and SAVELEN.

The parameter for SAVETID is node number and terminal number.And parameter for SAVELEN is LEN of the agent. For DPL lines a new optional parameter KEY has been added along with the existing parameter for both SAVETID and SAVELEN.The KEY parameter holds the key value of the call appearance.The key values can be obtained form the tool DPLTEST.

IF the agent is selected with out key value for DPL lines, the tool checks for number of call appearance associated with the selected TID or LEN. IF there is only one call appearance associated with the TID/LEN then it gives the information associated with that call. IF there are multiple call appearances, then it displays the message saying multiple calls associated with this call,please enter the key value.

1.1.6.4 CALLTRAK:

CALLTRAK tool is used to capture the IO messages and procedure traces for the agent selected. For DPL lines, Since all the VIDS are allocated dynamically, and deallocated by the time the call complete, there would not be any vids associated with the agent by the time logs are displayed using the display command. So the log may not show the exact agent information.

For DPL lines, the hook has been added in the calltrak,so that it will store only the base TID in the call data and also capture all the information associated with that TID. Since only the base TID is stored in the call data, the calltrak log will not show the KEY information in the IO message for DPL lines.

Ex:

INCOMING 14:48:20.116 NODE TYPE= LGRP_NODE SCP_X_ALERTING_MSG

NN= 00B5 TN= 002F MSGTAG= 00 ROUTE= 0080 ERROR= 00 LENGTH= 0C

AGENT= SS 00 0 00 46 DN 6136215046

6D 02 00 00

1.1.7 Information regarding the Network Services / Signalling Interworking:

The following tables illustrate the network services/signalling interworking information.

Client Services
Call Forward (local)
Call Return (local)
Call Waiting
Call Waiting Disable
Caller ID
Do Not Disturb (local)
Hold
3-Way Call
Call Transfer

Country Specific services

Austria - Carrier Pre-Selection (via TNS parameter)
Belgium LNP (OR, ACQ)
Belgium TOPS
Belgium Lawful Intercept
Belgium 8 / 9 Digit Dialplan
France ETSI V.23 CLASS
France Backward Charging via Tax Message
Germany Network AOC
Germany Carrier Pre-Selection
Germany Carrier Pre-Selection
Germany TNS Routing
Germany Lawful Intercept
Germany Call Compl Busy Sub
Germany QSIG
Germany LNP
Germany Variable Dial Plan
Israel Backward Charging for Intnl Calls
Israel Voice Mail
Netherlands LNP (OR, ACQ)
UK LNP (OR and ACQ)
UK Carrier Pre Selection
UK Bellcore CLASS
UK Automatic Recall
UK MSAC
UK CDR Billing

UK ACD / Compucall
UK Network ACD
UK DPNSS Feature Transparency
Mexico TOPS
Mexico CLASS
Mexico Trunk Offer
Australia Lawful Intercept
Australia ACD / Compucall
Australia Network ACD
Australia CLASS
Australia TOPS
Australia TR533 (IN variant)
Australia LNP (ACQ)
Australia E800
Australia Carrier Pre-selection
Australia Centrex IP

Agent Interworking

Agent Interworking Test - French BRI
Agent Interworking Test - Israel Res Lines (MMP15 only)
Agent Interworking Test - UK DASS 2
Agent Interworking Test - Mexico Fixed Wireless Access
Agent Interworking Test - Australia MFT
Agent Interworking Test - Australia TS13

Signalling Interworking

Signalling Interworking test - ETSI ISUP V1
Signalling Interworking test - ETSI ISUP V2

Signalling Interworking test - IBN7
Signalling Interworking test - H.323
Signalling Interworking test - QSIG
Signalling Interworking test - ETSI PRI
Signalling Interworking test - V5.2
Signalling Interworking Test - Austria ISUP
Signalling Interworking Test -Belgium ISUP(migrating to ETSI V2)
Signalling Interworking Test - France, SSUTR2
Signalling Interworking Test - France, SPIROU
Signalling Interworking Test - France, SSURN
Signalling Interworking Test - German ISUP
Signalling Interworking Test - Israel ISUP
Signalling Interworking Test - Israel PRI
Signalling Interworking Test - Israel FDCP R2
Signalling Interworking Test - Netherlands ETSI ISUP V2
Signalling Interworking Test - Netherlands Dutch PRI
Signalling Interworking Test - Norway ISUP
Signalling Interworking Test - Spain ISUP V1
Signalling Interworking Test - Spain PRI
Signalling Interworking Test - Swiss ETSI ISUP V2
Signalling Interworking Test - Swiss PRI
Signalling Interworking Test - UK IUP
Signalling Interworking Test - UK ISUP
Signalling Interworking Test - UK IBN7 Backbone
Signalling Interworking Test - Mexico ISUP
Signalling Interworking Test - Mexico Telmex ISUP
Signalling Interworking Test - Mexican R2

Signalling Interworking Test - Australia IE ISUP
Signalling Interworking Test - Australia I-ISUP
Signalling Interworking Test - Australia ATUP
Signalling Interworking Test - Australia AISUP
Signalling Interworking Test - Australia IBN7 Backbone
Signalling Interworking Test - Australia RLT
Signalling Interworking Test - Australia TS14
Signalling Interworking Test - NZ ISUP
Signalling Interworking Test - Newzealnd R2

PMA Based

Last Number Redial
Anonymous Call Rejection
IBN CFU/CFB/CFD intragroup / intergroup screening
IBN Do Not Disturb
Subscriber Activated Call Blocking - International Line Restriction for international deployment
IBN Call Forward Programming - No call forward interrogation option may be desired in some markets.
Call screening override
Speed Dial programming

Network based

Message Waiting
Station Message Detail Recording
Special Billing - CDR
Suspended Service
Terminating DN Billing
Tollfree Services

Multi-Switch Business Group (MBG) i/w
Interop with other Succession endpoints (PVG, MG9K, legacy lines via IW SPM IP, etc.)
Direct Inward Dial
Direct Outward Dial
E911 termination
IN - no digit collection
Lawful Intercept
Free Number Terminating
Customer groups with mix of Unistim, SIP, IBN lines
Subscriber Line Usage
Operator Number Identification
PIC
Dial Plan Management
Virtual Private Network (VPN)
INWATS / OUTWATS - Freephone number Intl.
VFG
Local Number Portability
Carrier Pre-Selection (provisioned and prefix dialing)
Simple MEETME and PRESET Conference
Carrier Toll Denial - International calls - Inter-Lata - Intra-Lata
NCOS restrictions
NCOS Time of Day routing
Denied Termination
Denied Origination

1.2 Hardware Requirements or Dependencies

None.

1.3 Software Requirements or Dependencies

The CORE OAMP functionality has dependencies associated with some of the other components in the overall SIP lines feature:

- SESM
- CS2KSS
- GWC
- OSSGATE
- NCAS Link

1.3.1 SESM:

SESM EM needs the enhancements in table LGRPINV for bulk provisioning and line provisioning.

1.3.2 CS2KSS:

- QSIP core client is dependent on the CS2KSS API for QSIP query.
- SCPLITE APIs should be present to support the QSIP messaging.
- The CS2KSS profile team has to provide an API to get the Registration status and the SIP URI information
- The CS2KSS callp should provide an API to give the Active sessions for a SIP Line
- The CS2KSS will need to know the syntax of the QSIP messages it will receive from and send to the Core.

1.3.3 GWC

- GWC EM requires table SERVRINV enhancements to support the new term type DPL and a new exec lineup DPLEX.
- The state changes due to the operations BSY, RTS, FRLS, HOLD, NEXT performed on SIP lines in core should be propagated to the GWC.
- When the CS2KSS or GWC are taken down, the same should be notified to the core.
- Audit messages will be sent between the CORE & GWC and the message protocol from both the parties should be understood by each other.
- Carcodes for the DPL lines are restricted to RDTLSG for the North American market whereas it is restricted to GWLPOT for the International market.

1.3.4 OSSGATE:

- It needs the IBNFEAT and servord enhancements for line provisioning and other servord+ line commands like DEO, ADO etc.

1.3.5 NCAS Link:

- It should be available for the QSIP query to take place.

1.4 Limitations and restrictions

- Since the CLTG command is applicable only to POTS and RES lines, the CLTG Servord command applies to only RES DPL lines. CHG NCOS will have to be used for providing the functionality to IBN DPL lines. The CLTG and CHG will be done via SESM.

1.5 Interactions

None.

1.6 Glossary

Term	Description
CS2K	Communication Server 2000
CPD	Call Processing Deloaded
CB	Connection Broker
DEL	Deloaded
GWC	Gateway Controller
INB	Installation Busy
LMB	Line Module Busy
LCC	Line Class Code
NCAS	Non Call Associated Signalling
NEQ	Not Unequipped
OSSGATE	Operation Support System Gate
OAMP	Operation, Administration, Maintenance & Provisioning
CS2KSS	Communication Server 2000 Session Server
SESM	Succession Element and Sub-Element Manager
SB	System Busy
SERVORD	Service Order
SOC	Software Optionality Control
SCTP	Stream Control Transmission Protocol

2: Configuration for A00008556

2.1 Hardware and Software Requirements

No new hardware or software requirements are created by this activity.

2.2 Initial Configuration

At initial configurations, it is assumed that standard datafill exists in the DMS/CS2K, GWC and CS2KSS. Since a usage SOC is used for this feature, the SOC limit decides whether any service will be provided initially by the design components applicable after the DPL line is provisioned.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

2.4 Upgrade Considerations

None.

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 below shows a list of new/modified tables.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
SERVRINV	CHANGED	UNCHANGED
LGRPINV	CHANGED	UNCHANGED
IPAPPL	CHANGED	UNCHANGED
IBNFEAT	CHANGED	UNCHANGED
LCCOPT	CHANGED	UNCHANGED
OPTOPT	CHANGED	UNCHANGED

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name: SERVRINV

SERVER INVENTORY

2.5.2.1.1 Functional description

Server Inventory table stores the information on GWC. Each entry in this table provides information about a specific GWC which includes the following:

- Server type and numeric ID, e.g. GWC 7.
- Packet network type (IP or ATM).

- GWC IP address.
  Note: The last element of this address must be a multiple of four, because four IP addresses are used by each GWC; the three IP addresses next in sequence are assigned automatically.
- The server exec(s) to be used, which determines the type of call processing to be performed by the GWC. A new entry is specified for this field by this feature.
- Toneset to be used.
- Bearer Networks.
- Optional attributes to be associated with this GWC.

2.5.2.1.2 Usage sequence and implications (CM Only)

The table SERVRINV can be datafilled independently through SESM. There is no change in the current table datafill order.

2.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVRINV	0	256	Memory is dynamically allocated at 16 tuples per allocation.

2.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVRINV.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVREXEC	Changed	TERM_TYPE EXEC_LINEUP	DPL_TERM DPLEX	This field now supports a new term_type DPL_TERM and a new exec_lineup DPLEX.

2.5.2.1.5 Datafill example

The following example shows sample datafill for table SERVRINV.

Table SERVRINV:

SRVRNAME SRVRADDR ***SRVREXEC*** *SRVRTONE BEARNETS SRVROPTS*
GWC 0 IP 45 46 47 48 ***(DPL_TERM DPLEX)*** *$ NORTHAA (NET_IP Y) $ $*

2.5.2.1.6 Table release history update

The table SERVRINV is enhanced to support new SRVREXEC entry DPL DPLEX. This entry for a new terminal_type and new exec_lineup is specifically going to be used to support the DPL agents on the GWC.

2.5.2.1.7 Supplementary information

None.

2.5.2.1.8 Translation verification and other tools

None.

2.5.2.2 Name: LGRPINV

LOGICAL GROUP INVENTORY

2.5.2.2.1 Functional description

Logical group inventory table defines the gateways or nodes supported under the gateway controller. The gateway or node entries are:

- Logical group number (site name, frame no, shelf no) e.g. LG 2 3
- Server name (GWC datafilled in table SERVRINV)e.g GWC 7
- Logical group type: This field is to specify the group type.
  Existing logical group types are

S	MG9K large lines gateways
M	CICM large lines gateways
C	Small lines gateways
LL_3RDPTY	Large Line Third Party gateways
SSDPL	DPL lines.

- When the LGRPINV is provisioned with a LGRP ‘SSDPL’, then a termtype ‘DPL’ is specified in LNINV table. When lines are provisioned in table LNINV, then an exec_lineup DPLEX corresponding to termtype ‘DPL’ will be downloaded to the GWC. Also, the cardcode of the DPL lines is restricted to RDTLSG for North American market and GWLPOT for International market.
- Logical group options
  Existing options are:(MTSTAPT, LGRPLOC, GTWYKEY)

2.5.2.2.2 Usage sequence and implications (CM Only)

The table LGRPINV depends upon the table SERVRINV. It references the server name from the table SERVRINV.

2.5.2.2.3 Size

The following table lists the size of LGRPINV table.

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LGRPINV	0	1000	Memory is dynamically allocated at 10 tuples per allocation.

2.5.2.2.4 Fields/OIDs

The following table lists fields/OIDs for LGRPINV

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GRPTYPE	Changed	N/A	SSDPL	A new LGRP SSDPL has been introduced to support DPL lines.

2.5.2.2.5 Datafill example

The following example shows sample datafill for table LGRPINV

Table LGRPINV:

LGRP_NO SRVR_NAME ***GRPTYPE*** *LGRPOPTS*
LG 1 1 GWC 5 ***SSDPL*** *$*

2.5.2.2.6 Table release history update

The table LGRPINV is enhanced to support DPL agents. As part of this enhancement new lgrp_type ‘SSDPL’ is introduced.

2.5.2.2.7 Supplementary information

None.

2.5.2.2.8 Translation verification and other tools

None.

2.5.2.3

2.5.2.4 Name: IPAPPL

Internet Protocol Application

2.5.2.4.1 Functional description

Table IPAPPL datafill provides instance of various connections to the DMS. The use of SCTP transport requires that the application store the specific remote IP addresses and local Port number. Therefore table IPAPPL is datafilled in order to provide these details. Table IPAPPL includes following fields.

TABLE IPAPPL Fields and description are as follows:

- InstKey is datafilled in order to map this instance with an internally assigned instance number. This field is the unique key to the tuple.
- InstanceName is datafilled in order for the telco personnel to be able to distinguish one connection from the other.
- Transport is datafilled in order to classify the instance to which transport protocol be used. Currently the table will support SCTP functionality ONLY.
- IPDevice is datafilled to indicate which IP interface hardware will be used. This table currently supports EIU and HIOP.
- IP addresses (upto 4 addresses) are allowed in one instance tuple. This may be used to support multihoming. The first IP address in the list will be used as the primary address. IPV4 type IP addresses are supported.Only one IP address will be used for DPL, the IP address of the CS2KSS Provisioning Manager.
- Port Number is the local port number at which the DMS-Core will expect to receive messages from this instance. (Note that the remote port is received during the INIT message from the far-end). Valid range of Source port allowed to be configured on the CORE is from 4900 to 4982
- OptList field may be datafilled with “SETPRIME” to set any of the IP address in an instance to be used as to set the primary destination address.
- Optlist sub-field “APPLICATION” can be datafilled to specify the application eg:DPL. Here the SIPMTC(Application) option is incorporated along with AIN option.
- Optlist sub-field “mode” is to specify the mode SERVER/CLIENT.
- Optlist sub-field “multihoming” is used to specify if the remote node supports multihoming. This option is currently only supported on the HIOP ipdevice.

2.5.2.4.2 Usage sequence and implications (CM Only)

The table IPAPPL is an independent table.

2.5.2.4.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IPAPPL	0	64	Memory is automatically allocated for 64 Intelligent Network SCTP instances

2.5.2.4.4 Fields/OIDs

The following table lists fields/OIDs for IPAPPL.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTS	Changed	Application	SIPMTC	A new application 'SIPMTC' is added to option list.

2.5.2.4.5 Datafill example

The following example shows sample datafill for table IPAPPL:

Table IPAPPL:

InstKey InstName Transport IPDevice IPaddrs port optlist
1 a sctp hiop 198.202.188.121 4982 (application ***sipmtc****)*
(setprime 1)

2.5.2.4.6 Table release history update

The table IPAPPL is enhanced to create an instance for SIPMTC service.

2.5.2.4.7 Supplementary information

- The NCAS link association is going to be used for the new QSIP command.
- The SIPMTC application is supported over HIOP only.
- The multihoming functionality is not supported in SIPMTC application.
- The port number allocated for SIPMTC application is 4982.
- Multiple instances for SIPMTC are not allowed; i.e. in table IPAPPL, there can be only one instance datafilled for SIPMTC.

2.5.2.4.8 Translation verification and other tools

None.

2.5.2.5 Name: IBNFEAT

IBN Feature

2.5.2.5.1 Functional description

IBNFEAT (IBN Line Feature) lists line features that are assigned to the IBN lines listed in table IBNLINES.

Table IBNFEAT fields and description are as follows:

LEN: Line equipment number. This field consists of the subfields SITE, FRAME, UNIT, DRAWER, LSG and CIRCUIT.

DNNO_RANGE: Directory number. This field specifies the DN of the LEN being referenced. Enter a value from 0 to 6 for the DN.

DF : Data feature. This field specifies the data feature assigned to the line.

FEATURE: Data feature. This field specifies the data feature assigned to the line.

DATA: SIP: Bool. Enter Y if a SIP line

MAX_NUM_CALLS: Enter a value between 1-10.

ALLOW_BSY_TERM: Bool. It determines whether or not a busy SIP line can take an additional call termination.

Only Servord can be used to datafill the DPL option. It cannot be done via table control.

2.5.2.5.2 Usage sequence and implications (CM Only)

- In table LCCOPT, DPL option should be made compatible with IBN LCC.
- The table IBNLINES should have the LEN datafilled before the DPL option can be added on it.

2.5.2.5.3 Size

2.5.2.5.4 Fields/OIDs

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNFEAT	0	TBD	TBD

The following table lists fields/OIDs for IBNFEAT.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DF	Changed	N/A	DPL	A new feature DPL to be assigned to an IBN line.
Feature	Changed	N/A	DPL	A new feature DPL to be assigned to an IBN line.
DATA	Changed	SIP MAX_NUM_CALLS Allow_Bsy_Term	Y/N 1-10 Y/N	Enter Y if a SIP line Max Simultaneous Call Appearances. It determines whether or not a busy SIP line can take an additional call termination.

2.5.2.5.5 Datafill example

The following example shows sample datafill for table IBNFEAT.

Table IBNFEAT:

LEN DNNO DF FEATURE DATA
LG 01 1 00 14 0 DPL DPL Y 10 Y

2.5.2.5.6 Table release history update

Table IBNFEAT has been enhanced to support a new feature DPL which will convert the IBN line into a DPL line.

2.5.2.5.7 Supplementary information
None.

2.5.2.5.8 Translation verification and other tools
None.

2.6 Service Orders (SO) (CM & SESM)
SERVORD+ will accept three new options related to DPL lines provisioning: DPL, SIP_PASSWORD and SIP_DATA. When provisioning a SIP line all three of the options described above must be present in the SERVORD+ NEW command. They can not be added later via ADO.

2.6.0.1 LCC and options
New line option DPL is introduced by this feature. It is compatible with RES and IBN line class codes only. DPL is not compatible with huntgrps, scmp, MADN, FTRG.

Table 10 Meridian digital centrex feature assignment requirements

Feature	500 2500	MDC SET	ISDN SET	MDC Set ISDN Set Relationship							
				SET	SUBSET	KEY	DN	DEDKEY	LAMP	CODE	DISPLAY
DPL	Y	N	N	N							

The feature in the table above requires a handsfree Business Set. This feature must be assigned to key 1.

2.6.1 New commands
No new commands are introduced with this feature.

2.6.1.1 How service order commands are presented

2.6.1.1.1 Description
The NEW command is used to associate a DN with a LEN due to which the line state changes from HASU (hardware assigned-software unassigned) to IDL, i.e. puts the line into service.

2.6.1.1.2 Applicability

The DPL line option can only be added with the NEW command. Other commands that prompt for options such as EST, ADD, DE0, ADO and NEWACD will be rejected if the DPL option is present with these commands. A warning message will be output. The CDN and CLN commands will be blocked if the DPL option is present on the line. The line must be OUTed and NEWed to effect a change of LEN or endpoint or DN. CHG of line class code will be blocked if DPL is present on the line.
The DPL option should only be added via SESM. It cannot be added via table control.

2.6.1.1.3 Example

The examples below show how SERVORD+ command NEW can be used to provision the DPL line. Servord+ should be used to add the DPL option. Th e prompt mode is shown as an example of the fields only. Note that SIP_PASSWORD and SIP_DATA are not valid options on the core and are shown here for example only.

Figure 1 Example of the NEW command in prompt mode (SERVORD only)

```
>NEW
SONUMBER:     NOW   4 10 20 PM
>$
DN:
>6212500
LCC_ACC:
>IBN
GROUP:
>BNR
SUBGRP:
>0
NCOS:
>0
SNPA:
>613
LATA:
>NILLATA
LTG:
>0
LEN_OR_LTID:
>LG 000 0 10 13
Option:
>DPL
SIP:
>Y
MAX_NUM_CALLS:
```

```
>3
ALLOW_BSY_TERM:
>Y
SIP_PASSWORD:
>xxx
SIP_DATA:
>bobby mb1
```

Figure 2 Example of the NEW command in no-prompt mode

In the no-prompt mode, the command as entered through SESM will be:

```
NEW $ 6212500 IBN BNR 0 0 613 NILLATA 0 LG 000 0 10 13 DPL Y 3  Y
xx bobby mb1
```

Figure 3 Example of the CHF command in no-prompt mode

```
CHF $ 6212500 DPL Y 7 N $
```

2.6.1.2 How service order options are presented

2.6.1.2.1 Description

A new option DPL is introduced as a part of this activity. This option DPL converts an IBN line into DPL line. The following sections lists how the DPL option and the sub-options associated with the DPL option are assigned through SERVORD.

2.6.1.2.2 Example

The following examples show how a new option DPL and its sub-options are added to a line to convert it into a DPL line.

Figure 4 Example of the DPL option in prompt mode (SERVORD only)

```
Option:
>DPL
SIP:
>Y
MAX_NUM_CALLS:
>3
ALLOW_BSY_TERM:
>Y
```

Figure 5 Example of the DPL option in no-prompt mode

```
DPL Y 3  Y xx bobby mb1
```

2.6.1.2.3 Option prompts

Table 11 System prompts for DPL option

Prompt	Valid input	Description	Areas affected by prompt
SIP	Y	Bool	
MAX_NUM_CALLS	1-10	Integer	
ALLOW_BSY_TERM	Y/N	Bool	

2.6.1.2.4 Line class code compatibility

The new DPL option is applicable only for the IBN and RES lines.

Table 12 DPL compatibility to LCC

Line class code	Compatible?
IBN	Yes
RES	Yes

2.6.1.2.5 Assignability

DPL is not a valid keyset option.
The following functionalities apply to this option:

- set functionality: <yes or no>
- subset functionality: <yes or no>
- DN functionality: <yes or no>
- key functionality: <yes or no>

2.6.1.2.6 Option prerequisites

None.

2.6.1.2.7 Notes

The subfields SIP and MAX_NUM_CALLS which will be prompted for will have the default values of Y and 1 shown respectively. For SN09, these are the only valid values and cannot be changed.

2.6.1.2.8 SERVORD+ Exceptions

None.

2.6.2 Line equipment format changes

2.6.2.1 LEN

There are no changes made in the LEN format.

2.6.2.2 Media gateway endpoint format

The MG endpoint format is similar to the LEN format to make the mapping between them easier.

The suggested endpoint format is:
<GW NAME> <SITE>/NNN/G/TTtt where
GW_NAME = up to 32 chars
<SITE> = a site name datafilled in Table SITE and used as the first part of the LGRPINV key.
NNN = logical frame number from core table LGRPINV
G = group number 0-9 from core table LGRPINV
TT = 00 to 10
tt = 00 to 99 except when TT = 10 then tt = 00 to 22
Example:
SIPVMG1.tampa.vz.com TMP1/000/2/0478 maps to LEN: TMP1 000 2 04 78

2.7 Software optionality control (SOC)

This feature will be controlled by standard usage-based SOC. The limit will define the maximum number of DPL lines that can be provisioned in the switch.

- The default usage limit will be zero, indicating that the DPL option can not be provisioned. New limits can be purchased via SOC in increments of 1 subscriber at a time if desired.
- There will not be a maximum limit. Hence, any limit can be assigned to the SOC CS2C0005.
- When a new DPL line is provisioned, the current DPL count (SOC usage count) will be compared to the purchased limit (SOC usage limit). If the limit has already been reached, the new line can not be provisioned. If the limit has not been reached, the new line is allowed, and the SOC usage count is incremented.
- When an existing DPL line is removed, the current SOC usage count will be decremented, but the SOC limit will not change.
- If the SOC limit is ever decreased to a value below the current usage count, existing DPL line agents will continue to function properly. However, new DPL lines can not be added. Further, if existing DPL lines are removed, they can not be re-added until the current count is below the limit.
- The SOC audit will generate a warning log on each pass if the usage count is above the usage limit.
- The SOC code is functional whenever a line is provisioned with the DPL option whether through table control / servord.
- The usage control of the SOC utility allows the activation/deactivation for provisioning of DPL lines.
- A new module will be created to contain the new SOC code. The new module will belong to a new user group called DPLOAMP.

- It is strongly recommended that the SOC code be sourced in SN09 if possible. This is due to the fact that patching of a usage-based SOC can introduce certain obstacles regarding usage limits and usage counts being updated during ONP. To minimize these obstacles, the SOC code can be sourced in SN09.
- Table 13 below shows the SOC details.

Table 13 SOC

SOC option name:	CS2C0005
SOC option title:	Number of SIP CLient
SOC option control type:	USAGE
New SOC option?	Yes
SOC option order code	CS2C0005
Option defined in DRU:	CCM
Affected products:	CS2K

2.8 Element Management

Not Applicable.

2.9 User interface changes

2.9.1 Directory:

N/A

2.9.2 Command: QSIP

2.9.2.1 Command type: NON-MENU

2.9.2.2 Command target: BRISC, POWERPC

2.9.2.3 Command availability: NONRES

2.9.2.4 Command description

The QSIP command at the CI level will query the CS2KSS to get the SIP information. QSIP command will query the following for the DPL agent:

SIP URI

Registration State

Allow Post Busy Termination

Number of Contacts

Contacts

Service Package

Services

Endpt ID

Virtual Media Gateway

Middle Box ID List

Client Type

Static Client

Node number and Terminal number of the VIDs of all the Active Call Appearances

Number of Active Sessions in CS2000 Session ServerSIP URI

- The CS2KSS will handle the query from the CS2K via the NCAS link for the QSIP command and respond back to the CS2K with the requested data.

- The default time interval for getting a response to the QSIP query is 15 seconds. Time can be set from 1 to 30 seconds. If any value lesser than 1 and greater than 30 is given then the time value will be set to the default value of 15. It is an optional parameter in the QSIP command.

- The QSIP command's format is listed below
  CI:
  >q qsip
  DISPLAY SIP LINE INFORMATION
  Command Format: QSIP <DR_LEN_TYPE>
  Parms: [<TIMEOUT> {1 TO 30}]

- If the NCAS Link is unavailable or the CS2KSS did not respond, the QSIP command's timer will expire with the following message:

  >qsip 8675309
  SIP DATA CANNOT BE DISPLAYED DUE TO RESPONSE
  TIMEOUT FROM CS2000 SESSION

2.9.2.5 Command syntax

Table 14 QSIP command parameters and variables

Command	Parameters and variables
QSIP	<DR_LEN_TYPE> [<Timeout> {1 to 30}]
Parameters and variables	Description
DR_LEN_TYPE	The DN/LEN of a SIP line agent is specified
TIMEOUT	Maximum time for which QSIP waits for a response from CS2KSS. Min value:1 seconds Max value:30 seconds Default value:15 seconds

2.9.2.6 Qualifications and warnings

QSIP query takes place through the NCAS link. Hence, the command response depends upon the availability of the NCAS link.

When the response is not received in a specified time interval, a message is displayed at the console:

“NO RESPONSE FROM CS2KSS WITHIN TIMEOUT OF 15 SECONDS”.

2.9.2.7 Responses

Table 15 MAP outputs with associated meanings and actions

Command
Example 1: >qsip 8675309 --- SIP USER DATA ========== SIP URI: 6138675309@NORTELNETWORKS.COM ACCOUNT STATUS: ACTIVE REGISTERED: Y ALLOW POST BSY TERMINATIONS: N NUMBER OF CONTACTS: 12 CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061 6138675309@1.2.3.4:5062 SERVICE PACKAGE: DEFAULT_PKG SERVICES: ADHOC 4 ADDRBK 50 VMAIL SIP LINE DATA ========== ENDPT ID: PHX/003/0/1000 VMG: vmg MIDDLE BOX ID(s): 1234 1234 3456 CLIENT TYPE: ONT STATIC CLIENT: N SIP CALL DATA ========== ACTIVE CALL APPEARANCES: NODENO TERMNO NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12 ---
Meaning: The querying was successful. All the data obtained is displayed. **System or user actions:** None.

Table 15 MAP outputs with associated meanings and actions

Command
Unsuccessful Query: **Example 2:** >qsip 8675309 SIP DATA CANNOT BE DISPLAYED DUE TO RESPONSE TIMEOUT FROM CS2000 SESSION SERVER **Meaning:** The response was not received before the QSIP timer expired either because the NCAS link is either busy/not available or the CS2KSS did not respond before the timeout occured. **System or user actions:** The user is expected to run QSIP again. **Example 3:** >qsip 122456783 QSIP SHOULD BE GIVEN FOR SIP LINES ONLY **Meaning:** The DN supplied is not a SIP line. **System or user actions:** The user is expected to give a valid SIP Line DN for QSIP. Example 4: >qsip 122456783 INVALID DN SPECIFIED FOR THE QSIP COMMAND Meaning: The DN supplied is not a valid DN. System or user actions: The user is expected to give a valid SIP Line DN for QSIP. Example 5: >qsip LG 0 2 3 4 INVALID LEN SPECIFIED FOR THE QSIP COMMAND Meaning: The LEN supplied is not a valid LEN. System or user actions: The user is expected to give a valid SIP Line LEN for QSIP. Example 6: >qsip 8675309 SIP DATA CANNOT BE DISPLAYED DUE TO BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER Meaning: The response received from CS2KSS in not valid. System or user actions: The user is expected to run QSIP again. Example 7: >qsip 8675309 SIP DATA CANNOT BE DISPLAYED BECAUSE NO DATA RECEIVED FROM CS2000 SESSON SERVER Meaning: The response received from CS2KSS does not have any data to display System or user actions: The user is expected to run QSIP again.

Example 8:

```
>qsip 8675309
SIP DATA CANNOT BE DISPLAYED DUE TO QSIP SEND REQUEST
FAILURE
```

Meaning: An error occured while the QSIP sent the query to the CS2KSS.

System or user actions: The user is expected to run QSIP again.

Example 8:

```
>qsip 8675309
PARTIAL DATA RECEIVED FROM THE CS2000 SESSION SERVER.
--------------------------------------------------------------------------------
SIP USER DATA
=============
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12
CONTACTS:
SERVICE PACKAGE: DEFAULT_PKG
SERVICES: ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
=============
ENDPT ID: PHX/003/0/1000
VMG: vmg
MIDDLE BOX ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
=============
ACTIVE CALL APPEARANCES:
  NODENO   TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12
--------------------------------------------------------------------------------
```

Meaning: the response from CS2KSS did not have data for all the parameters..

System or user actions: None.

2.9.2.8 Example

Table 16 Usage examples for QSIP command

Description of task	The QSIP command at the CI level will query the CS2KSS to get the SIP information.
Command: MAP response:	Example: QSIP 8731932 >qsip 8675309 --- SIP USER DATA ========== SIP URI: 6138675309@NORTELNETWORKS.COM ACCOUNT STATUS: ACTIVE REGISTERED: Y ALLOW POST BSY TERMINATIONS: N NUMBER OF CONTACTS: 12 CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061 6138675309@1.2.3.4:5062 SERVICE PACKAGE: DEFAULT_PKG SERVICES: ADHOC 4 ADDRBK 50 VMAIL SIP LINE DATA ========== ENDPT ID: PHX/003/0/1000 VMG: vmg MIDDLE BOX ID(s): 1234 1234 3456 CLIENT TYPE: ONT STATIC CLIENT: N SIP CALL DATA ========== ACTIVE CALL APPEARANCES: NODENO TERMNO NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12 ---

2.10 OSSGate Interface Changes

Not Applicable.

2.11 Security

None.

2.12 Configuration Walkthrough

The following shows a sequence in which the tables are datafilled:

Table SERVRINV (Provisioned through SESM):

*SRVRNAME SRVRADDR **SRVREXEC** SRVRTONE BEARNETS SRVROPTS*
*GWC 0 IP 45 46 47 48 **(DPL_TERM DPLEX)** $ NORTHAA (NET_IP Y)$ $*

Table LGRPINV (Provisioned through SESM)

*LGRP_NO SRVR_NAME **GRPTYPE** LGRPOPT*
*LG 1 1 GWC 5 **SSDPL** $*

Table LNINV (Provisioned through SESM):

LEN CARDCODE PADGRP STATUS GND BNV MNO CARDINFO
LG 1 1 10 13 RDTLSG PKLNL HASU N NL Y NIL

Servord+ Command (Provisioned through SESM):

NEW $ 6212500 IBN BNR 0 0 613 LG 000 0 10 13 DPL 3 SIP_PASSWORD xx SIP_DATA bobby mb1

Table IPAPPL (Provisioned by Crafts person):

InstKey InstName Transport IPDevice IPaddrs port optlist
*1 a sctp eiu 12 12 12 12 4901 (application **sipmtc**)*
(setprime 1)

Product = CS 2000

A00008601 -- IW-SPM-IP Fully Provisionable Codec Lists for G.711/G.729

Functional Description

1: Applicable Solution(s)

PT-IP

1.1 Description

This feature is to allow IW SPM IP's Codec list to be fully provisionable for G.711 and G.729.

The existing functionality of IW-SPM-IP supports the following two codec configurations.

1. G.711 Only
2. G.729 Preferred (1st Choice) and G.711 Supported(2nd Choice).

This feature extends the codec support of IW SPM IP by allowing codec list to be fully provisionable for G.711 and G.729. With this feature the following codec configuration can be provisionable in MNIPPARM table:

a. G.711 Only (G711 as default codec and NONE as preferred codec)
b. G.729 (preferred) / G.711(2nd Choice)
c. G.711 (preferred) / G.729(2nd Choice)
d. G729 Only (G729 as default codec and NONE as preferred codec).

The following codec list can be supported by IWIP SPM from SN09 for codec negotiation with the far end:

Table 1: Codec list supported by IWIP SPM from SN09

PRFCODEC **in MNIPPARM table**	**DFCODEC in MNIPPARM table**	Codec list supported by IWIP SPM
None	G711ALAW	G711ALAW, G711MuLAW
None	G711MuLAW	G711MuLAW, G711ALAW
None	G729	G729
G711ALAW	G729	G711ALAW, G711MuLAW, G729
G711MuLAW	G729	G711MuLAW,G711ALAW, G729
G729	G711ALAW	G729, G711ALAW, G711MuLAW
G729	G711MuLAW	G729, G711MuLAW, G711ALAW

Definitions for G711 and G729 codec are as follows:

G.711 is 64kbps codec. When G.711 is used, overall voice quality provided by IW-IP will have an ITU R Rating (G.107) of 90, which corresponds to a minimum average MOS of 4.3 (“Very Satisfactory” speech quality).

G.729 is 8kbps codec. When G.729A is used, overall voice quality provided by IW-IP will have an ITU R Rating (G.107) of 80, which corresponds to a minimum average MOS of 4.0 (“Satisfactory” speech quality).

Codec information is already provisionable in default codec[DFCODEC] and preferred codec[PRFCODEC] fields of MNIPPARM table. This feature only adds new values to support full provisioning of codec.

The default values of these fields remains same. The default value for DFCODEC filed is G711ULAW and the default value for PRFCODEC field is NONE.

Detailed information is available in Configuration Section.

1.2 Hardware Requirements or Dependencies

No new hardware required for this feature

1.3 Software Requirements or Dependencies

This functionality requires SN09 load in the Call Server, IW-IP CEM and GEM RM.

1.4 Limitations and restrictions

None

1.5 Interactions

None

1.6 Glossary

Term	Description
CEM	Common Equipment Module
GEM	Gigabit Ethernet (Resource) Module
IP	Internet Protocol
ITU	International Telecommunication Union
IW	Inter Working
MOS	Mean Opinion Score
RM	Resource Module
SPM	Spectrum Peripheral Module
TDM	Time Division Multiplexer

2: Configuration for A00008601

2.1 Hardware and Software Requirements

This functionality requires SN09 load in the Call Server, IW-IP CEM and GEM RM.

2.2 Initial Configuration

Not Applicable

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

2.4 Upgrade Considerations

2.4.1 Dump and Restore (CM)

During the upgrade[ONP] from SN07/SN08 to SN09, in the following two cases the DFCODEC and PRFCODEC values will convert as shown:

Figure 1 Case1: DFCODEC-G711ULAW, PRFCODEC-NONE,

```
Before upgrade [SN07/SN08]:
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G711ULAW NONE 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM

After upgrade [SN09]:
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G729 G711ULAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM
```

RFC2833-ENABLE

Figure 2 Case 2: DFCODEC-G711ALAW, PRFCODEC-NONE,

```
Before upgrade [SN07/SN08]:
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G711ALAW NONE 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM

After upgrade [SN09]:
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G729 G711ALAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM
```

RFC2833-ENABLE.

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
MNIPPARM	CHANGED	UNCHANGED

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name: MNIPPARM

Multiservice Node Internet Protocol PARaMeters.

2.5.2.1.1 Functional description

Table MNIPPARM contains customer provisionable parameters applicable to the IW IP SPM peripheral. This table has no logical dependencies on other tables and each tuple is applicable to all SPMs of the specified type (i.e. all parameters in the tuple for IWSPM apply to every IW IP SPM configured as a BRIDGE ONLY SPM in the office).

2.5.2.1.2 Usage sequence and implications (CM Only)

There are no requirement to datafill tables in a specific order. However, the values specified in MNIPPARM will have no meaning unless an SPM of the IWIPBRG type is datafilled and operational in the office.

2.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNIPPARM	Unchanged	Unchanged	Unchanged

2.5.2.1.4 Fields

The following table lists fields for table MNIPPARM.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MNKEY	Unchanged	None	IWSPM, DPTSPM	T_MNPARM_KEY. This is the tuple key, no default value provided.
DFCODEC	**Changed**	**None**	**G711ALAW, G711ULAW, G729**	**DEFAULT_CODEC. This specifies the default codec to be used in call processing. The default offered is G711ULAW.** **As part of this feature G729 can be provisioned as DFCODEC**
PRFCODEC	**Changed**	**None**	**NONE, G729, G711ALAW, G711ULAW**	**PREFERRED_CODEC. This specifies the preferred codec to be used in call processing. The default offered is NONE.** **As part of this feature G711ALAW or G711ULAW can be provisioned as PRFCODEC**
PKTRATE	Unchanged	None	10, 20	PACKETIZATION_RATE. This specifies the packetization rate in milliseconds to be used for voice packets. The default offered is 10.
INGRESS	Unchanged	None	-6 TO 6	GAIN. This specifies the gain to be applied to the ingress side of the call. The default offered is 0.
EGRESS	Unchanged	None	-6 TO 6	GAIN. This specifies the gain to be applied to the egress side of the call. The default offered is 0.
JITMIN	Unchanged	None	0 TO 300	JITTER. This specifies the minimum jitter setting in milliseconds. The default offered is 100.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
JITMAX	Unchanged	None	0 TO 300	JITTER. This specifies the maximum jitter setting in milliseconds. The default offered is 100.
JITTARG	Unchanged	None	0 TO 300	JITTER. This specifies the target jitter setting in milliseconds. The default offered is 100.
ECAN	Unchanged	ECHOLOSS, ECHOTAIL	ENABLE, DISABLE	STATUS. This specifies if Echo Cancellation is active or inactive. The default offered is DISABLE. The following subfields are given when ENABLE is specified.
		ECHOLOSS	0, 3, 6	ECHO_RETURN_LOSS. This subfield specifies the loss on the echo return signal.
		ECHOTAIL	16, 24, 32, 64, 96, 128	ECHO_TAIL_LENGTH. This subfield specifies the echo tail length in milliseconds.
VOICE	Unchanged	None	OFF, CONSERV, AGGRESS	VOICE_DETECTION. This specifies the level of voice detection. The default offered is OFF.
CMFNOISE	Unchanged	None	ENABLE, DISABLE	CMFNOISE. This specifies if comfort noise is provided. The default offered is DISABLE.
T38	Unchanged	None	ENABLE, DISABLE	T38. This specifies if T38 fax is supported. The default offered is DISABLE.
RFC2833	Unchanged	None	ENABLE, DISABLE	RFC2833. This specifies if RFC2833 is supported. The default offered is DISABLE.
RTCP	Unchanged	INTERVAL	N,Y	RTCP. This specifies if RTCP is active. The default offered is N.
		INTERVAL	1 TO 60	INTERVAL. This subfield specifies the RTCP interval when field RTCP is set to Y.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TONESET	Unchanged	None	NORTHAMERICA,SPAIN,UK,FRANCE,PORTUGAL,BELGIUM,GERMANY,NETHERLANDS,SWEDEN,AUSTRIA,ITALY,SWITZERLAND,AUSTRALIA,BRAZIL,IRELAND,MEXICO,ISRAEL,ROMANIA,TURKEY,CZECH,CHINA,TAIWAN,KOREA,JAPAN,PANAMA,ARGENTINA,GREECE,POLAND,NEWZEALAND,SINGAPORE,VENEZUELA,CHILE,HONGKONG,MALAYSIA,PHILIPPINES,THAILAND,INDIA	TONESET. This specifies the unique tonset to be utilized based on the resident country. The default offered in NORTHAMERICA.
LOGINT	Unchanged	None	1 TO 120	LOGINT. This specifies the log interval. The default offered is 5.
CRCERROR	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for CRC error logs. The default offered is 20, 10.
USIZEPKT	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the undersize packet logs. The default offered is 20, 10.
OSIZEPKT	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the oversized packet logs. The default offered is 20, 10.
FRAGMENT	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the fragments logs. The default offered is 20, 10.
JABBER	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the jabber logs. The default offered is 20, 10.
DROPEVNT	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the drop event logs. The default offered is 20, 10.
BRDCAST	Unchanged	RISE, FALL	0 T0 100	MNPARM_THRESHOLD. This specifies the settings for the broadcast logs. The default offered is 20, 10.
JITTER	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the jitter logs. The default offered is 20, 10.
LATENCY	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the latency logs. The default offered is 20, 10.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
VPKTLOST	Unchanged	RISE, FALL	0 TO 100	MNPARM_THRESHOLD. This specifies the settings for the voice packets lost logs. The default offered is 20, 10.
MINLOG	Unchanged	None	0 TO 1000000	LOG_REPORT_MIN_VOLUME. This specifies the minimum packet volume for log reporting. The default offered is 1000.
OMPARMS	Unchanged	RTPLOSTE, JTREXC, LATEXC	1 TO 100, 1 TO 3000, 1 TO 3000	OMPARMS. This specifies operational measurement parameters. RTPLOSTE specifies the threshold value of RTP packets lost for pegging a particular OM. JTREXC specifies the threshold jitter value for pegging a particular OM. LATEXC specifies the threshold latency value for pegging a particular OM.
DIFFSERV	Unchanged	EF_CODEPOINT	6-bits as ASCII, prefixed by “CP” for CodePoint, ie:CP101110	The codepoint for voice band defaults to CP101110
	Unchanged	EF_PRIORITY	0 TO 7	The priority for voice defaults to 6
	Unchanged	CS5_CODEPOINT	6-bits as ASCII, prefixed by “CP” for CodePoint, ie: CP101000	The codepoint for signalling data defaults to CP101000
	Unchanged	CS5_PRIORITY	0 TO 7	The priority for signalling defaults to 6
MEDINTEG	Unchanged	None	ENABLE or DISABLE	Indicates the state of Media Integrity on this GEM card, defaults to DISABLE

2.5.2.1.5 Datafill example

The following example shows sample datafill for table MNIPPARM.

Figure 3 Datafill for table MNIPPARM

```
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
---------------------------------------------------------------------------
IWSPM G729 G711ULAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
BOTTOM
```

Codec information is already provisionable in default codec[DFCODEC] and preferred codec[PRFCODEC] fields of MNIPPARM table. This feature only adds new values to support full provisioning of codec.

Following new values are added in default codec and preferred codec fields in MNIPPARM table as shown in Figure 4, “New codec values.’

Table 4 New codec values.

Field	Entry values prior to this feature	Entry values after this feature.
DFCODE	G711ALAW, G711ULAW	G711ALAW, G711ULAW, G729
PRFCODEC	NONE, G729	NONE, G729, G711ALAW, G711ULAW

Provisioning of both DFCODEC and PRFCODEC fields with the same values are blocked. The error message is displayed as shown in Figure 4, “Error msg display when same value given to both DFCODEC and PRFCODEC fields.’

Figure 4 Error msg display when same value given to both DFCODEC and PRFCODEC fields.

```
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G711ULAW NONE 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
>cha
>JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
DFCODEC: G711ULAW
>G711ULAW
PRFCODEC: NONE
>G711ULAW
.........
.........
.........
.........
ERROR: DFCODEC and PRFCODEC values should be unique.
TUPLE TO BE CHANGED:
IWSPM G711ULAW G711ULAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE
ENABLE N NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20
10 20 10 1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
```

Provisioning of both DFCODEC and PRFCODEC fields with the G711 values are blocked. The error message is displayed as shown in Figure 4, “Error msg display when same value given to both DFCODEC and PRFCODEC fields.’

Figure 5 Error msg display when G711 given in both DFCODEC and PRFCODEC fields.

```
MNKEY DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG ECAN
VOICE CMFNOISE T38 RFC2833 RTCP TONESET LOGINT CRCERROR USIZEPKT OSIZEPKT
FRAGMENT JABBER DROPEVNT BRDCAST JITTER LATENCY VPKTLOST MINLOG OMPARMS
DIFFSERV MEDINTEG
------------------------------------------------------------------------
IWSPM G711ULAW NONE 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE ENABLE N
NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10
1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
>cha
>JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
DFCODEC: G711ULAW
>G711ULAW
PRFCODEC: NONE
>G711ALAW
.........
.........
.........
.........
ERROR: Both DFCODEC and PRFCODEC should not have G711 value.
TUPLE TO BE CHANGED:
IWSPM G711ULAW G711ALAW 10 0 0 0 100 0 ENABLE 6 128 OFF DISABLE DISABLE
ENABLE N NORTHAMERICA 5 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20 10 20
10 20 10 1000 50 1000 1000 CP101110 6 CP101000 6 DISABLE
```

Following combinations are allowed to provision in DFCODEC and PRFCODEC fields of MNIPPARM table.

Table 5 DFCODEC and PRFCODEC in MNIPPARM table.

Preferred codec	Default codec
None	G711ALAW
None	G711ULAW
None	G729
G711ALAW	G729
G711ULAW	G729
G729	G711ALAW
G729	G711ULAW

2.5.2.1.6 Table release history update
Table MNIPPARM was created in the SN06 software release.

2.5.2.1.7 Supplementary information
None.

2.5.2.1.8 Translation verification and other tools
MNIPPARM does not use translation verification tools.

Product = CS 2000

A00008629 -- GEM-II AAL2 IW-SPM SN09 Core Preparation Work
Functional Description

1: Applicable Solution(s)
PT-AAL1, PT-IP

Notice a change in nomenclature. When referencing the original GEM card or GEM RM, GEM means “GigE Module” for IP applications. But when referencing the new GEM-II card, GEM means “Generic Equipment Module” since GEM-II can support either Gig-E (IP) and AAL2 applications.

1.1 Description
This activity implements all Core work in SN09 for the AAL2 ATM feature being delivered in MTX14. The AAL2 IW-SPM feature will allow customers of CDMA Wireless MTX switches to extend their ENET connected peripherals to ATM networks for voice and data call processing over AAL2 connections.

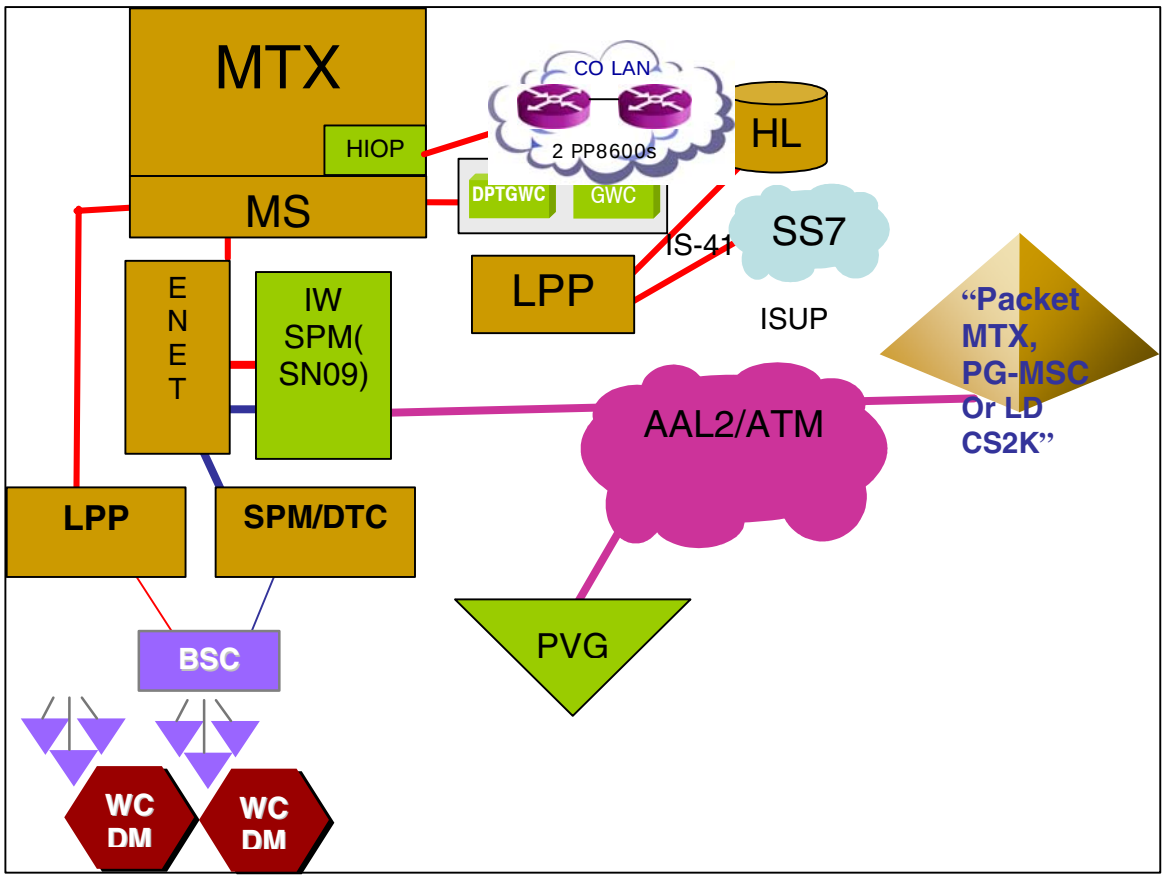
The ATM/AAL2 RM, based on the new ‘Generic Equipment Module 2’ (GEM-II) NTLZ20DA circuit pack, will be delivered as part of the Succession IW-SPM product offering beginning in the MG4K23 release. The GEM-II hardware is being introduced in SN09/MG4K22 as a replacement for the ‘Giga-bit Ethernet Module’ (GEM) RM which supports IP applications. The GEM-II RM has additional hardware capability of supporting ATM based applications over AAL2. The GEM-II runs on an IW-SPM configured as IP or AAL2. The GEM II provides PQII, TI DSPs (on board), winpath787, ECAN tone detection, generation, vocoding, etc.

Working AAL2 functionality will be delivered in MTX14, which is based on SN09 and MG4K23. The required AAL2 local code in the CEM and RM will be delivered in MG4K23. The A00008629 Core activity is being done in SN09

as a preparation activity to avoid later patching of the Core. With activity A00008629, the customer can datafill an IW-SPM as AAL2 bearer fabric with NTLZ20DA as an ATM RM. The customer can also datafill the AAL2 protocol parameters and the five required ATM carriers (same 5 that are required on AAL1 ATMs). A single office parm will control whether the AAL2 IW-SPM feature is active; this parm is "off" by default and should be enabled in MTX14 once the production MG4K23 loads become available.

Figure 1 below shows a network diagram of a wireless MTX switch with the AAL2 IW-SPM bridging calls from SPM/DTC over AAL2 to PVG.

Figure 1 Wireless Base Station Network using IW-SPM AAL2 solution. that



Note there is also a TDM bearer path connection between BSC and PVG.

1.2 Hardware Requirements or Dependencies

The new NTLZ20DA GEM-II circuit pack is being introduced in SN09 for IP applications running on a GEM-type RM. In MTX14, this same NTLZ20DA pack can be configured in software to work as an ATM RM providing AAL2 connectivity.

The GEM-II pack provides these external user interfaces on the faceplate, listed in top-down order:

1. Red triangular LED: works like standard SPM RM to indicate OOS status. When lit, card is OOS; when blank, card is InSv.
2. Green square LED: works like standard SPM RM to indicate activity status. When lit, card is active; when blank, card is in standby mode.
3. Green circular LED labeled “LINK”: lights steady to indicate signal is being received; blank if no signal is being received. For AAL2 application, this signal would be the SONET signal from the far end. For IP application, this signal would be the Ethernet signal from the CS2K.
4. SFP (Small Form Pluggable) connector: for IP applications, this connector accepts a MT-RJ or LC plug that provides GigE (Gigabit Ethernet) interface for 1000B-SX or 1000B-LX. For AAL2 applications, this connector accepts a LC plug that provides OC3 SONET interface for SR (Short Reach), IM (Intermediate Reach), or LR (Long Reach). The SFP connector is compliant with specification SFF-8472 revision 9.3 (produced by the SFF Committee).

For AAL2, the transmit and receive SONET fibers are connected to an OC3 SONET plug inserted in the SFP. Note that the SFP interface is considered part of the cable and hence will not be ordered with the card.

The supported cable types for both SONET and GigE applications are:

a. single mode: good up to 5-6km and always uses a laser.
b. multi mode: good up 500m and can use LED instead of laser.

1.3 Software Requirements or Dependencies

A new GM2xxxx firmware load will be introduced in SN09/MG4K22 for the GEM-II configured as GEM RM for IP application.

In MG4K23, a new AL2xxxx load will be introduced to provide the AAL2 application on the GEM-II card. This new AL2xxxx load will only be supported on a GEM-II card configured as an ATM RM on a IW-SPM configured for AAL2 ATM fabric.

CEM changes are also required in MG4K23 for the IWSxxxx load to support AAL2 on the IW-SPM.

1.4 Limitations and restrictions

1. Attempts to load or RTS AAL2 ATM RM in SN09 are not permitted until the MG4K23 loads are available for the CEM and RM. Hence, AAL2 calls cannot be made until MTX14 when MG4K23 loads are available.
2. The GEM-II card can operate as IP or AAL2, but not both at the same time.

1.5 Interactions

Feature A00007926 was implemented in SN08 to introduce provisioning of the new NTLZ20DA PEC code for IP applications. In SN09, this same NTLZ20DA PEC code can be datafilled for AAL2 applications.

1.6 Applicable customer facing sections

Fault Management

Logs ____X_

Alarms ____X_

Configuration

Data Schema ____X_

User Interface ____X_

Element Management __N/A_

Security __N/A_

Service Order __N/A_

Office Parameters ____X_

Accounting (includes AMA billing) __N/A_

Performance (includes operational measurements) __N/A_

1.7 Glossary

Term	Description
AAL2	ATM Adaption Layer 2
GEM	Gig-E Module (for IP applications)
GEM-II	Generic Equipment Module II (the NTLZ20DA)
PQII	Power Quick II processor
SFP	Small Form Pluggable

2: Configuration for A00008629

2.1 Hardware and Software Requirements

Since AAL2 IW-SPM is a new product introduction, there will be no discussion of how to upgrade an AAL1 or IP IW-SPM to AAL2.

2.2 Initial Configuration

1. To initially configure an AAL2 IW-SPM, first equip an IW-SPM with two NTLX82BA or later CEM packs in slots 7 and 8, and NTLZ20DA GEM-II packs in slots 9 and 10. Only the lower shelf will be used; no other cards should appear on the lower shelf (e.g. No DSP cards since GEM-II has built-in DSP). The upper shelf should be empty.
2. Equip 4 ENET links to each CEM. Four will be needed to realize a capacity 2016 bridges on the IW-SPM (less than 2016 if ECAN used).
3. Plug in OC3 SFP (Small Form Pluggable) connector into the front of each GEM-II card, then connect the SONET TX/RX fibers to this connector. Other end of fiber will connect to AAL2 port on a Passport.
4. Datafill following tables in the order given:
5. Insure network is mu-law as used in North America. A-law (for International) is not currently supported for ATM AAL2.
6. Office parm ECAN_EDGE_STRATEGY in OFCENG should be set to "Y" (same as needed for IP) so DPT GWCs, MG4Ks, and line GWCs will request ECAN on the IW-SPM.
7. Office parm AAL2_ATM_ENABLE in OFCENG should be set to "Y" so NTLZ20DA ATM RM can be added to an AAL2 IW-SPM.
8. CLLI: add ENET_TO_AAL2 tuple with ADMININF ENET_TO_AAL2_POOL.
9. BEARNETS: add an AAL2 network fabric.
10. NETBRDGE: add an ENET_TO_AAL2 BRDGCLLI that connects TDM_ENET to ATM_AAL2 with DISPLAY of E_A2.
11. NETPATH: specify path that will use the desired bridge by adding this tuple: "2 (ENET_TO_AAL2) $"
12. NET2NET: show that ENET and AAL2 can connect by changing CONNNETS of NET_AAL2 tuple to: "(TDM_ENET 2) $".
13. MNNODE: add an IW class SPM that is BRDG_ONLY with BRDGCLLI of ENET_TO_AAL2.
14. MNSHELF: add lower and upper NTLX51BA shelves to a NTLX91BA frame; the lower shelf will house the CEM and ATM packs for the IW-SPM, while the upper shelf will remain empty.
15. MNPRTGRP: add ATM_GRP and STS3L_GRP protection groups with revertive N+1 sparing for the IW-SPM.
16. PMLOADS: add AL2xxx load for the AAL2 NTLZ20DA. Insure IWSxxx load available for CEM cards on the IW-SPM.
17. MNCKTPAK: add two NTLX82BA (or later) CEMs in slots 8 and 9. Add two NTLZ20DA GEM-II packs in slots 7 and 8 with AL2xxx load name.

18. ENCDINV: add four ENET crosspoints for the IW-SPM.
19. MNLINK: add four C-side ENET links for the IW-SPM.
20. MNATMIF: add AAL1 and AAL2 parameters by adding a new tuple for IW-SPM.
21. MNMGPIP: add IP over AAL5 signalling info by adding a new tuple for IW-SPM.
22. MNIPPARM: add DIFFSERV for IP over AAL5 signalling by addiing a new tuple for IW-SPM.
23. MNHSCARR: add the 5 ATM carriers to the IW-SPM: two OC3S, two STS3L, and one STS3cP.
24. MAPCI;MTC;NET;SHELF <nn>;CARD <nn> BSY/RTS front and back of the ENET card, then BSY/RTS the 4 ENET links to the IW-SPM.
25. MAPCI;MTC;PM;POST SPM <nn>;SELECT CEM 0: BSY/LOADMOD/RTS each CEM card.
26. MAPCI;MTC;PM;POST SPM <nn>;SELECT ATM 0; BSY/LOADMOD/RTS each ATM RM.
27. MAPCI;MTC;TRKS;CARRIER;POST SPM <nn>;BSY/RTS the five ATM carriers on the IW-SPM, finishing with the STS3cP carriers which will create the bridges.
28. MAPCI;MTC;APPL;BRGMTCE;POST SPM <nn>;BSY ALL;RTS ALL to RTS the bridges on the 4 C-side ENET links and make the bridges available for CallP.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

CM

2.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/CHANGED/DELETED/RELOCATED	Domain (CM or Subnet Management
OFCENG	AAL2_ATM_ENABLE	New	CM

2.3.2 Parameter information

2.3.2.1 AAL2_ATM_ENABLE

Enable AAL2 ATM bearer fabric over IW-SPM with NTLZ20DA GEM-II card.

2.3.2.1.1 Functional description

The AAL2_ATM_ENABLE parameter is required to enable the AAL2 ATM IW-SPM feature, which utilizes the new NTLZ20DA GEM-II card. The parameter is disabled by default. While disabled, the user will not be allowed to datafill an ATM RM with NTLZ20DA PEC code. When enabled, the datafill is allowed.

Here's the warning message shown when user enables this parm:

WARNING: Ensure that production IWSxxx and AL2xxx local loads'

are available for AAL2 IW-SPM before LoadMod/RTS.'

and here's the info message shown when parm is disabled:

INFO: Will no longer be able to datafill AAL2 IW-SPM.

Reason for parm is to control introduction of this new feature where the Core part will be available first in SN09, followed by the Local part in SN10. Once the production IWSxxx AL2xxx loads are available in SN10, this parameter can be enabled by customers wanting to deploy ATM AAL2 traffic.

2.3.2.1.2 Provisioning rules

User should insure that a working/verified AL2xxx load is available before enabling this parameter. Should only be enabled for mu-law networks (i.e. North America). The AAL2 IW-SPM feature does not currently support A-law (e.g. for International).

2.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
N	Y	N

2.3.2.1.4 Activation

Immediate activation. No restart required.

2.3.2.1.5 Dependencies

MNCKTPAK: will not be allowed to datafill NTLZ20DA as ATM RM until this parameter is enabled.

2.3.2.1.6 Consequences

None.

2.3.2.1.7 Verification

Confirm NTLZ20DA can be datafilled as ATM RM.

2.3.2.1.8 Memory requirements
No memory impact.

2.3.2.1.9 Parameter release history update
None.

2.4 Upgrade Impact

2.4.1 Dump and Restore
None. Parameter will default to “N” when dumping from pre-SN09 loads to SN09 or later loads.

2.4.2 Element Management Upgrade
None

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
NETBRDGE	Changed	Unchanged
MNCKTPAK	Changed	Unchanged
MNATMIF	Changed	Unchanged
MNMGPIP	Changed	Unchanged
MNIPPARM	Changed	Unchanged

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name: NETBRDGE
Network Fabric Bridges

2.5.2.1.1 Functional description
Existing table.

2.5.2.1.2 Usage sequence and implications (CM Only)
Tables must be datafilled in the following sequence:

BEARNETS

NETBRDGE

NETPATH

NET2NET

MNNODE

2.5.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
NETBRDGE	0	15	Memory is automatically allocated for 16 tuples.

2.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for NETBRDGE.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
BEARNETS	Changed	none	Select two tuples from table BEARNETS.	Allows selection of the two interfacing network types. For AAL2 IW-SPM, this would be TDM_ENET to NET_AAL2.

2.5.2.1.5 Datafill example

The following example shows sample datafill for table NETBRDGE, NETPATH, and NET2NET:

```
TOP
         BRDGCLLI    BRDGTYPE DISPLAY           BEARNETS
-------------------------------------------------------
     ENET_TO_AAL2 CORE_BRDGE     E_A2 TDM_ENET NET_AAL2
       ENET_TO_IP CORE_BRDGE     E_IP TDM_ENET   NET_IP
BOTTOM

TOP
PATHIDX                                    NETBRDGE
-----------------------------------------------
       0                                          $
       1                        (       ENET_TO_IP)$
       2                        (     ENET_TO_AAL2)$
BOTTOM

TOP
BNETNAME
                                                                        CONNNETS
------------------------------------------------------------------------------
TDM_ENET
```

```
                                                    (  NET_IP    1) (NET_AAL2    2)$
  NET_IP
                                                       (TDM_ENET    1)$
NET_AAL2
                                                       (TDM_ENET    2)$
BOTTOM
```

2.5.2.1.6 Table release history update

Modify NETBRDGE to allow AAL2 network type.

2.5.2.1.7 Supplementary information

Cannot delete a tuple in NETBRDGE until all references to it in MNNODE have been deleted.

Cannot change a tuple network type to/from AAL2 until all references to in MNNODE have been deleted.

2.5.2.1.8 Translation verification other tools

The following example shows the output from MAPCI when it is used to verify Table NETBRDGE.

mapci;mtc;pm;post spm <nn>

```
 XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
Baseln   RExByp   NO AMA     .      3 SPM   5   RS     .      205C..   1 Maj   ATM_8+
  M                *C*              *C*     *C*              *C*       M       *C*
                                     SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit           PM                  1        0       25        0       11       28
 2 Post_          SPM                 0        0        2        0        7        0
 3 ListSet
 4 ListRes    SPM    8  ISTb  Class: IW         BRG_Only  NETBRDGE: E_A2
 5 Trnsl
 6            Shlf0 SL A Stat  Shlf0 SL A Stat  Shlf1 SL A Stat  Shlf1 SL A Stat
 7 ATMConn    -----  1 - ----  CEM 1  8 I ISTb  -----  1 - ----  -----  8 - ----
 8 IPConn     -----  2 - ----  ATM 0  9 A ISTb  -----  2 - ----  -----  9 - ----
 9 OfClk      -----  3 - ----  ATM 1 10 I SysB  -----  3 - ----  ----- 10 - ----
10            -----  4 - ----  ----- 11 - ----  -----  4 - ----  ----- 11 - ----
11 Disp_      -----  5 - ----  ----- 12 - ----  -----  5 - ----  ----- 12 - ----
12 Next       -----  6 - ----  ----- 13 - ----  -----  6 - ----  ----- 13 - ----
13 Select_    CEM 0  7 A ISTb  ----- 14 - ----  -----  7 - ----  ----- 14 - ----
14 QueryPM
15 ListAlm
16 Clock
17 SPERFORM
18 Upgrade_
  RLYNCH4
```

2.5.2.2 Name: MNCKTPAK

SPM Circuit Pack

2.5.2.2.1 Functional description

Existing table.

2.5.2.2.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

MNNODE

MNCKTPAK

ENCDINV

2.5.2.2.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNCKTPAK	0	?	Memory is dynamically allocated.

2.5.2.2.4 Fields/OIDs

The following table lists fields/OIDs for MNCKTPAK.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PEC	Changed	none	NTLZ20DA	Specifies the new GEM-II pack that can operate as AAL2 (for ATM RM) or IP (for GEM RM)
LOAD	Changed	none	AL2nnnn GM2nnnn	Select valid tuple from table PMLOADS. New AL2nnnn load for AAL2 ATM, or new GM2nnnn load for IP GEM.

2.5.2.2.5 Datafill example

The following example shows sample AAL2 datafill for table MNCTKPAK.

```
     CPKKEY                                                    CPKINFO
                    PEC  RELEASE       LOAD
SPM  8 0  9 ATM 0 1 WORKING (SYSB CR RPT) (MANB MJ RPT)
            (ISTB MN RPT) (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $
            NTLZ20DA       01    AL220AD
SPM  8 0 10 ATM 1 1 SPARE (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
            (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $
            NTLZ20DA       01    AL220AD
```

and this shows sample of NTLZ20DA configured a IP GEM:

```
TOP
            CPKKEY                                                    CPKINFO
                          PEC  RELEASE       LOAD
-------------------------------------------------------------------------------
       SPM  0 0  9 GEM 0 1 WORKING (SYSB CR RPT) (MANB MJ RPT)
                   (ISTB MN RPT) (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $
                   NTLZ20DA       01    GM221BG
       SPM  0 0 10 GEM 1 1 SPARE (SYSB CR RPT) (MANB MJ RPT) (ISTB MN RPT)
                   (PROTFAIL CR RPT) (PATCHFAIL MJ RPT) $
                   NTLZ20DA       01    GM221BG
```

2.5.2.2.6 Table release history update

Modify MNCKTPAK to allow NTLZ20DA GEM-II pack for GEM (IP) and ATM (AAL2) RM types.

2.5.2.2.7 Supplementary information

For GEM RMs, the NTLZ20DA acts as a replacement for the earlier NTLZ20BA and NTLZ20CA packs which are being discontinued due to parts obsolesence. Standard upgrade practice is used to go from NTLZ20BA/CA to the newer DA: BSY GEM, change PECCODE to NTLZ20DA and LOAD to GM2xxxx, LoadMod, RTS GEM.

For ATM RMs, the NTLZ20DA is allowed on IW-SPM class node assigned as BRDG_ONLY with BEARNETS field (in MNNODE) that supports AAL2 fabric. OFCENG parameter AAL2_ATM_ENABLE must be enabled before NTLZ20DA can be assigned as an AAL2 ATM RM.

2.5.2.2.8 Translation verification other tools

The following example shows the output from MAPCI when it is used to verify Table MNCKTPAK.

mapci;mtc;pm;post spm <nn>;select atm <n>

```
             XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
Baseln   RExByp   NO AMA      .       3 SPM   5    RS     .      205C..    1 Maj   ATM_8+
  M                *C*                *C*     *C*                *C*       M       *C*
                                      SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit          PM                      1        0       25        0       11       28
 2               SPM                     0        0        2        0        7        0
 3 ListSet         ATM                   1        0        0        0        1        0
 4
 5            SPM 8    ATM 0    Act    ISTb
 6 Tst
 7 Bsy        Loc : Row M  FrPos 40 ShPos  6 ShId 0 Slot  9   Prot Grp : 1
 8 RTS        Default Load: AL220AD                          Prot Role: Working
 9 OffL
10 LoadMod
11
12 Next
13 Select_
14 QueryMod
```

```
15 ListAlm
16 Prot
17 SPERFORM
18
  RLYNCH4
```

Here's an example for the GEM RM:

mapci;mtc;pm;post spm <nn>;select gem <n>

```
 XAC       MS      IOD      Net       PM      CCS      Lns      Trks     Ext      APPL
Baseln   RExByp   NO AMA     .      3 SPM   5   RS      .      205C..   1 Maj   ATM_8+
  M                *C*              *C*     *C*                *C*      M       *C*
                                     SysB     ManB     OffL     CBsy     ISTb     InSv
 0 Quit           PM                   1        0       25        0       11       29
 2                SPM                  0        0        2        0        7        0
 3 ListSet          GEM                0        0        1        0        1        0
 4
 5             SPM    0 GEM    0  Act     ISTb
 6 Tst
 7 Bsy         Loc : Row N  FrPos 31 ShPos  6 ShId 0 Slot  9    Prot Grp : 1
 8 RTS         Default Load: GM221BG                            Prot Role: Working
 9 OffL
10 LoadMod
11
12 Next
13 Select_
14 QueryMod
15 ListAlm
16 Prot
17
18
  RLYNCH
```

2.5.2.3 Name: MNATMIF

SPM ATM Protocol Interface Parameters

2.5.2.3.1 Functional description

Existing table that specified AAL1 ATM protocol parameters. Adding AAL2 ATM protocol parameters. An AAL2 RM will need both the AAL1 and AAL2 protocol parameters.

2.5.2.3.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

MNLINK

MNATMIF

MNMGPIP

2.5.2.3.3 Size

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNATMIF	0	86	Memory is dynamically allocated as each ATM node is added.

2.5.2.3.4 Fields/OIDs

The following table lists fields/OIDs added to table MNATMIF for AAL2 IW-SPMs.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
CIDPRSVC	New	none	1..247	Specifies the maximum number of AAL2 CIDs that may be allocated on an AAL2 SVC. The local node may allocate no more than this number of trunks. Default value is 10. Note: value used in IW-SPM will be 10 (despite setting here) till a follow-up notice issued indicated IW-SPM will follow this table value.
PRECREAT	New	none	Y or N	Specifies whether Pre-creation of SVCs is enabled. If svcPreCreation is enabled, then an SVC set up is initiated when the bandwidth available in existing VCCs (between two NSAP addresses) is such that a new SVC would be required for the next call. Default Y for enabled.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
TIMERCU	New	none	0..15875 nsec in 125 usec steps	Maximum period of time in usec (micro seconds) before a partially filled AAL2 packet is scheduled for transmission. Default 0 usec. Note 1000 usec = 1 msec.
SVCHOLD	New	none	0..600 sec in 1 sec steps	Length of time that an AAL2 SVC is kept up after the last narrowband call to use it has been deleted. This attribute is used to modify the SVC caching system. Longer values result in larger caches of SVCs. Default 180 sec to match PVG.
SRVCAT	New	none	CBR (Constant Bit Rate) or VBR (Variable Bit Rate)	ATM Service Category for SVC. Default is VBR.
PKCLRT	New	none	0..353207	Peak cell rate of the ATM connection on a per SVC basis. Default is 800 cells per sec.
SUSTCR	New	none	0..353207	Sustained cell rate of the ATM connection on a per SVC basis. Default is 800 cells per sec

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
MAXBURSZ	New	none	0..353207	Maximum burst size of the ATM connection on a per SVC basis. This “burst” defines how far beyond PKCLRT the connection will go before cells are dropped. Default is 0 cells
REMADDR	New	none	40 character address	ATM address of the node that may be reached.
CODEC	New	none	G711 (other values to be added in future)	Type of on-board CODEC in-use. Allows up to 16 different CODECs to be specified. Default is G711.
SILSUP	New	none	Y or N	Whether silence suppression is enabled or not. Default is Y for enabled.
MAXBRI	New	none	0..2016	Max number of bridges provided by an AAL2 IW. If silence suppression (SILSUP) is disabled, the max bridges possible is 1865. Allows telco to limit the traffic over an AAL2 IW-SPM. Default is 2016.

2.5.2.3.5 Datafill example

The following example shows sample datafill for table MNATMIF.

ATMKEY

ATMDATA

SPM 8

V40 PRIV BOTH 1 2300 8 16 255 32 2048 2048 PASSPORT RTPH_SPM_8 Y USER N NSAP

39345678901234567890A4A4A4F402F678901200 4 25 67 16 2048 2048 1000 2000 7000

15000 750 180 4 30 30 4 4 10 110 110 4 Y 0 180 VBR 800 800 0

39345678901234567890A4A4A4F402F678901201 Y G711 Y 2016

2.5.2.3.6 Table release history update

Modify MNATMIF to add AAL2 protocol parameters.

2.5.2.3.7 Supplementary information

Cannot CHAnge or DELete a tuple for AAL2 IW-SPM unless that node is OOS.

2.5.2.3.8 Translation verification other tools

None

2.5.2.4 Name: MNMGPIP

SPM IP Protocol Parameters

2.5.2.4.1 Functional description

Existing table. Normally applies to IP nodes, but AAL2 IW-SPM needs it to specify parameters for IP over AAL5 signalling.

2.5.2.4.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

MNATMIF

MNMGPIP

MNHSCARR

2.5.2.4.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNMGPIP	0	86	Memory is dynamically allocated as each IP/AAL2 node is added.

2.5.2.4.4 Fields/OIDs

The following table lists fields/OIDs for MNMGPIP.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GEMSIGIP	Changed	none	same	Change to allow this field for AAL2 IW-SPM.
SIGMASK	Changed	none	same	Change to allow this field for AAL2 IW-SPM.
SIGGWIP	Change	none	same	Change to allow this field for AAL2 IW-SPM.

2.5.2.4.5 Datafill example

The following example shows sample datafill for table MNMGPIP.

```
            MGPKEY
          GEMSIGIP           SIGMASK           SIGGWIP
-------------------------------------------------------------------
       SPM  0 0  9
   172  16 121  11  255 255 255   0  172  16 121   1
       SPM  0 0 10
   172  16 121  11  255 255 255   0  172  16 121   1
```

2.5.2.4.6 Table release history update

Modify MNMGPIP to add AAL2 parameters.

2.5.2.4.7 Supplementary information

Cannot CHAnge or DELete a tuple for AAL2 IW-SPM unless that node is OOS.

2.5.2.4.8 Translation verification other tools

None.

2.5.2.5 Name: MNIPPARM

SPM IP Protocol Parameters

2.5.2.5.1 Functional description

Existing table. Normally applies to IP nodes, but AAL2 IW-SPM needs it to specify parameters for IP over AAL5 signalling.

2.5.2.5.2 Usage sequence and implications (CM Only)

Tables must be datafilled in the following sequence:

MNMGPIP

MNIPPARM

MNHSCARR

2.5.2.5.3 Size

Table 12 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MNIPARM	0	86	Memory is dynamically allocated once when first .

2.5.2.5.4 Fields/OIDs

The following table lists fields/OIDs for MNIPPARM.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DIFFSERV	Changed	none	same	Change to allow this field for AAL2 IW-SPM.

2.5.2.5.5 Datafill example

The following example shows sample datafill for table MNIPPARM.

```
MNKEY  DFCODEC PRFCODEC PKTRATE INGRESS EGRESS JITMIN JITMAX JITTARG
         ECAN   VOICE CMFNOISE     T38 RFC2833 RTCP      TONESET LOGINT
CRCERROR USIZEPKT OSIZEPKT FRAGMENT  JABBER DROPEVNT BRDCAST  JITTER LATENCY
VPKTLOST  MINLOG         OMPARMS              DIFFSERV
              MEDINTEG
-------------------------------------------------------------------------------
IWSPM G711ULAW     NONE      10       0       0      0    100       0
     DISABLE      OFF  DISABLE DISABLE  ENABLE   N  NORTHAMERICA      5
  20  10   20  10   20  10   20  10  20  10   20  10  20  10  20  10  20  10
  20  10    1000  50  1000  1000 CP101110 6 CP101000 6
             DISABLE
```

2.5.2.5.6 Table release history update

Modify MNIPPARM for AAL2 IW-SPM.

2.5.2.5.7 Supplementary information

Cannot CHAnge or DEL ete an IW-SPM tuple unless all IW-SPM nodes are OOS.

2.5.2.5.8 Translation verification other tools

None.

2.6 Service Orders (SO) (CM & SESM)

None.

2.7 Software optionality control (SOC)

No SOC. Feature activation will be controlled thru AAL2_ATM_ENABLE office parameter in OFCENG.

2.8 Element Management

None

2.9 Command interface changes

IWCOMMCI is the only user tool changed by this feature. Two designer-only tools are also impacted (IWBMCI and IWSELCI), but they will not be covered in this user section.

2.9.1 Directory: IWCOMMCI

2.9.1.1 Directory description

Resident tool for commissioning an IW-SPM.

2.9.1.2 Accessing directory: IWCOMMISSION

2.9.1.2.1 Access to directory or MAP level and return to CI

To access IWCOMMISSION from the CI environment, enter IWCOMMCI.

To return to the CI environment, enter QUIT.

2.9.2 Command: BSY_IW

2.9.2.1 Command type: NON-MENU

2.9.2.2 Command target: All

2.9.2.3 Command availability: RES

2.9.2.4 Command description

Manually Busy bridges on a select ENET link on the IW-SPM.

2.9.2.5 Command syntax

Table 14 BSY_IW command parameters and variables

Command	Parameters and variables
BSY_IW	<SPM number> (0..85) ~~<Bridging type> (ATM, IP)~~ <Link number> (0..3) <Keep CPB calls up> (KEEP, KILL)
Parameters and variables	Description
Link number	The ENET link on the IW-SPM
Keep CPB calls up	Whether bridges with CPB calls should remain up or busied out. Optional parameter that defaults to KILL

The only change to the BSY_IW command is removal of the “Bridging type” parameter. The system will now rely on the setting in MNNODE’s BEARCLLI field to determine if the IW-SPM is ATM AAL1, ATM AAL2, or IP.

No change to the output of these commands, so no further info needs to be provided.

2.9.3 Command: RTS_IW

2.9.3.1 Command type: NON-MENU

2.9.3.2 Command target: All

2.9.3.3 Command availability: RES

2.9.3.4 Command description

Manually Return-to-Service bridges on a select ENET link on the IW-SPM.

2.9.3.5 Command syntax

Table 15 BSY_IW command parameters and variables

Command	Parameters and variables
RTS_IW	<SPM number> (0..85) ~~<Bridging type> (ATM, IP)~~ <Link number> (0..3)
Parameters and variables	Description

Table 15 BSY_IW command parameters and variables

Command	Parameters and variables
Link number	The ENET link on the IW-SPM

The only change to the RTS_IW command is removal of the “Bridging type” parameter. The system will now rely on the setting in MNNODE’s BEARCLLI field to determine if the IW-SPM is ATM AAL1, ATM AAL2, or IP.

No change to the output of this command, so no further info needs to be provided.

2.10 SECURITY

None.

2.11 Configuration Walkthrough

Earlier section on “Initial Configuration” describes the equipment and provisioning required to setup this feature. Setting up CallP to route calls over IW-SPM bridges has not changed (same as IP and AAL1 ATM), so it will not be covered here.

Product = CS 2000

A00008724 -- OMDD Enhancements and Robustness

Functional Description

1: Applicable Solution(s)

PT-AAL1

1.1 Description

This Activity address the following items:

1. implementing a FTP retry mechanism for OMDD application: If FTP fails to send OM reports to any of the configured downstream machines for various reasons like downstream reboot, network congestion, password change and maintenance in downstream etc., those reports will be attempted to be sent to downstream at the next scheduled interval.

2. Improving OMDD audit mechanism: With current design there is a possibility of omdata filesystem getting filled up before the audit happens.

Current audit period is every 6 hours. The improved audit mechanism will ensure that the omdata filesystem will not reach 100% at any instance for the currently supported OM capacity for SN09 release.

3. Enhancing file rotation mechanism: Currently there is a file rotation problem from *open* to *closedNotSent* directory when SDM/CBM and CM are not in sync with respect to time.This will result in configured downstream not receiving OM reports at scheduled time. This activity will make sure that all OM reports will be sent to downstream according to configured schedule.

1.2 Introducing ftp retry mechanism

Currently user can configure OMDD to send OM report to single/multiple downstream destinations. If the ftp fails for some reason, OMDD will not try to send the OM reports downstream again and the files are moved from *closedNotSent* to *closedSent* directory. To be specific, once ftp is attempted for an OM report file, OMDD will move the file to *closedSent* directory irrespective of the success or failure of the file transfer. On failure cases, log will be generated to notify the failure of the file transfer.

In case of failure to transfer the OM reports to downstream destination, this activity will ensure that reports are re-attempted to be sent.

If the OM report transfer fails for any destination, OMDD will keep track of the destination to which the report could not be transferred. At the next File Transfer Schedule, OMDD will attempt to send the report to the destination again. This will be done on every file transfer schedule until

- a successful transfer or
- this file exceeds the retention period of the *closedNotSent* directory or
- the file gets deleted during audit.

1.3 Improving OMDD Audit mechanism

OM reports are stored in omdata filesystem. Currently, this filesystem is audited every 6 hours. During the audit, if omdata filesystem usage is found to be more than 60%, then OMDD generates a warning log to the user stating *"ODM: WARNING omdata storage use exceeds 60 percent. Files will be deleted in next audit if the usage exceeds 70 percent"*.
In the next audit, if omdata filesystem usage is found to be more than 70%, then OMDD deletes all the files from *closedSent* directory. The filesystem usage will be calculated again and if is still more than 50%, files from *closedNotSent* directory will be deleted starting from the oldest file.This procedure is repeated till omdata filesystem usage is less than or equal to 50%. Customer will be notified on deletion of each file from *closedNotSent* directory through *Major* log.

With the current audit interval of 6 hours, there is still a high chance that omdata filesystem might get filled up in between two audits.

This activity will reduce the audit interval to 30 minutes with the following changes:

- Generate Major log when omdata filesystem usage reaches 60%.
- Generate Major Trouble log when omdata filesystem usage reaches 80%.
- Generate Info log and delete all files in *closedSent* directory on reaching 90% usage of omdata filesystem.
- If omdata filesystem usage does not fall below 80% after deletion of all the files in *closedSent* directory, files from *closedNotSent* directory will be deleted starting from the oldest file till the usage reaches 80% or less.
- Generate Info log for each file deletion from *closedNotSent* directory.
- Generate the corresponding Clear logs for all Major logs.

This activity will ensure that omdata filesystem usage will not reach 100% at any instance for the currently supported OM capacity for SN09 release.

1. The following log is generated when audit finds omdata file system usage exceeds 60%.
SDM338 MAJOR TBL SDM OM FILE RETENTION
ODM: Audit finds omdata usage exceeds 60 percent.OM files will be deleted in the next audit if the usage exceeds 90 percent.

2. The following clear log is generated when audit finds omdata file system usage goes below 60%.
SDM638 NONE INFO SDM OM FILE RETENTION
ODM: Audit finds omdata usage has gone below 60 percent.

3. The following log is generated when audit finds omdata file system usage exceeds 80%
SDM338 MAJOR TBL SDM OM FILE RETENTION
ODM: Audit finds omdata usage exceeds 80 percent.OM files will be deleted in the next audit if the usage exceeds 90 percent.

4. The following clear log is generated when audit finds omdata file system usage goes below 80%
SDM638 NONE INFO SDM OM FILE RETENTION
ODM: Audit finds omdata usage has gone below 80 percent.

5. The following log is generated when audit finds omdata file system usage exceeds 90%
SDM639 CRITICAL TBL SDM OM FILE RETENTION
ODM: Audit finds omdata usage exceeds 90 percent.All the OM files from closedSent directory will be deleted now

6. The following log is generated when a file in *closedNotSent* directory is deleted by audit to make morethan 80% available space in omdata file system.
SDM631 MINOR INFO SDM OM FILE RETENTION
ODM:The File<filename> from closedNotSent directory deleted by audit to free up space in omdata.

-where <filename> is the name of the file deleted from *closedNotSent* directory.

1.4 Enhancing File Rotation Timer

OM reports for an office transfer(OT) period will be sent from CM in either 15 or 30 minutes interval based on the CM configuration.When SDM and CM are out of sync by ~3 minutes OMDD fails to trigger the file rotation from *open* to *closedNotSent* directory in accordance with file rotation schedule[FRS]. This causes reports not reaching the downstream on time.

This activity will enhance the file rotation mechanism, so that files are rotated in accordance with FRS even when SDM/CBM and CM are not in sync.

1.5 Hardware Requirements or Dependencies

- SDM with basic configuration
- CBM with basic configuration

1.6 Software Requirements or Dependencies

Latest SDM22/CBM22 load with Table Access and OM Access services should be in service.

CM - SDM/CBM connectivity should be up.

1.7 Limitations and restrictions

None

1.8 Interactions

None

1.9 Glossary

Term	Description
CBM	Core and Billing Manager
CM	Computing Module
FTP	File Transfer Protocol
FRS	File Rotation Schedule
OM	Operation Measurement

Term	Description
OMDD	Operational Measurements and Data Delivery
OT	Office Transfer
SDM	Supernode Data Manager

Product = CS 2000

A00009036 -- Table HOMELRN Option SITE Expansion

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Feature Background

Local Number Portability (LNP) allows users to change local service providers and yet retain their current 10-digit directory number (DN). Location Routing Numbers (LRNs), not DNs, are used to identify the switch serving a ported subscriber.

LRNs are used for routing and billing purposes and are associated with host and remote switching units via table HOMELRN. Table HOMELRN uses the SITE option to assign SITE (remote switching unit) names for a particular non-HOST LRN entry in the table.

To accommodate succession office collapse solutions there is a need to provision more than the current maximum of 10 SITE names that may be associated with a single LRN entry. This activity expands the maximum number of SITE names that can be assigned to the SITE option for an LRN entry in table HOMELRN from 10 to 256.

1.2 Feature Description

This activity affects the provisioning of LRNs for remote switching units in Table HOMELRN. Remote switching units are defined by entries in Table SITE. Prior to SN09, a maximum of 10 SITE names can be associated with a particular LRN entry in Table HOMELRN using the SITE option. This activity allows a maximum of 256 SITE names to be associated with a particular LRN entry in Table HOMELRN using the SITE option.

The option SITE enables multiple site names to be associated with a single LRN. The supported site names are valid names provisioned in Table SITE(i.e. HOST, REM1, REM2,. etc.). The maximum number of SITEs in one tuple is expanded to 256. Once the maximum number of SITE names has been entered for an LRN entry, HOMELRN table control stops prompting for additional SITE names as was done for the prior limit of 10. Other than the new (256) maximum limit for SITE names per HOMELRN entry, there are no other changes to the provisioning capabilities of table HOMELRN.

An external view of the table HOMELRN changes is shown in the following figure.

Figure 1 Table HOMELRN Option SITE Entry Changes

Old Maximum - Up to 10 SITE Names per LRN Example:

TABLE: HOMELRN
AREACODE OFCCODE STNCODE OPTIONS
---
312 858 $ (SITE (REM1) (REM2) (REM3) (REM4) (REM5) (REM6) (REM7) (REM8) (REM9) (REM10) $)**$**

New Maximum - Up to 256 SITE Names per LRN Example:

TABLE: HOMELRN
AREACODE OFCCODE STNCODE OPTIONS
---
312 858 $ (SITE (REM1) (REM2) (REM3) (REM4) (REM5) (REM6) (REM7) (REM8) (REM9) (REM10) **(REM11) (REM12) (REM13) (REM14) (REM15) (REM16) (REM17) (REM18) (REM19) (REM20) (REM21) (REM22) (REM23) (REM24) (REM25) (REM26) (REM27) (REM28) (REM29).....(REM57).....(REM127)..... ..... (REM208).....(REM256)** $)**$**

Note: This capability is NOT under Software Optionality Control (SOC). This capability is an enhancement to LNP00100 functionality.

1.3 Hardware Requirements or Dependencies

There are no hardware requirements or dependencies associated with this functionality.

1.4 Software Requirements or Dependencies

There are no software requirements or dependencies associated with this functionality.

1.5 Limitations and restrictions

No more than 256 SITE names can be associated with an LRN entry in table HOMELRN.

1.6 Interactions

None

1.7 Glossary

Term	Description
New term	Definition
DN	Directory Number
LNP	Local Number Portability
LRN	Location Routing Number
SOC	Software Optionality Control

Product = CS 2000

A00009078 -- ICM Dual CTI

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP, DMS

1.1 Description

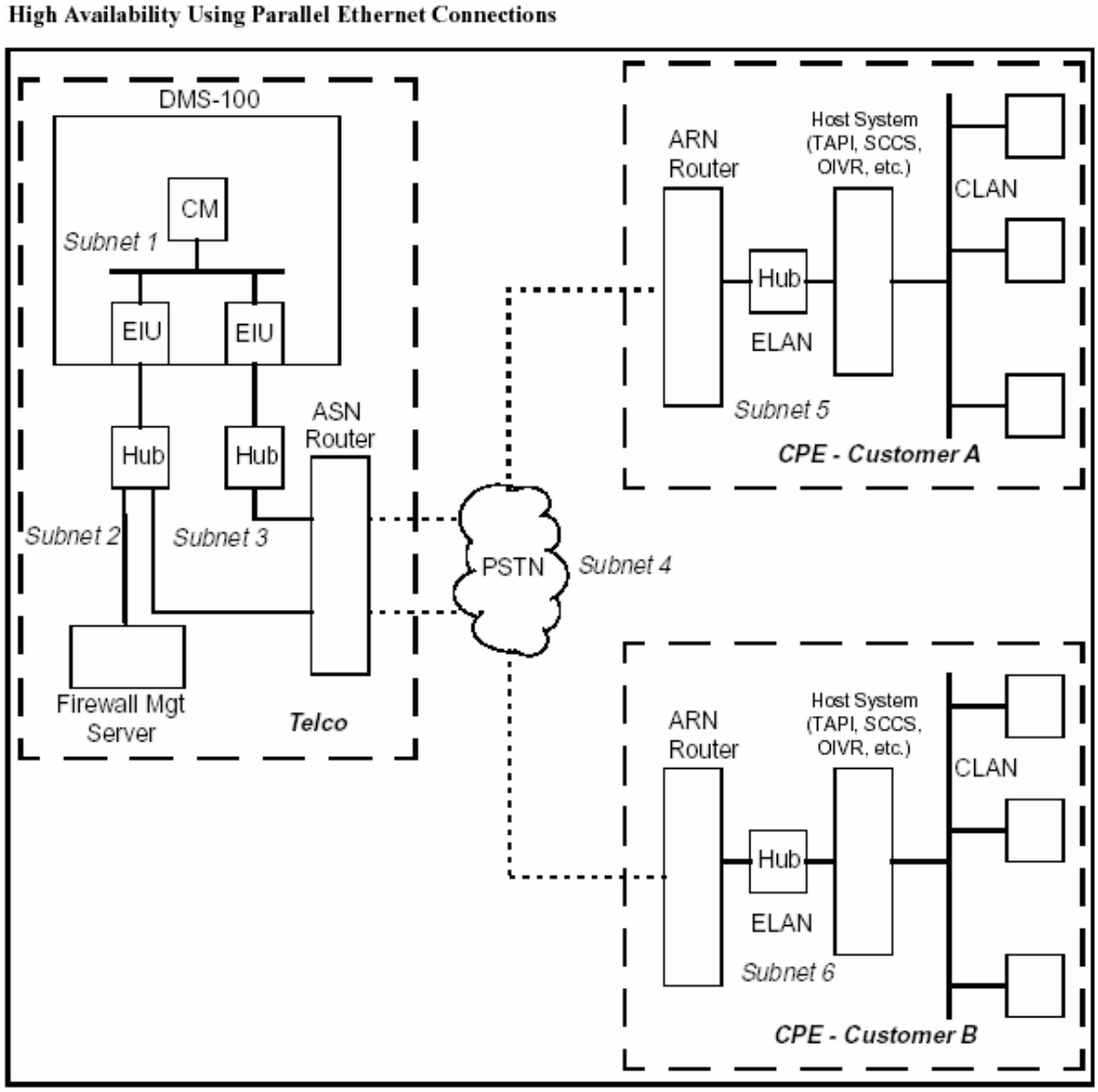
Currently ICM only has one TCP/IP link per linkset. This feature will allow two TCP/IP connections to exist in one SCAI session. The second link will mirror the first link by broadcasting all switch to Host messages except the continuity test messages to both the TCP links. The switch would only expect a response where necessary from the Host through one of the TCP links within the linkset.

This feature does not need more than one EIU to function. The two TCP/IP links within the linkset can connect to a single EIU. It is the customer's

responsibility to provide a reliable and properly configured network. For reliablity, Nortel recommends that the EIU's be configured on separate subnets and be configured in interface mode such that one TCP/IP link within the linkset connects to one EIU within one subnetwork and the other TCP/IP link within the linkset connects to the EIU in the other subnetwork. When EIU's are configured in the interface mode, the Host must use the IP address of the EIUs to connect to DMS-100.

For CS2Kc customers the connection will be made using one IP address for both ICM links within a linkset

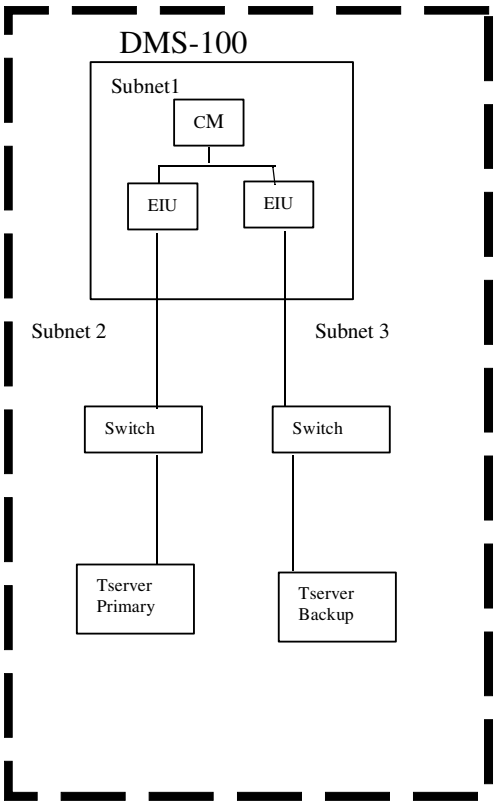
Figure 1 : High Availability Using Parallel Ethernet Connections



In the figure 1 above, the EIUs may be connected to either Eithernet hubs or switches. Hubs are blocking devices which will drop a packet when thereis a packet collision. Switches are non-blocking and should be utilised when there is a possibility of collisions(eg: When other Ehternet devices are connected).

Another simplified configuration can be used if the Tserver and the DMS-100 are co-located, meaning they are not far apart. The allowed distance between the Tserver and DMS-100 for this configuration depends on the hardware specification for each unit used.

Figure 2 Simplified Configuration for High Availability



Please refer to the CN section of this document for details on the datafill needed for this feature to work

1.1.1 Continuity Testing

The continuity test for the TCP links within a linkset will be enhanced to work as it does for multiple X.25 links within a linkset.

The continuity test message will be sent in a round robbin fashion to both links from the DMS. The DMS will wait for the response up to the datafilled response time before it will send it to the next link. DMS will expect a response from the corresponding link on the application. If the DMS does not receive

the response to this test within the response time, the test would have failed for that link after the number of attempts has been exhausted.

If both links fail the test, then the session will be either taken down or not according to how the Terminet parm is datafilled per linkset. When the DMS detects that one of the link has failed, the broadcasting of messages to both links will stop and only the live link will be used to send the ICM messages.

When the continuity test is initiated from the Tservers, the DMS will respond to each of the continuity messages it receives by broadcasting the response to both links.

1.1.2 SOC

This feature uses Software Optionality Control (SOC). The SOC order code is ICM00081. Please refer to the CN section of this document for further details on SOC. This feature will not function if the SOC is not turned on.

1.1.3 OMs & Logs

Changes will be made to the OMs for TCP/IP linksets. The OM will now show the existing registers for each TCP/IP link as a separate tuple.
Example:

Existing tuple

16 TCP_AA

0 0 0 0

Will now appear as

16 TCP_AA **0**

0 0 0 0

If there a two links within a linkset it will appear as below:

21 TCP_BB **0**

0 0 0 0

23 TCP_BB **1**

0 0 0 0

The number next to the linkset name represents the link number within the linkset

No new logs or changes to the existing logs are needed for this feature.

1.1.4 Tools

SCIDBG13: This tools is used to debug the SCAI application. Changes will be made to the following commands in the tool to accommodate the second TCP/IP link within the TCP linkset.

- PRINT

-CLEAR
- RESET

SCAITCP: This is a MAP level tool to monitor the ICM application. The following commands of the tool will be enhanced to accommodate the addition of another TCP/IP link within the TCP linkset.

Query Linkset
Clear SessionID

Clear Linkset

Clear Invokes

Clear Transport

SCAItest Sanity.

1.2 Hardware Requirements or Dependencies

The TCP/IP transport uses the existing TLI interface to provide connectivity between the DMS-100 and a business computer. It also makes use of Local Area Network (LAN) and an internet router. The DMS is provided with LAN connectivity by an Ethernet Interface Unit (EIU). The EIU acts as an router between the DMS-100 and an internet router. If there are more than one link per linkset, the EIUs need to be in an interface mode for reliability. Messages originated from the business computer are routed through internet and finally terminates on a router which is connected to Ethernet LAN and are sent to the EIU which forwards the messages to the destination node on the DMS.

For CS2Kc, a primary and a backup 3PC card will be used to make the TCP/IP connections. Only a single IP address will be available for the Host to connect to the CS2Kc.

1.3 Software Requirements or Dependencies

The feature enhances already existing ICM software to handle the following areas:

- Table Control mechanism to support additional TCP/IP link within a linkset.
- Auditing for two TCP/IP link per linkset.

- OMs and Logs changes for redundant TCP/IPlink per linkset.
- SCAI tools, SCIDBG13 (CI tool) and SCAITEST (MAP level tool).
- This feature also adds new code to support SOC for this feature.

1.4 Limitations and restrictions

Maximum number of TCP/IP connections are 96. No more than 96 service nodes and switches could be connected to a single switch. This is assuming no other applications are using TCP/IP connections from the CM. Therefore the maximum linksets available if all of the TCP/IP linksets are provisioned with two TCP/IP links will be 48.

CS2K will only provide one IP address for the Host to connect to it. Both links will use the same IP address to connect to the CS2K.

1.5 Interactions

This feature will interact with the existing SCAI X.25 transport due to enhancements made in the existing X.25 Table Control mechanism to support two TCP/IP links per linkset.

It will also interact with the current TCP/IP transport implementation that supports a single TCP/IP link per linkset.

1.6 Glossary

Term	Description
IP	Internet Protocol
TCP	Transmission Control Protocol
SCAI	Switch Computer Application Interface
TCP	Transmission Control Protocol

2: Configuration for A00009078

2.1 Hardware and Software Requirements

For DMS-100, at least two EIUs are needed it the customer wants each TCP/IP links to connect to different EIUs.

For CS2Kc, a primary and a backup 3PC card (Ethernet card) is needed.

2.2 Initial Configuration

Subscription to this feature has to be done according to the DS section. SOC for this feature needs to be turned on. EIU needs to be configured as in

interface, if the customer wants each TCP/IP links to connect to different EIU's.

2.3 Upgrade Considerations

2.3.1 Dump and Restore (CM)

Al l of the existing TCP/IP linksets with one link will remain the same after a Dump and Restore.

All of the existing OMs for TCP/IP linksets will remain with a slight change of a link number of 0 appearing after the linkset name.

2.3.2 Element Management Upgrade

2.3.3 Downgrade impact

2.4 Data schema (DS) (CM, MIBS, RDB)

2.4.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
SCAICOMS	Changed	NEW

2.4.2 Table/MIB/Remote Database Schema information

2.4.2.1 Name: SCAICOMS

SCAI Communications Table

2.4.2.1.1 Functional description

The operating company uses table SCAICOMS to define the CompuCALL (X.25) and ICM (TCP/IP)links.

Changes will be made to support another TCP/IP link within an existing linkset.

2.4.2.1.2 Usage sequence and implications (CM Only)

To support another TCP/IP link within an existing linkset the following changes have to be made.

The datafill of this table is done in the following order for the TCP/IP linksets.

LINKSET: enter the linkset name.

LNKSEL: TCP

IPADDR: ### ### ### ###

Where # is a digit ranging from 0 to 9. Please note that the space should be present after entering each set of digits.

IPADDR: ### ### ### ###

MULTIMSG: Y/N

OPTION: CONTAUD

AUDIT: N

OPTION: $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

> Y

Everything above except the entry in bold exists now. A prompt for a second IP address will be provided. If a customer only wants a single IP address, this will be achieved by typing a $ at the prompt for second IP address.

IPADDR: $

Please look at secion 2.4.2.1.5 for the examples

2.4.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SCAICOMS	0	256 (x.25) + 96 (TCP/IP) = 352	Protected

2.4.2.1.4 Fields/OIDs

The following table lists fields/OIDs for table SCAICOMS.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
IPADDR	Changed	Prompt for another IP address will be displayed	### ### ### ###	IP address. If only one IP address is needed the second prompt for IP address should be cancelled by typing in a $.

2.4.2.1.5 Datafill example

The following example shows sample datafill for table SCAICOMS.

LINKSET: TCP_AA

LNKSEL: TCP

IPADDR: 47 150 19 1

IPADDR: 47 102 3 4

MULTIMSG: N

OPTION: CONTAUD

AUDIT: N

OPTION: $

TUPLE TO BE ADDED

TCP_AA TCP (47 150 19 1) (47 102 3 4) N (CONTAUD N) $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

> Y

Another example for adding just one link.

LINKSET: TCP_BB

LNKSEL: TCP

IPADDR: 47 10 3 2

IPADDR: $

MULTIMSG: N

OPTION: CONTAUD

AUDIT: N

OPTION: $

TUPLE TO BE ADDED

TCP_BB TCP (47 10 3 2) $ N (CONTAUD N) $

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.

> Y

2.4.2.1.6 Table release history update

A prompt for another IPADDR field was added.

2.4.2.1.7 Supplementary information

N/A

2.4.2.1.8 Translation verification and other tools

SCAICOMS does not use translation verification tools.

2.5 Software optionality control (SOC)

Order code ICM00081, ICM Dual Link optionalizes the functionality of the second TCP/IP link within a linkset. When ICM00081 SOC is in the IDLE state, datafill of the second TCP/IP link will be allowed. But the second attempt to connect to a link within the linkset will fail. Only one connection is allowed at a time. second TCP/IP link within a linkset.When ICM00081 SOC is in the IDLE state, datafill of the second TCP/IP link will be allowed. But the second attempt to connect to a link within the linkset will fail. Only one connection is allowed at a time

Table 4 SOC

SOC option name:	ICM
SOC option title:	ICM Dual Link
SOC option control type:	STATE
New SOC option?	Yes
SOC option order code	ICM00081
Option defined in DRU:	CCM
Affected products:	LEC00022, LET00022, LLT00022, SN09, ISN09

Product = CS 2000

A00009085 -- ACD & ICM Capacity Expansion

Functional Description

1: Applicable Solution(s)

PT-AAL1, PT-IP, DMS

1.1 Description

Currently, the following limitations apply to the ACD and ICM capacities in a SL-100 or DMS-100 switch:

1. A maximum of 30,000 ACD Agents can be provisioned.
2. A maximum of 1,024 ACD Groups can be provisioned.
3. A maximum of 256 ACD Subgroups can be defined for a given ACD Group.
4. A maximum of 256 Supervisors can be defined for a given ACD Group.
5. A maximum of 1,024 ACD Agents can be associated with a given ACD Group.
6. A maximum of 511 calls can be simultaneously queued for a given ACD Group.
7. A maximum of 511 incoming overflowed calls can be simultaneously queued for a given ACD Group.

8. A maximum of 100 DNs can be associated with a given ICM Session.

This feature will expand these capacities to the following limits:

1. The maximum number of ACD Agents per switch will be increased to 99,999.
2. The maximum number of ACD Groups per switch will be increased to 5,000.
3. The maximum number of ACD Subgroups per Group will be increased to 2,500.
4. The maximum number of Supervisors per ACD Group will be increased to 2,500.
5. The maximum number of ACD Agents per Group will be increased to 10,000.
6. The maximum number of simultaneously queued calls per ACD group will be increased to 8,192.
7. The maximum number of simultaneously queued incoming overflowed calls per ACD Group will be increased to 8,192.
8. The maximum number of DNs that can be associated with a given ICM Session will be increased to 250.

1.2 Hardware Requirements or Dependencies

N/A

1.3 Software Requirements or Dependencies

This feature enhances the existing ACD and ICM software to provide the increased capacities. The following areas will be impacted by this feature:

- Table ACDGRP will be expanded to allow the provisioning of up to 5,000 ACD Groups per switch.
- Table ACDSGRP will be enhanced to allow provisioning of up to 2,500 ACD Subgroups per Group.
- Table ACDLOGIN will be expanded to hold a maximum of 99,999 tuples.
- Table ACDENLOG will be expanded to hold a maximum of 99,999 tuples per partition.
- SERVORD commands (NEW, ADO, NEWACD, CHF, etc.) will be enhanced to support position IDs up to 99999.
- A new ACDMIS protocol version (BCS57) will be defined to support the expanded login and position IDs.
- The ACDMIS load management/remote load management code will be enhanced to support the expanded login and position IDs.

- ACD and ICM Call Processing code will be enhanced to support the expanded login and position IDs.
- ACDDEBUG and ACDSHOW tools will be enhanced to support the expanded login and position IDs.
- Enhancements will be made to the ACD00101 SOC code to support the increase in the maximum number of ACD Agents per switch.

This feature also adds new code to provide the following SOCs to manage the various capacity increases:

- ACD00104 - to control the maximum number of ACD Groups per switch. This SOC will also control the maximum number of ACD Subgroups and Supervisors per Group.
- ACD00105 - to control the maximum number of ACD Agents per Group.
- ACD00106 - to control the maximum number of incoming and incoming overflowed calls per ACD Group.
- ICM00082 - to control the maximum number of DNs that can be associated per ICM Session.

1.4 Limitations and restrictions

It must be noted that all of the capacities described in this document can not be taken to the maximum simultaneously in a given switch.

1.5 Interactions

No changes are made to the existing interactions by this feature.

1.6 Glossary

Term	Description
ACD	Automatic Call Distribution
ACDMIS	ACD Management Information Systems
DMS	Digital Multiplex System
DN	Directory Number
ICM	Intelligent Call Management
SOC	Software Optionality Control

2: Configuration for A00009085

2.1 Hardware and Software Requirements

2.2 Initial Configuration

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

2.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/CHANGED/DELETED/RELOCATED	Domain (CM or Subnet Management
OFCOPT	MAX_NUMBER_ACD_AGENTS_PER_SWITCH	CHANGED	CM

2.3.2 Parameter information

2.3.2.1 MAX_NUMBER_ACD_AGENTS_PER_SWITCH

Maximum Number of Automatic Call Distribution Agents Per Switch

2.3.2.1.1 Functional description

This is a pre-existing office parameter which specifies the maximum number of ACD agent positions that the operating company can provision in the switch.

The purpose of this parameter will not be changed by this activity.

The range of this parameter will be increased to have a maximum value of 99,999. The ability to assign a new value to this parameter is restricted. A new value can only be assigned by changing the limit of the ACD00101 SOC.

When the SOC usage limit is increased or decreased, the value stored in the office parameter is automatically updated to reflect the new limit.

2.3.2.1.2 Range information

Table 2 Range Information

Minimum	Maximum	Default
0	99,999	0

2.3.2.1.3 Memory requirements

No memory impact.

2.3.2.1.4 Parameter release history update

The maximum value is being increased from 30,000 to 99,999 for SN09.

2.4 Upgrade Considerations

None

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 3 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
ACDGRP	CHANGED	UNCHANGED
ACDSGRP	CHANGED	UNCHANGED
ACDMISPL	CHANGED	UNCHANGED
ACDLOGIN	CHANGED	UNCHANGED
ACDENLOG	CHANGED	UNCHANGED

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name: ACDGRP

ACD Group Info.

2.5.2.1.1 Functional description

ACDGRP is an existing table. This table defines ACD groups. Currently, this table can accomodate a maximum of 1,024 tuples. This table will be modified by this activity to accomodate a maximum of 5,000 tuples.

2.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

2.5.2.1.3 Size

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDGRP	0	5,000	Protected

2.5.2.1.4 Fields/OIDs

No change is made to the fields table ACDGRP.

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

2.5.2.1.5 Datafill example

The following example shows sample datafill for table ACDGRP.

2.5.2.1.6 Table release history update

Table is expanded to accomodate a maximum of 5,000 tuples.

2.5.2.1.7 Supplementary information

N/A

2.5.2.1.8 Translation verification and other tools

ACDGRP does not use translation verification tools.

2.5.2.2 Name: ACDSGRP

ACD Sub-Group Info.

2.5.2.2.1 Functional description

ACDSGRP is an existing table. This table defines ACD sub-groups. Currently, this table allows provisioning of a maximum of 256 sub-groups per ACD group. This table will be modified to allow the provisioning of a maximum of 2,500 sub-groups per ACD group.

2.5.2.2.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

2.5.2.2.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDGRP	0	5,000	Protected

2.5.2.2.4 Fields/OIDs

No change is made to the fields table ACDSGRP.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action

2.5.2.2.5 Datafill example

The following example shows sample datafill for table ACDSGRP.

2.5.2.2.6 Table release history update

2.5.2.2.7 Supplementary information

N/A

2.5.2.2.8 Translation verification and other tools

ACDSGRP does not use translation verification tools.

2.5.2.3 Name: ACDMISPL

ACDMIS Pool Info.

2.5.2.3.1 Functional description

ACDMISPL is an existing table. This table defines ACDMIS Pools. The existing field PROTOCOL is modified to add a new value BCS57.

2.5.2.3.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

2.5.2.3.3 Size

The size of table ACDMISPL is not impacted by this activity.

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory

2.5.2.3.4 Fields/OIDs

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
PROTOCOL	CHANGED	None	BCS24 or BCS25 or BCS26 or BCS27 or BCS29 or BCS30 or BCS31 or BCS32 or BCS33 or BCS34 or BCS35 or BCS42 or BCS43 or **BCS57**	New protocol version BCS57 is added.

2.5.2.3.5 Datafill example

The following example shows sample datafill for table ACDMISPL.

2.5.2.3.6 Table release history update

The PROTOCOL field of the table ACDMISPL is modified to add the new value BCS57.

2.5.2.3.7 Supplementary information

N/A

2.5.2.3.8 Translation verification and other tools

ACDGRP does not use translation verification tools.

2.5.2.4 Name: ACDLOGIN

ACD Login Table.

2.5.2.4.1 Functional description

ACDLOGIN is an existing table. This table maps ACD Login IDs to a corresponding password, if needed. This table also maps Customer groups to the corresponding ACD Login IDs, if requested. This table will be expanded by this activity to accomodate a maximum of 99,999 tuples.

2.5.2.4.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

2.5.2.4.3 Size

Table 10 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDLOGIN	0	99,999	Memory is allocated dynamically through the use of SEGSTOR in blocks of 512.

2.5.2.4.4 Fields/OIDs

The following table lists the fields for ACDLOGIN.

Table 11 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LOGINID	CHANGED	None	5 digit number between 00001 and 99999	The range of ACD Login ID is expanded to accomodate 99,999 Login IDs.

2.5.2.4.5 Datafill example

The following example shows sample datafill for table ACDLOGIN.

2.5.2.4.6 Table release history update

Table is expanded to accomodate a maximum of 99,999 tuples.

2.5.2.4.7 Supplementary information

N/A

2.5.2.4.8 Translation verification and other tools

ACDLOGIN does not use translation verification tools.

2.5.2.5 Name: ACDENLOG

ACD Enhanced Login Table.

2.5.2.5.1 Functional description

ACDENLOG is an existing table. This table allows multiple customer groups the full range of Login IDs for their ACD agents. This table is indexed by a two part key, made up of the Partition Number (PARTNO) and Login ID (LOGINID). This table will be expanded by this activity to accomodate a maximum of 99,999 tuples per partition.

2.5.2.5.2 Usage sequence and implications (CM Only)

Current datafill order is unchanged.

2.5.2.5.3 Size

Table 12 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
ACDENLOG	0	99,999	Memory is allocated dynamically through the use of SEGSTOR in blocks of 512.

2.5.2.5.4 Fields/OIDs

The following table lists the fields for ACDENLOG.

Table 13 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
LOGINID	CHANGED	None	5 digit number between 00001 and 99999	The range of Login ID is expanded to accomodate 99,999 Login IDs.

2.5.2.5.5 Datafill example

The following example shows sample datafill for table ACDENLOG.

2.5.2.5.6 Table release history update

Table is expanded to accomodate a maximum of 99,999 tuples per partition.

2.5.2.5.7 Supplementary information

N/A

2.5.2.5.8 Translation verification and other tools

ACDENLOG does not use translation verification tools.

2.6 Service Orders (SO) (CM & SESM)

This activitty does not introduce any new Service Order commands, LCCs, or options.

2.6.1 Service order change details

When the ACD option is added to a line (ADO, NEW, NEWACD commands), or when ACD option data is changed (CHF command), one of the prompts offered by SERVORD is POSID. Currently, any value between 00001 and 30000 is accepted as valid input for the POSID. This activity will change the acceptable value of POSID to be in the range of 00001 to 99999.

2.6.1.1 How service order options are presented

2.6.1.1.1 Description

The range of valid input for the POSID prompt has been modified to be between 00001 and 99999.

2.6.1.1.2 Example

Figure 1 Example of the ADO command in prompt mode

```
SO:
>ado
SONUMBER:   NOW  3 11  6 AM
>
DN_OR_LEN:
>6218000
OPTKEY:
>1
OPTION:
>acd
ACDGRP:
>acdtest1
ACDSGRP:
>0
IDNUM:
>y
POSID:
>99999
OPTKEY:
>$
COMMAND AS ENTERED:
ADO NOW 3 11 6 AM 6218000 ( 1 ACD ACDTEST1 0 Y 99999 ()()) $
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT
>y
```

Figure 2 Example of the ADO command in no-prompt mode

```
SO:
>ado $ 6218000 1 acd acdtest1 0 y 99999 $
```

The NEW, NEWACD, and CHF commands also offer the POSID prompt when used to manipulate ACD data. Examples of these commands are not provided because the effect of this change is identical to the ADO example shown above.

2.6.1.1.3 Option prompts

Table 14 System prompts for POSID

Prompt	Valid input	Description	Areas affected by prompt
POSID	00001 to 99999	ACD agent position ID	Affects SERVORD commands ADO, NEW, NEWACD, and CHF when used to manipulate ACD option data.

2.7 Software optionality control (SOC)

Table 15 SOC

SOC option name:	ACD00101
SOC option title:	ACD Agent Expansion
SOC option control type:	USAGE
New SOC option?	NO
SOC option order code	00037650
Option defined in DRU:	CCM
Affected products:	NA100, SL100
SOC option name:	ACD00104
SOC option title:	Group Increase to 5K
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	00041836
Option defined in DRU:	CCM
Affected products:	NA100, SL100
SOC option name:	ACD00105
SOC option title:	Agents Per Group Exp
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	00041837
Option defined in DRU:	CCM
Affected products:	NA100, SL100

Table 15 SOC

SOC option name:	ACD00106
SOC option title:	Maximum Queued Calls
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	00041838
Option defined in DRU:	CCM
Affected products:	NA100, SL100
SOC option name:	ICM00082
SOC option title:	DNs Per ICM Session
SOC option control type:	STATE
New SOC option?	YES
SOC option order code	00041839
Option defined in DRU:	CCM
Affected products:	NA100, SL100

2.8 Element Management

N/A

2.9 User interface changes

N/A

2.10 OSSGate Interface Changes

N/A

2.11 Security

N/A

2.12 Configuration Walkthrough

N/A

Product = CS 2000

A00009091 -- Equal Access (EA) LPIC Privilege Routing

Functional Description

1: Applicable Solution(s)

PT-AAL1, PT-IP, DMS

1.1 Introduction

This feature introduces two new capabilities to the SN09 release:

1. The capability to partition a DMS100/CS2000 into multiple Virtual End Offices (VEO) using a new translation attribute intended for public translation capabilities.
2. New LPIC Privilege Routing capability, which is the first functionality to make use of the new VEO partitioning.

Future releases may provide additional enhancements of public translation to utilize the new VEO partitioning capability.

1.2 Description

Two new capabilities are introduced by this feature. Please refer to the following sections for additional information:

- Section 1.2.1 “New Virtual End Office Capability” on page 1121
- Section 1.2.2 “New LPIC Privilege Routing Functionality” on page 1124

1.2.1 New Virtual End Office Capability

With this feature, a DMS100/CS2000 can be partitioned into two or more virtual end-offices. This provides a logical partitioning of originating agents on one DMS100/CS2000 into multiple VEOs.

Table VEONAME is introduced by this feature to provide an inventory of the VEO names. A VEO name is associated with valid “originating EO agent types” through new provisioning option VEONAME, in table XLAPLAN or table CXGRP.

The originating EO agent types that are supported by this activity include:

- All line types (e.g., RES, POTS, IBN, console) in the SN09 release except Line Class Codes (LCC) of *EOW* (Enhanced Outwats) and *ETW* (Enhanced Two-Way WATS).
- IBN trunks
- PRI trunks

- PX trunks (with exception of EWATS agents)
- virtual lines - RCF, RCFEA
- VFGs

VEO functionality is completely optional via provisioning in tables XLAPLAN and CXGRP.

For additional information please refer to the following sections:

- Section 1.2.1.1 “New Table VEONAME” on page 1122
- Section 1.2.1.2 “New option VEONAME, Table XLAPLAN” on page 1123
- Section 1.2.1.3 “New option VEONAME, Table CXGRP” on page 1123

1.2.1.1 New Table VEONAME

New table VEONAME contains the list of VEO names. Each VEO name represents a virtual end office that is partitioned on the DMS100/CS2000.

Table VEONAME can provision up to a maximum of 999 VEO names, with an additional VEO name reserved as nil VEO name (NILV).

Refer to Table 1 for a description of the key field of table VEONAME. The key field VEONAME is a string of up to 16 characters and is mapped to a string range.

Table 1 New Table VEONAME

Key	Values	Comments
Key: VEONAME	CHAR_VECTOR (16)	The table key specifies the Virtual End Office Name.

Following is a provisioning example for new table VEONAME.

Figure 1 Example of Table VEONAME

Table VEONAME:

```
VEONAME
--------------------
NILV
ENDOFFICE1
ENDOFFICE2
```

1.2.1.2 New option VEONAME, Table XLAPLAN

Table XLAPLAN provides an association between End Office (EO) originating agents and their translation types.

New option VEONAME is added to table XLAPLAN. Option VEONAME provides an association between the originating line/trunk agent and the Virtual End Office (VEO). This provides the flexibility to partition the DMS100/CS2000 into multiple virtual end offices.

Example datafill for table XLAPLAN is as follows.

Figure 2 Example datafill of Table XLAPLAN

```
Table XLAPLAN:

XLAPIDX  SCRNCLHSTS  PRTNMZEROMPOS RESINF  OPTIONS  ADMINF
-------------------------------------------------------------------------------------------------
613_P621_0 FR01  613   P621  TSPS Y  RESGRP 0 2 VEONAME ENDOFFICE1   $
```

1.2.1.3 New option VEONAME, Table CXGRP

Table CXGRP (Customer Group Options) is required in local or combined local/toll switches to define the options associated with a PX digital trunk. The PX trunk agent tuple in table TRKGRP contains the field for PX Customer Group which is the index into table CXGRP.

New option VEONAME is added to table CXGRP. Option VEONAME provides an association between the originating PX trunk agent and the Virtual End Office (VEO). This provides the flexibility to partition the DMS100/CS2000 into multiple virtual end offices.

Note: Table CXGRP does not show up in Traver. See Figure 12.

Example datafill for table CXGRP is as follows:

Figure 3 Example datafill of Table CXGRP

```
Table CXGRP:

CUSTKEY SPB CTD FCTDNTER FCTDNTRA FCTDINT EWATS EWATSI
PXOPTION
-----------------------------------------------------------------------------------------
50 N N N N N N N (LPIC CAR1 Y) ( VEONAME ENDOFFICE2 ) $
```

1.2.2 New LPIC Privilege Routing Functionality

The second capability introduced by this activity is LPIC Privilege Routing. When an LPIC is assigned to an originator, the DMS100/CS2000's behavior prior to this feature was to route all intraLATA toll calls to the LPIC. This feature introduces the ability to provision intraLATA toll NPANXX codes as exceptions to LPIC handling. Instead of routing to the LPIC, these NPANXX codes will be handled by the LEC.

A new table LPICPXLA is introduced to allow NPANXX LPIC privilege codes to be provisioned on a per VEO basis. New SOC EQA00032 is also introduced as a call processing and Traver control for the LPIC Privilege Routing capability.

For additional information please refer to the following sections:

- Section 1.2.2.1 "New Table LPICPXLA" on page 1124
- Section 1.2.2.2 "New SOC EQA00032" on page 1126
- Section 1.2.2.3 "Call Processing Enhancements" on page 1127
- Section 1.2.2.4 "Traver Enhancements" on page 1129
- Section 1.2.2.5 "Service Interactions with LPIC Privilege Routing" on page 1139

1.2.2.1 New Table LPICPXLA

New table LPICPXLA is implemented to provision a list of NPANXX codes to be excluded from LPIC routing on per VEO basis. This table will be implemented using digilators for storing the NPNXX Codes and will be using 1 digilator pool of 32k 1-digits blocks.

Table LPICPXLA is accessed during call processing for an originating agent when the following is provisioned:

- VEONAME is provisioned in table VEONAME,

- table XLAPLAN entry for the originating agent's pretranslator has option VEONAME assigned (or for a PX trunk originator, option VEONAME is assigned in table CXGRP),

- and SOC EQA00032 'VEO LPIC Privilege' is turned ON.

Refer to Table 2 for a description of table LPICPXLA. The key field PRIVCODE is made up of two parts:

- VEONM: Virtual End Office Name provisioned in Table VEONAME

- DIGITS: up to six NPANXX digits from the dialled number.

Table control enforcements:

— a VEONAME tuple can not be provisioned as nil VEO name (NILV),

— upto six-digit NPANXX codes are allowed to be provisioned as privilege codes in Table LPICPXLA.

Table 2 New Table LPICPXLA

Key	Values	Comments
Key 1: VEONM	VEO_NAME (String range 0 to 999)	Key 1 specifies the originating subscriber's Virtual End Office Name.
Key 2: DIGITS	DIGIT_REGISTER	Key 2 specifies NPANXX codes provisioned for each VEONAME.

Following is a provisioning example for new table LPICPXLA.

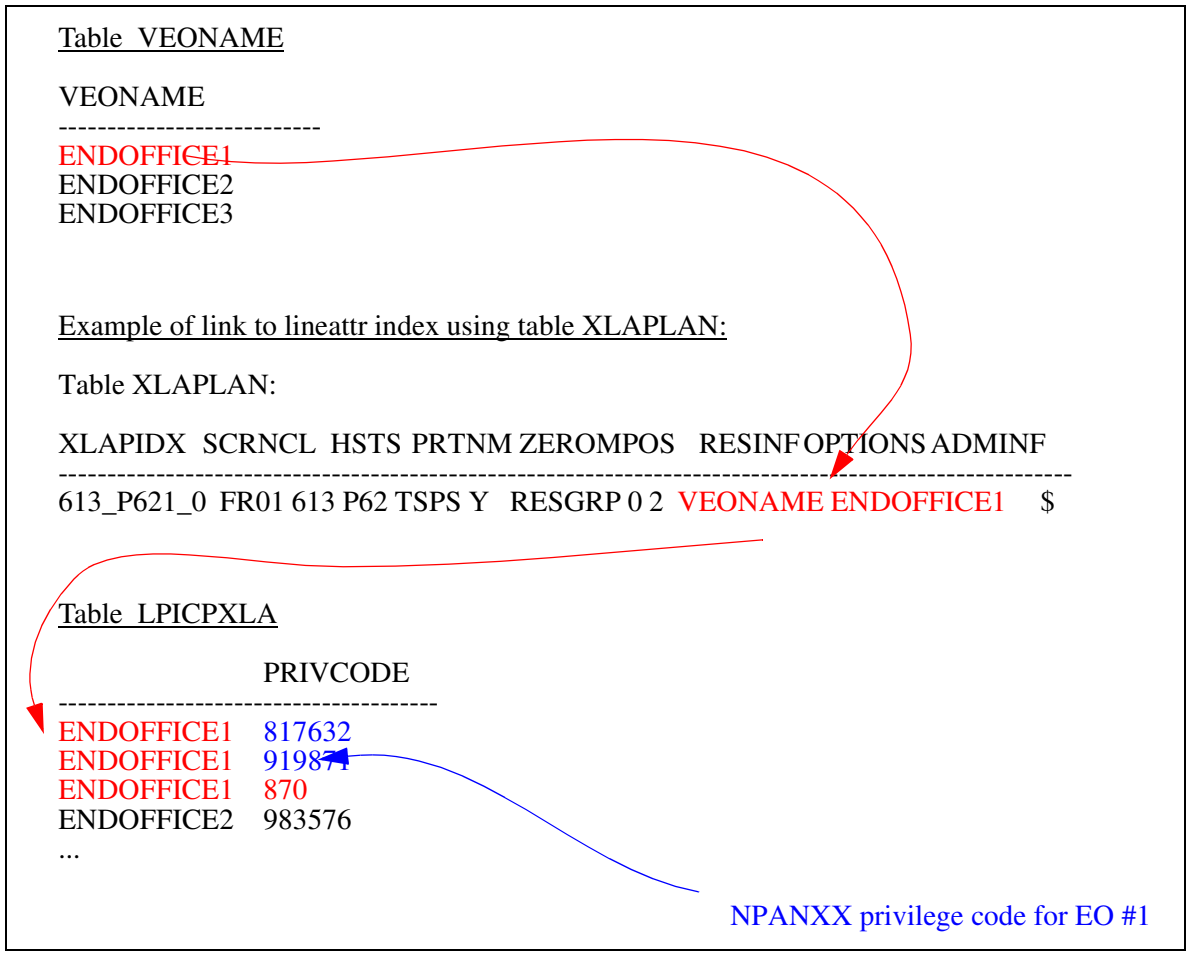
Figure 4 Example of Table LPICPXLA

Table LPICPXLA:

```
                    PRIVCODE
----------------------------------
ENDOFFICE1      919484
ENDOFFICE2      212
```

The following figure illustrates the association between tables VEONAME, XLAPLAN, and LPICPXLA. For additional information please refer to Section 1.2.2.3 "Call Processing Enhancements" on page 1127.

Figure 5 LPIC Exception Routing Datafill



1.2.2.2 New SOC EQA00032

A new state controlled SOC, EQA00032 ‘VEO LPIC Privilege’ is added by this activity. The SOC will have two states: IDLE, ON. This SOC, along with the assignment of the VEONAME option for the originating agent, controls both the call processing and Traver enhancements provided by this activity.

When SOC is in IDLE state:

- Table VEONAME can be provisioned.
- The new option VEONAME can be provisioned in table XLAPLAN and table CXGRP.
- The new option VEONAME can be provisioned in table LPICPXLA with NPANXX privilege codes.
- Table LPICPXLA is not accessed by call processing or by Traver. For further detail, refer to Section 1.2.2.3 “Call Processing Enhancements”

on page 1127, and Section 1.2.2.4 “Traver Enhancements” on page 1129.

When SOC is in ON state:

— Call processing and Traver will both access new table LPICPXLA if the originating agent has VEONAME assigned.

The functional group ordering code for EQA00032 is EQA00001, EQA Local.

All service interactions with SOC EQA00032, including EQA00024 ‘Override LPIC Priv’ feature, are described in Section 1.2.2.5 “Service Interactions with LPIC Privilege Routing” on page 1139.

1.2.2.3 Call Processing Enhancements

The DMS100/CS2000 call processing software is enhanced to support the LPIC Privilege Routing capability. Figures 6 and 7 provide flowcharts of the enhanced call processing behavior. This feature is active only when SOC EQA000032 is set to ON and the originator has a VEONAME assigned.

Supplemental Information for the flowcharts.

1. Deriving LATA status of the call - There are no changes to the method of deriving the LATA status from Table LATAXLA. Existing behavior is to index Table LATAXLA with the originator’s LATA name and the dialed number. If the dialed number is a 7 digit dialplan then originator’s LATA name and the SERVING NPA[1](SNPA) plus the dialed number are used for the index into Table LATAXLA. Special considerations are required for some services. Please refer to Section 1.2.2.5 “Service Interactions with LPIC Privilege Routing” on page 1139, for more details.
2. Performing Look-up in Table LPICPXLA - The index for the new Table LPICPXLA is the originator’s VEONAME and the terminating number. If the terminating number does not contain enough digits to determine if a match is found then more digits must be collected. As with Table LATAXLA, if the dialed number is a 7 digit dialplan then originator’s VEONAME and the SNPA with the dialed digits are used for the index into Table LPICPXLA. Special considerations are required for some services. Please refer to Section 1.2.2.5 “Service Interactions with LPIC Privilege Routing” on page 1139 for more details.

[1] Serving NPA is the NPA of the originating party.

Figure 6 Equal Access Translations

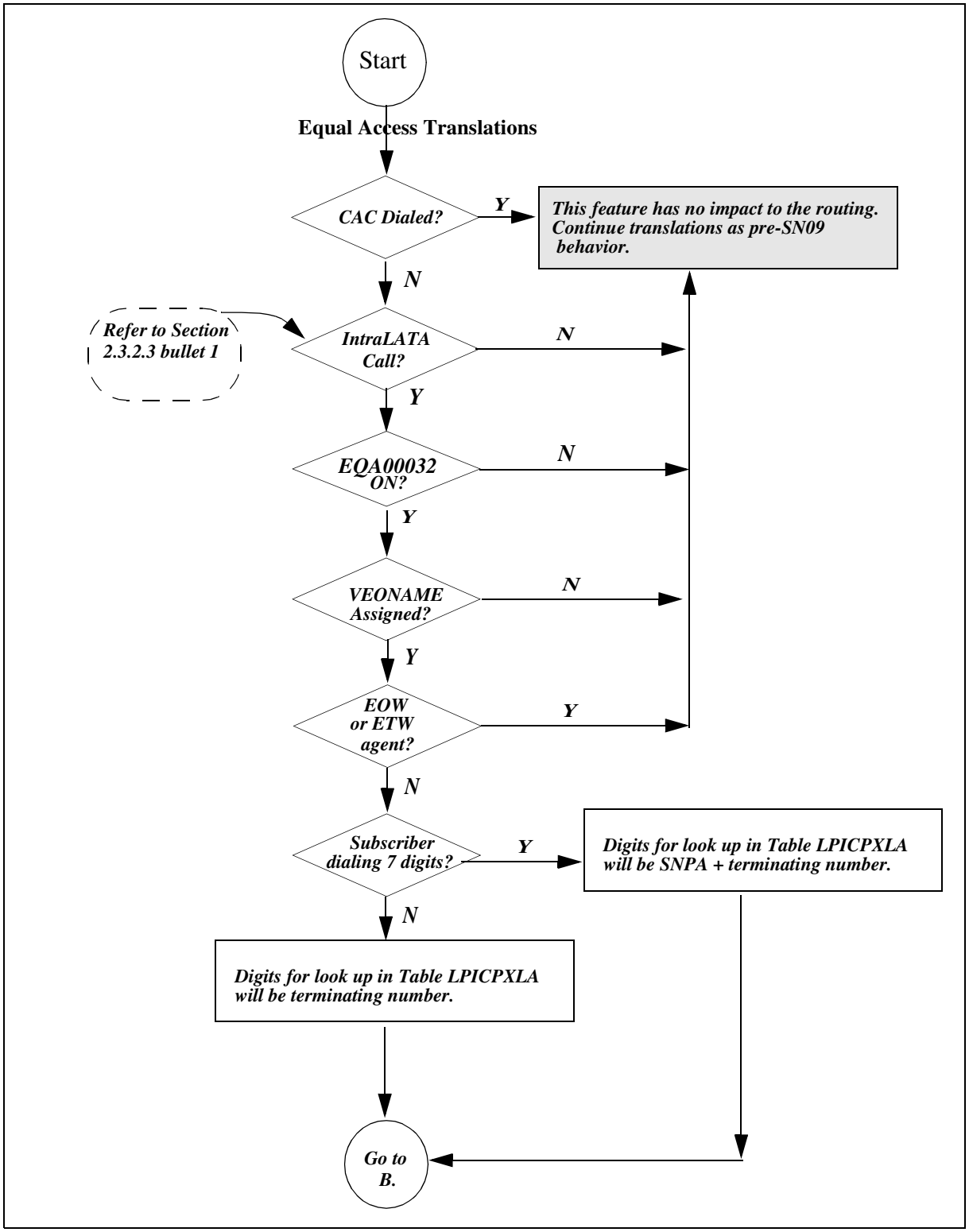
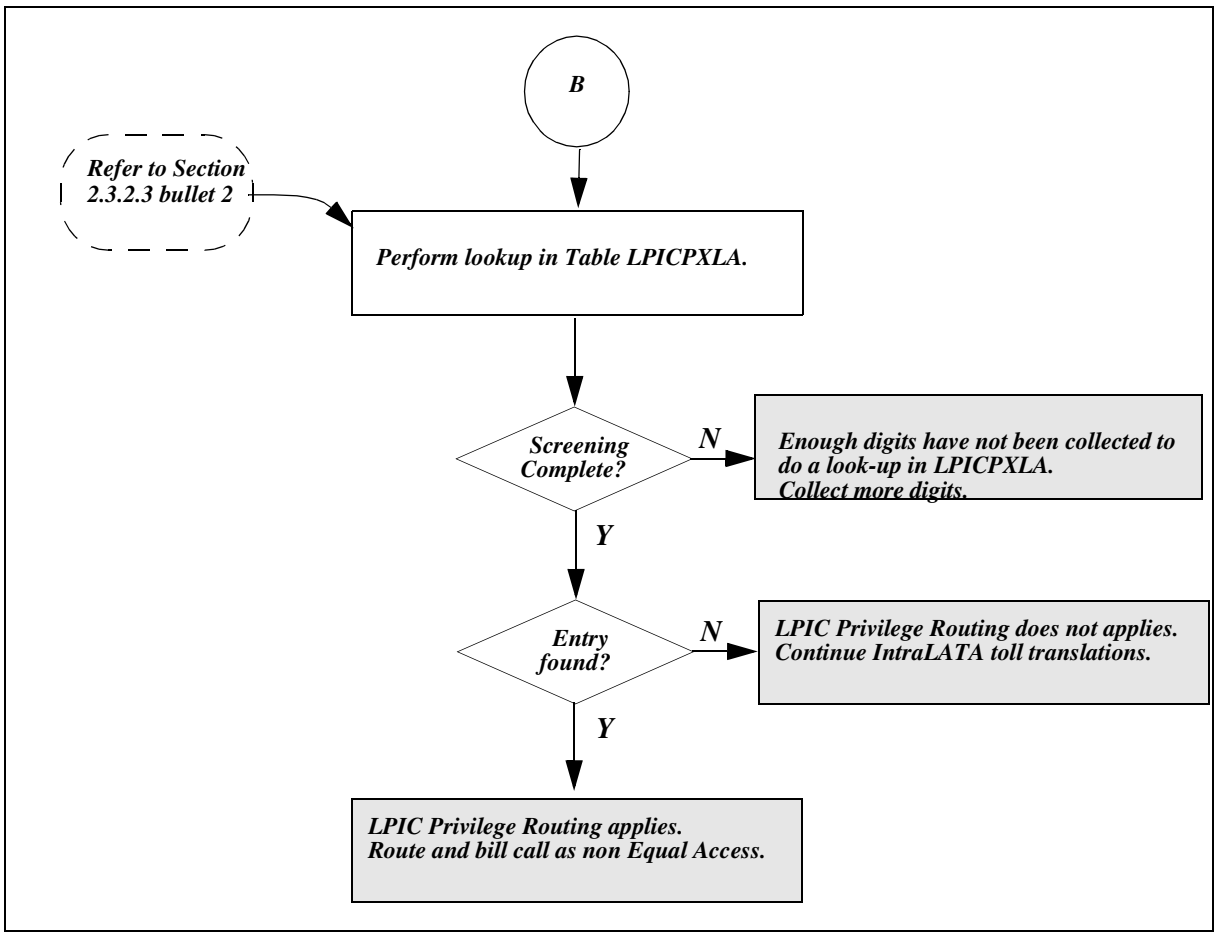


Figure 7 Continued - Equal Access Translations



1.2.2.4 Traver Enhancements

The DMS100/CS2000 EO Traver software is enhanced to support the display of new option VEONAME and to display the contents of new table LPICPXLA. The Traver enhancements are active only when SOC EQA00032 is set to ON and option VEONAME is provisioned for the originator. The following chart describes the Traver impact for the different combinations. Figures 8 through 11 are examples of the modified Traver output.

Table 3 Traver Impact

SOC State	VEONAME Assigned	LPICPXLA entry found?	Traver Impact
IDLE	No	N/A	There will be no new messages in the traver output.

SOC State	VEONAME Assigned	LPICPXLA entry found?	Traver Impact
IDLE	Yes	No	There will be no new messages in the traver output.
IDLE	Yes	Yes	There will be no new messages in the traver output.
ON	No	N/A	There will be no new messages in the traver output.
ON	Yes	No	New Message after displaying Table LATAXLA data: **'TABLE LPICPXLA** **TUPLE NOT FOUND '**
ON	Yes	Yes	New Message after displaying Table LATAXLA data: **'TABLE LPICPXLA** **VEO1 919528** ... **OPERATING TELCO WILL HANDLE THIS CALL'**

Figure 8 EQA00032 is ON & LPICPXLA datafilled

```
traver l 5206000 19195282112 b
TABLE LINEATTR
0 1FR NONE NT 0 0 NILSFC 0 NIL NIL 00 619_POT1_0 LPOT_L123_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
619_POT1_0 NSCR 619 POT1 RTE1 Y RES1 0 0 VEONAME VEO2$ $
TABLE RATEAREA
LPOT_L123_0 LPOT NIL L123 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE LENFEAT
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
AIN Orig Attempt TDP: no subscribed trigger.
TABLE STDPRTCT
POT1 ( 1) ( 1) 7
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1919 199 N DD 1 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
619 Y 919 8 ( 114) ( 1) ( 0) ( 0) 1 $
 . SUBTABLE HNPACODE
 . 919 919 FRTE 919
 . SUBTABLE RTEREF
 .  919 N D ISUPIT4DIG 0 N N
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
619 LPOT ( 29) OPTL N N Y
 . SUBTABLE LCASCRN
 . TUPLE NOT FOUND.  DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL DD N DD UNDT
TABLE LENFEAT
HOST 04 0 00 17 S LPIC LPIC CAR1 Y
TABLE LENFEAT
HOST 04 0 00 17 S PIC PIC CAR2 Y

<continued>
```

Figure 9 EQA00032 is ON & LPICPXLA datafilled

```
<continued>
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
VEO1 919528
TABLE OCCINFO
CAR1 6900 EAP Y Y Y Y Y N N  Y Y Y Y LONG 0 FGRPC Y N Y N N N N N N N N N N Y
TABLE EASAC
TUPLE NOT FOUND
OPERATING TELCO WILL HANDLE THIS CALL
AIN Info Collected TDP: no subscribed trigger.
AIN Info Analyzed TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 ISUPIT4DIG              9195282112                ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 ATB

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 10 EQA00032 is ON & LPICPXLA not datafilled

```
traver l 5206000 19195282112 b
TABLE LINEATTR
0 1FR NONE NT 0 0 NILSFC 0 NIL NIL 00 619_POT1_0 LPOT_L123_0 $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
619_POT1_0 NSCR 619 POT1 RTE1 Y RES1 0 0 VEONAME VEO2$ $
TABLE RATEAREA
LPOT_L123_0 LPOT NIL L123 $
TABLE DNATTRS
TUPLE NOT FOUND
TABLE DNGRPS
TUPLE NOT FOUND
TABLE LENFEAT
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP NIL
AIN Orig Attempt TDP: no subscribed trigger.
TABLE STDPRTCT
POT1 ( 1) ( 1) 7
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1919 199 N DD 1 NA
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
619 Y 919 8 ( 114) ( 1) ( 0) ( 0) 1 $
 . SUBTABLE HNPACODE
 . 919 919 FRTE 919
 . SUBTABLE RTEREF
 .  919 N D ISUPIT4DIG 0 N N
 . EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
619 LPOT ( 29) OPTL N N Y
 . SUBTABLE LCASCRN
 . TUPLE NOT FOUND.  DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL DD N DD UNDT
TABLE LENFEAT
HOST 04 0 00 17 S LPIC LPIC CAR1 Y
TABLE LENFEAT
HOST 04 0 00 17 S PIC PIC CAR2 Y

<continued>
```

Figure 11 EQA00032 is ON & LPICPXLA not datafilled - continued

```
<continued>
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
TUPLE NOT FOUND
TABLE OCCINFO
CAR1 6900 EAP Y Y Y Y Y N N Y Y Y Y LONG 0 FGRPC Y N Y N N N N N N N N N N Y
TABLE EASAC
TUPLE NOT FOUND
OVERLAP CARRIER SELECTION (OCS) APPLIES
TABLE STDPRTCT
POT1 ( 1) ( 1) 7
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1016900 1016900 EA DD 7 P PCAR1 CAR1 Y OFRT 908 8 25 Y
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
 . . TABLE OFRT
 . .  908 CND EA INTNL SK 3
 . .      N D EATANDEMOG 15 D069 N
 . .      N D ISUPIT4DIG 15 D069 N
 . .      CND ALWAYS SK 2
 . .      N D EATANDEMOG 15 D169 N
 . .      N D ISUPIT4DIG 15 D169 N
 . . EXIT TABLE OFRT
 . TABLE STDPRTCT
 . PCAR1 ( 1) ( 0) 6
 . . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
  . . 19 19 EA DD 1 T NA CAR1 N
.TABLE HPCPATTN
TUPLE NOT FOUND
AIN Info Collected TDP: no subscribed trigger.
AIN Info Analyzed TDP: no subscribed trigger.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 EATANDEMOG          D069                  ST
2 ISUPIT4DIG           D069                  ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 ATB

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 12 PX trunks: EQA00032 is ON & LPICPXLA datafilled

EXAMPLE of PX trunk datafilled with LPIC and VEONAME in table CXGRP. Note that table CXGRP does not show up in traver.

Table CXGRP:
CUSTKEY SPB CTD FCTDNTER FCTDNTRA FCTDINT EWATS EWATSI PXOPTION
---
52 N N N N N N N **(LPIC CAR1 Y) (VEONAME VEO1)** $

> traver tr carypx 5414402502 b
TABLE TRKGRP
CARYPX PX 10 ELO NCRT IC NIL MIDL N P621 PBX1 613 613 LCL NONE TSPS L613 N N **52**
NIL 6211234 DIALTN N Y CAR2 Y LATA1 N $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE STDPRTCT
P621 (1) (0) 1
. SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
. 54 60 N NP 0 NA
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
613 Y 915 2 (85) (1) (0) (0) 2 $
. SUBTABLE HNPACODE
. 541 541 FRTE 541
. SUBTABLE RTEREF
. 541 N D 2WEAIT 3 276 N
. EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
613 L613 (56) OPTL N N Y
. SUBTABLE LCASCR
. TUPLE NOT FOUND. DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL NP N DD UNDT
TABLE CLSVSCRC
KEY NOT FOUND
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
VEO1 541
TABLE OCCINFO
CAR1 6524 EAP Y Y Y Y Y N N Y N Y Y LONG 0 FGRPD N N N N Y N N N N Y N Y N N Y

<continued>

Figure 13 PX trunks: EQA00032 is ON & LPICPXLA datafilled - continued

```
<continued>

TABLE EASAC
TUPLE NOT FOUND
OPERATING TELCO WILL HANDLE THIS CALL
TABLE OFCVAR
AIN_OFFICE_TRIGGRP LNPOFFICE
AIN Info Collected TDP: no subscribed trigger.
TABLE TRIGGRP
LNPOFFICE INFOANAL
 . PODP ( DG PODPDIG)$ NIL
Trigger AIN PODP is applicable to office.
 . LNP ( DG LNPDIG) ( ESCEA ) ( ESCOP ) ( ESCDN ) ( ESCCN DD)$ NIL
Trigger AIN LNP is applicable to office.
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 2WEAIT

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 T120

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

Figure 14 PX trunks: EQA00032 is ON & LPICPXLA not datafilled

EXAMPLE of PX trunk datafilled with LPIC and VEONAME in table CXGRP. Note that table CXGRP does not show up in traver.

Table CXGRP:
CUSTKEY SPB CTD FCTDNTER FCTDNTRA FCTDINT EWATS EWATSI PXOPTION
---
52 N N N N N N N **(LPIC CAR1 Y) (VEONAME VEO1)** $

> traver tr carypx 5414402502 b
TABLE TRKGRP
CARYPX PX 10 ELO NCRT IC NIL MIDL N P621 PBX1 613 613 LCL NONE TSPS L613 N N **52**
NIL 6211234 DIALTN N Y CAR2 Y LATA1 N $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE STDPRTCT
P621 (1) (0) 1
. SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING. CALL TYPE DEFAULT IS NP. PLEASE REFER TO
DOCUMENTATION.
. 54 60 N NP 0 NA
. SUBTABLE AMAPRT
. KEY NOT FOUND
. DEFAULT VALUE IS: NONE OVRNONE N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE HNPACONT
613 Y 915 2 (85) (1) (0) (0) 2 $
. SUBTABLE HNPACODE
. 541 541 FRTE 541
. SUBTABLE RTEREF
. 541 N D 2WEAIT 3 276 N
. EXIT TABLE RTEREF
EXIT TABLE HNPACONT
LNP Info: Called DN is not resident.
LNP Info: HNPA results are used.
TABLE LCASCRCN
613 L613 (56) OPTL N N Y
. SUBTABLE LCASCR
. TUPLE NOT FOUND. DEFAULT IS NON-LOCAL
TABLE PFXTREAT
OPTL NP N DD UNDT
TABLE CLSVSCRC
KEY NOT FOUND
TABLE LATAXLA
TUPLE NOT FOUND
ASSUMED TO BE DEFAULT INTRALATA, INTRASTATE, STD
TABLE LPICPXLA
TUPLE NOT FOUND
TABLE OCCINFO
CAR1 6524 EAP Y Y Y Y Y N N Y N Y Y LONG 0 FGRPD N N N N Y N N N N Y N Y N N Y

<continued>

Figure 15 PX trunks: EQA00032 is ON & LPICPXLA not datafilled - continued

```
<continued>

TABLE EASAC
TUPLE NOT FOUND
 TABLE STDPRTCT
P621 ( 1) ( 0) 1
 . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 . 1016524 1016524 EA DD 7 P P524 CAR1 Y OFRT 889 3 20 Y
 . SUBTABLE AMAPRT
 . KEY NOT FOUND
 . DEFAULT VALUE IS:   NONE OVRNONE  N
 .  . TABLE OFRT
 .  .  889 CND EA INTNL SK 3
 .  .      S D OGEACAR1
 .  .      S D ISUP2WCAR1
 .  .      CND ALWAYS SK 2
 .  .      N D OGEACAR1 15 D121 N
 .  .      N D ISUP2WCAR1 0 D121 N
 .  . EXIT TABLE OFRT
 . TABLE STDPRTCT
 . P524 ( 1) ( 0) 4
 .  . SUBTABLE STDPRT
WARNING: CHANGES IN TABLE STDPRT MAY ALTER OFFICE
BILLING.  CALL TYPE DEFAULT IS NP.  PLEASE REFER TO
DOCUMENTATION.
 .  . 5 9 EA DD 0 T NA C524 N
TABLE HPCPATTN
TUPLE NOT FOUND
TABLE OFCVAR
AIN_OFFICE_TRIGGRP LNPOFFICE
AIN Info Collected TDP: no subscribed trigger.
TABLE TRIGGRP
LNPOFFICE INFOANAL
 . PODP ( DG PODPDIG)$ NIL
Trigger AIN PODP is applicable to office.
 . LNP ( DG LNPDIG) ( ESCEA ) ( ESCOP ) ( ESCDN ) ( ESCCN DD)$ NIL
Trigger AIN LNP is applicable to office.
AIN Info Analyzed TDP: trigger criteria not met.

+++ TRAVER: SUCCESSFUL CALL TRACE +++


DIGIT TRANSLATION ROUTES

1 OGEACAR1            5414402502              ST
2 ISUP2WCAR1          5414402502              ST

TREATMENT ROUTES.  TREATMENT IS: GNCT
1 T120

+++ TRAVER: SUCCESSFUL CALL TRACE +++
```

1.2.2.5 Service Interactions with LPIC Privilege Routing

1.2.2.5.1 Interactions with Existing EA Translation Capabilities

The interactions between existing EA LPIC translation capabilities and the LPIC Privilege Routing are addressed below.

0+ Local Routing:

SOC EQA00015[2], "IntraLATA PIC Enhancements Phase 1," provides the flexibility to route 0+ local calls to the LEC, the subscriber's LPIC, or a designated carrier. Office parameter ZERO_PLUS_LOCAL_CARRIER in combination with SOC EQA00015 controls the switch behavior. If the 0+ local capability determines the call will route to the carrier provisioned for parameter ZERO_PLUS_LOCAL_CARRIER or to the LPIC, the call is handled as an LPIC toll call.

The LPIC Privilege Routing capability introduced by this activity adheres to the same behavior, and performs screening for the called NPANXX in table LPICPXLA when SOC EQA00032 is ON and the originator has the VEONAME option assigned. If the LPIC Privilege Routing applies, the call will route to the LEC as a non-EA call.

If SOC EQA00015 is OFF, the call will route to the LEC as a non-EA call (this behavior is unchanged by the functionality of this activity).

If NILC or USE_PREVIOUS is provisioned for parameter ZERO_PLUS_LCL_CARRIER, the call will route to the LEC as a non-EA call (this behavior is unchanged by this activity).

1+ Coin IntraLATA Routing Flexibility:

SOC EQA00015, "IntraLATA PIC Enhancements Phase 1," in combination with field INTRCOIN in table OCCINFO provides the ability to route 1+intraLATA toll *coin* originations to either the LEC, the subscriber's LPIC, or a designated carrier. If the coin 1+intraLATA toll capability determines the call will route to the carrier provisioned for INTRCOIN or to the LPIC, the call is handled as an LPIC toll call.

The LPIC Privilege Routing capability introduced by this activity adheres to this behavior and performs screening for the called NPANXX in table LPICPXLA when SOC EQA00032 is ON and the originator has the VEONAME option assigned. If LPIC Privilege Routing applies, the call will route to the LEC as a non-EA call.

If 'Y NILC' is provisioned for field INTRCOIN, the call will route to the LEC as a non-EA call (this behavior is unchanged by this activity).

If SOC EQA00015 is OFF, the call is handled as an LPIC toll call. The LPIC Privilege Routing capability introduced by this activity adheres to

[2] Introduced by feature AN1811.

this behavior and performs screening for the called NPANXX in table LPICPXLA when SOC EQA00032 is ON and the originator has the VEONAME option assigned. If the LPIC Privilege Routing applies, the call will route to the LEC as a non-EA call.

LATAXLA LPIC Privilege:

SOC EQA00024[3], "Override LPIC Privilege," provides the ability to mark intraLATA codes as privilege on a per LATA basis via table LATAXLA. When EQA00024 is ON, LPIC calls are handled by the LEC for those codes that are provisioned as privilege in table LATAXLA.

The LPIC Privilege Routing capability introduced by this activity provides the same capability as EQA00024, but on a per VEO basis. EQA00032 and EQA00024 are independent of each other. The LPIC Privilege Routing capability takes precedence when SOC EQA00032 is ON and VEONAME is provisioned on the originating agent. If the originator does not have VEONAME provisioned or SOC EQA00032 is IDLE, the new LPIC Privilege Routing capability does not apply. In this case SOC EQA00024 continues to be used to provide intraLATA privilege routing.

Table LATAXLA NON_EA Datafill:

Table LATAXLA allows NPA/NPANXX codes to be provisioned as a NON_EA calltype. If NON_EA calltypes, the call routes as a non-EA call. Casual access dialing to NON_EA codes is not permitted. This behavior takes precedence over the LPIC Privilege Routing feature. If the dialed number (NPA or NPANXX) is provisioned as NON_EA in table LATAXLA, the call will be routed as a non-EA call. In this case, table LPICPXLA is not referenced.

Alternate Service Provider:

An alternate service provider can be specified for any of the following services:

In-Session Activation (ISA): AQ1700

Special Delivery Service (SDS): AQ1335

Universal Voice Messaging (UVM): AQ1303

Virtual Call Framework (VCF): AJ4936

Who's Calling (WC): A59012655

These services specifically request an alternate carrier be used to complete the call.

With pre-SN09 behavior, privilege routing takes precedence over the alternate carrier. If table LATAXLA is provisioned as privilege, the call is

[3] Introduced by feature AN1811.

handled by the LEC regardless of whether an alternate carrier is provided by the service. This applies to both “Override LPIC Privilege” (SOC EQA00024), and interLATA privilege in table LATAXLA.

The LPIC Privilege Routing capability introduced by this feature is consistent with this behavior and takes precedence over alternate carrier. Screening will be performed for intraLATA toll NPANXX codes in table LPICPXLA when SOC EQA00032 is ON and the originator has the VEONAME option assigned. If LPIC privilege routing applies, the call will route to the LEC as a non-EA call.

1.2.2.5.2 Advanced Intelligent Networks (AIN)

This feature also interacts with AIN response translations. When AIN database response returns an intraLATA routing number, SOC EQA00032 is active, and VEONAME is associated, the new Table LPICPXLA is accessed to determine if LPIC privilege applies.

The routing number is always used as part of the index into LPICPXLA. The other part of the index is the VEONAME, which is retrieved as discussed below:

- When AIN response translation routes through a VFG the existing behavior is to retrieve the LATA name associated with the subscriber, and not the VFG. The LPIC feature is consistent with this behavior. The VEONAME is retrieved from the subscriber for intraLATA calls when the LPIC SOC EQA00032 is active. In these cases the LPICPXLA will be indexed using the subscriber’s VEONAME and the routing number returned in the AIN DB response.
- Using AIN it is possible to alter the translation through table XLAMAP and table PXLAMAP. Either the pretranslator name or the LINEATTR index can be altered. In this case deriving the VEONAME is dependent on whether the AIN translation specifies a new pretranslator name or a new LINEATTR index:
  - — If the AIN translation specifies a new pretranslator name, the VEONAME is derived from the subscriber.
  - — If the AIN translation specifies a new LINEATTR index, the VEONAME is derived based on the XLAPLAN associated to the new LINEATTR.
- The use of the LARP capability provides a method to override various translation attributes for the AIN response translation via option LARP in Table TRIGITM. These translation attributes include LINEATTR, XLAPLAN, and RATEAREA indices. LARP TRAVER option[4] and call processing derives the LATANAME associated with the LARP datafill in Table TRIGITM. This feature will adhere to this behavior and derive the

[4] Introduced by feature A59022554.

VEONAME associated with the XLAPLAN index provisioned in table TRIGITM.

- All other cases derive the VEONAME from the originating agent.

1.2.2.5.3 Local Number Portability (LNP)

LNP calls perform translations twice. The first one is referred to as the pre-query translation which occurs prior to the sending the query to the LNP database. The second one is referred to as the post-query translation which occurs after the receipt of the LNP database response.

If SOC NPE00005[5], "1000 Blk Nbr Pooling," is ON, the LPIC Privilege Routing capability introduced by this activity will use the LATAXLA results from the pre-query translation. Specifically, if the pre-query LATAXLA result determines the call is intraLATA, the LPIC privilege capability performs a lookup in table LPICPXLA if LPIC SOC EQA00032 is ON and the VEONAME is assigned to the originator. The ported DN is used for the look-up in table LPICPXLA.

IF NPE00005 is IDLE, the LPIC Privilege Routing capability uses the LATAXLA results from the post-query translation. Specifically, if the post-query LATAXLA result determines the call is intraLATA, the LPIC Privilege Routing capability performs a lookup in table LPICPXLA if the LPIC Privilege Routing SOC is ON and the VEONAME is assigned to the originator. The ported DN is used for the look-up in table LPICPXLA.

The LNP TRAVER option LNPAR provides the ability to simulate an SCP response containing an FLRN, HLRN, or ported DN. The LPIC Privilege Routing capability introduced by this activity requires the use of option LNPAR to correctly display the contents of table LPICPXLA. VEONAME is derived the same for TRAVER as with call processing but the NPANXX used to access LPICPXLA is derived differently. Specifically, the LNPAR option contains the ported DN which is used as the other part of the key to Table LPICPXLA. Thus, TRAVER is consistent with call processing.

The syntax for the LNPAR option is as follows:

TRAVER L 6215000 N CDN NA <routing #> AINRES R01 LNPAR <ported DN> B

Where an LRN or the ported DN can be entered as the <routing #> and a 10 digit DN or 'N' can be entered for <ported DN>.

[5] Introduced by activity A59012192.

1.2.2.5.4 In-Session Activation (ISA)

In-Session Activation (ISA)[6] is an originating line service that is activated when the originator places a call and the called party is either busy or a ringing timeout occurs. When either of these two conditions occur, the switch software performs *called party screening* to determine whether to offer the ISA service. The *called party screening* function looks at various call characteristics to determine whether to activate ISA. With pre-SN09 behavior, if the call is provisioned as privilege in table LATAXLA, the ISA service is offered. This applies to both intraLATA and interLATA privilege in table LATAXLA. The LPIC Privilege Routing capability will be consistent with this behavior and ISA service will be offered for intraLATA calls if SOC EQA00032 is ON, the originator has the VEONAME option assigned, and the NPANXX code is provisioned in table LPICPXLA. If the service redirects the call to a new number, LPIC Privilege Routing capability may apply.

1.2.2.5.5 Special Delivery Service (SDS)

Special Delivery Service (SDS)[7] is a feature that provides the originating line with the option to invoke message delivery when the called party is busy or does not answer within an office-defined interval. When either of these two conditions occur, the originating line is connected to a Voice Messaging System (VMS) either directly via an SMDI link or indirectly via an outgoing ISUP trunk.

Prior to terminating to VMS, the SDS features performs *call characteristics screening* to determine whether to offer the SDS service. The *call characteristics screening* function looks at various call characteristics to determine whether to activate SDS. With pre-SN09 behavior, if the call is provisioned as intraLATA privilege in table LATAXLA, the SDS service is offered. The LPIC Privilege Routing capability will be consistent with this behavior. The SDS service will be offered for intraLATA calls if the LPIC SOC EQA00032 is ON, the originator has the VEONAME option assigned and the NPANXX code is provisioned in table LPICPXLA. If the service redirects the call to a new number, LPIC Privilege Routing capability may apply.

1.2.2.5.6 Call Forwarding (CFW) Interactions

Call ForWarding (CFW) allows a subscriber to redirect a call to a new number. The LPIC feature interacts with CFW since it is possible to redirect a call to an IntraLATA number. For intraLATA calls LPIC privilege routing applies if the LPIC SOC EQA00032 is ON, the redirecting agent has the VEONAME option assigned, and the NPANXX code of the forwarding number is provisioned in table LPICPXLA.

---

[6] Introduced by activity AQ1700.

[7] Introduced by activity AQ1335.

1.2.2.5.7 IntraLATA Full Carrier Toll Denied (FCTDNTRA)

Subscribers may have option FCTDNTRA assigned to their phone. This option functionality is controlled by SOC EQA00015[8]. Subscribers assigned this option are either prohibited from making toll calls using any carrier, or are allowed to have access to a limited number of carriers. Since calls being handled by LPIC Privilege Routing feature will be terminated by the LEC, the FCTDNTRA functionality does not block the call.

1.2.2.5.8 Toll DeNied (TDN)

Subscribers may have the option Toll DeNied (TDN) assigned to their phone. This option restricts an originator from making toll calls. Since the privilege codes for LPIC Privilege Routing are treated as toll codes, originating agents with TDN shall be blocked from accessing privilege codes.

1.3 Hardware Requirements or Dependencies

Not applicable

1.4 Software Requirements or Dependencies

Not applicable

1.5 Limitations and restrictions

The following limitations and restrictions apply to Virtual End Office (VEO) partitioning capability:

- VEO capability is not supported by DMS200. It is only supported by DMS100/CS2000.
- VEO is only for public translations capabilities.
- VEONAME option can not be assigned in Table XLAPLAN or Table CXGRP with VEO name of NILV (NIL VEO name).
- Maximum 999 VEOs are supported.

The following limitations and restrictions apply to the LPIC Privilege Routing functionality:

- EOW (Enhanced Outwats) and ETW (Enhanced Two-Way WATS) originating agents are not supported.
- MDC EWATS which was introduced by feature AF1664 and AF7559 is not supported.
- CALEA is not supported.
- Up to six-digit (NPANXX) codes are allowed to be provisioned as privilege codes in table LPICPXLA.

[8] Introduced by activity AN1811.

- The maximum size of table LPICPXLA will be determined by the digits pattern used in the table LPICPXLA, and the total number of VEO names provisioned in table VEONAME.
- P2 trunks are not supported.
- AIN local trunk capability[9] allows a call to reroute to a carrier when incoming on local trunks (i.e. TI, T2, IT, ATC). AIN local trunk capability is not supported by this feature.
- Packet (X.25, X.75) translations are not supported.
- This feature is not supported on non-conforming end offices.

1.6 Interactions

Refer to Section 1.2.2.5 "Service Interactions with LPIC Privilege Routing" on page 1139.

1.7 Glossary

Term	Description
AIN	Advanced Intelligent Network
CAC	Carrier Access Code
CALEA	Communications Assistance for Law Enforcement Act
CFW	Call Forwarding
EA	Equal Access
EO	End Office
EOW	Enhanced OutWats
ETW	Enhanced Two-Way WATS
FLRN	Foreign Location Routing Number
HLRN	Home Location Routing Number
ISA	In-Session Activation
LARP	Line Attribute Response Processing
LATA	Local Access and Transport Area
LCC	Line Class Code
LEC	Local Exchange Carrier
LNP	Local Number Portability

[9] Introduced by feature AJ3999.

Term	Description
LNPAR	LNP Analyze Route
LPIC	intraLata Primary Interexchange Carrier
MDC	Meridian Digital Centrex
NPA	Numbering Plan Area
SCP	Service Control Point
SDS	Special Delivery Service
SNPA	Serving Numbering Plan Area
SOC	Software Optionality Control
TDN	Toll Denied
UVM	Universal Voice Messaging
VCF	Virtual Call Framework
VEO	Virtual End Office
WC	Who's Calling

1.8 References

1. Feature AN1811, IntraLATA PIC Enhancements, Phase 1

2. Feature AJ3999, AIN 0.1 FGC-FGD Interworking

3. Feature AQ1700, IN-SESSION ACTIVATION

4. Feature AQ1335, Special Delivery Services (SDS)

5. Feature A59022554, AIN: Line Attributes for PFC/TRAVER Support

6. Feature AQ1303, Universal Voice Messaging

7. Feature AJ4936, Virtual Call Framework

8. Feature A59012655, Who's Calling

Product = CS 2000

A00009120 -- Multi-Time Zone Enhancements

1: Applicable solution(s)

UA-IP

1.1 Description

In order to support networks that span Multiple Time Zones (MTZ) features in the Succession/CS2K products must be enhanced. Feature A59038784 introduced a framework to support MTZ and DST (Daylight Savings Times) for subscriber visible services. This feature extends this functionality to the following:

1. Time of Day (TOD) Routing
2. Selected Malicious Call Trace (MCT/MCH) Logs LINE 125 & 126, MCT 103 &105

Currently with the TDM-based MMP/DMS products, a callserver is allocated within each time zone. However, with the introduction of Succession/CS2K products, the callserver and the line gateways aren't bound by this limitation and can be located in different time zones. This means that line features/logs/billing that use or display the local time must be able to modify the callserver time based on the time zone they are located in.

Activity A59038784 introduced a framework for multiple time zones and DST (Daylight Savings Time) for subscriber visible services, supporting IBN and RES lines. The activity introduced a line option, MTZ, which when assigned to a subscriber line provides an index into table MULTITM. Table MULTITM contains information as to the time difference based on the time zone and DST data.

Activity A00005734, Multiple time zone option for KSET lines expanded the functionality to KSET lines with the M5216 Line Class Code. This allows for the support of CICM lines together with those on the MG9K.

Line features/logs are all currently based on the switch/callserver time, this feature uses the framework to obtain offsets from the switch time and hence the ability to calculate local time for Time of Day (TOD) Routing and select Malicious Call Trace logs. A separate activity will extend this functionality to billing.

There is no Software Optionality Control (SOC) for this activity.

The MTZ framework provides support for core based IBN, RES and M5216 KSET lines, this activity has the same limitation. However, it is assumed that this confers support for succession access lines CICM, MG9K, IADs, MTA and MG9K ABI together with SIP lines.

This activity is broken down into the following design components:

1.1.1 TOD Routing:

The desired behavior of the TOD Routing support with MTZ will be able to do TOD routing when MTZ exists. This will allow a call to route based on the Time of Day even if multiple time zones and DST are present. When TOD routing occurs, a time is scheduled when to route the call. This feature will check if MTZ exists, convert the time given by the user on the individual line from the timezone they are in, into the CM clock time. The call will then be scheduled to route based on that converted time. If MTZ does not exist, the TOD routing behavior before this feature will occur.

The TOD system is based on datafill of five tables, DAYTYPES, TODHEAD, DAYOWEEK, DAYOYEAR and TIMEODAY.

Table Name	Function
DAYTYPES	Defines the DAYTYPES (such as weekday, weekend, midweek etc) to be used by the other tables
TODHEAD	Defines the name (TODNAME) and the DAYTYPE for the TOD system entry.
DAYOWEEK	This table is used to map the day of the week into a DAYTYPE.
DAYOYEAR	This table is used to map the specified day of year into the DAYTYPE. This overrides the entry in DAYOWEEK based on the TODNAME.
TIMEODAY	The first four tables exist only to allow you to get to the TIMEODAY table. This table defines the actual result for the time, DAYTYPE and TODNAME.

To achieve TOD Routing, datafill of TOD routing must be done in one of the routing tables IBNRT(X), OFR(X), RTEREF of HNPACONT or FNPACONT

TOD Route Datafill in routing tables IBNRTE, OFRT,RTEREF

Table Fields	Definition	Datafill
RTE	Route Ref Index	{0-1023}
IBNRTESEL/ RTESEL	Route Selector	CND (Conditional Route)
CNDSEL	Conditional Selector	TOD (Time of Day)

TOD Route Datafill in routing tables IBNRTE, OFRT,RTEREF

Table Fields	Definition	Datafill
TODNAME	TOD Name Datafilled in the TODHEAD table	TOD Name
TIMES	ibn_time_range (results of TOD system will be resolved into this type)	{0 -15}
RTETYPE	CND_RTE_TYPE	{ST,T,SK}
{RTEREF, TABNAME -index, , SKIPNUM}	Route Ref Index Routing Table Name Number of Routes to skip	{0-1023} {Routing tables} {0-7}
INDEX	Route ref index	{0-1023}

Example of TOD route datafill:

Table IBNRTE/OFRT

RTE: 1005

IBNRTESEL: CND

CNDSEL: TOD

TODNAME: CGATOD
TIMES: 1

RTETYPE: T

TABNAME: OFRT

INDEX: 100

```
>list
 RTE                                          RTELIST

                                             OPTIONS

-------------------------------------------------------------------------

1005          ( CND      TOD   CGATOD          2  T     OFRT  100)$$
```

1.1.2 MCT Logs

There are a number of MCT logs supported by the CS2K both in the North American and International market, however, not all of these logs need to be modified for multiple time zones. The following logs have been identified by the customer as requiring support for MTZ:

LINE125
LINE126
MCT103
MCT105

For each of these logs a new field, LOCAL TIME, will be added, this field will display the local time for that subscriber line based on the switch time modified by the value in table MUTITM if assigned to that line. This feature doesn't impact when or where these logs are output.

The log report format for LINE125 is as follows:

LINE125 mmmdd hh:mm:ss ssdd INFO TRACE_ON_MALICIOUS_CALL_INI...

len DN dn INCOMING TRUNK = CKT trkid

CALLID = callid

CALLING NUMBER = dn

SOURCE = source

LOCAL TIME = <Time>

An example of log report LINE125 follows:

LINE125 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_INITIATED

HOST 00 0 19 20 DN 2557811999

INCOMING TRUNK = CKT ICCAMA 15

CALLID = 123456

CALLING NUMBER = 2149975015

SOURCE = CALLING NUMBER

LOCAL TIME = 10:00:00

The format for log report LINE126 is as follows:

LINE126 mmmdd hh:mm:ss ssdd INFO TRACE_ON_MALICIOUS_CALL_ INITIATED

len DN dn

CALLING LINE = LEN len DN dn onitxt

CALLID = callid

LOCAL TIME = <Time>

An example of log report LINE126 follows.

LINE126 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_INITIATED

HOST 00 0 19 20 DN 2557811999

CALLING LINE = LEN HOST 05 1 15 16 DN 7812001

CALLID = 123456

LOCAL TIME = 10:00:00

The log report format for MCT 103 is as follows:

MCT103 mmmdd hh:mm:ss ssdd INFO TRACE_ONMALICIOUS_CALL_ACTIVATED

CALLING_PARTY : <cli> <originating agent>

CALLED_PARTY : <full number><terminating agent>

CALLING_PARTY_CATEGORY : <cpc>

LOCAL TIME = <Time>

An example of log report MCT 103 follows:

MCT103 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_ACTIVATED

CALLING_PARTY : CKT ICATUPTRUNK 1

CALLED_PARTY : 2762345 LEN HOST 00 0 01 10

CALING_PARTY_CATEGORY : 16

LOCAL TIME = 10:00:00

The log report format for MCT 105 is as follows:

MCT105 mmmdd hh:mm:ss ssdd INFO TRACE_ONMALICIOUS_CALL_ACTIVATED

CALLING_PARTY : <full number> CKT <originating agent>

CALLED_PARTY : <full number> CKT <terminating agent>

LOCAL TIME = <Time>

An example of log report MCT 105 follows:

MCT105 APR01 12:00:00 2112 INFO TRACE_ON_MALICIOUS_CALL_ACTIVATED

CALLING_PARTY : 9717718745 CKT ICATUPTRUNK 1

CALLED_PARTY : 2762345 CKT ICATUPTRUNK 12

LOCAL TIME = 10:00:00

1.2 Hardware Requirements or Dependencies

N/A

1.3 Software Requirements or Dependencies

SN09

1.4 Limitations and restrictions

The limitations and restrictions specified in activity A59038784 are also applicable to this activity.

In addition the following limitations and restrictions apply:

- Multitime Zone enhancements will not be supported if the MTZ option is not on the subscriber's line.
- The feature is only supported on IBN/RES and M5216 KSET sets.
- MTZ is only supported by the LINE125, LINE126, MCT103 and MCT105 logs.
- The new field 'LOCAL TIME' will be present in all LINE125, LINE126, MCT103 and MCT105 logs irrespective of whether the subscriber is in a different time zone than the callserver. In these cases the local time will be the same as the switch time.

1.5 Interactions

This feature interacts with the existing features Multi-Time Zone, A59038784 and A00005734, Multiple time zone option for KSET lines.

1.6 Glossary

Term	Description
CICM	Centrex IP Client Manager
CLF	Call LIne Identification with Flash
CLI	Calling Line Identity

Term	Description
CM	Computing Module
CPC	Calling Party Category
CNDSEL	Conditional Selector
DMS	Digital Multiplex Switch
DST	Daylight Savings Time
IAD	Integrated Access Device
IBNRTESEL	IBN Route Selector
MCH	Malicious Call Hold
MCT	Malicious Call Trace
MTA	MultiMedia Terminal Adaptor
MTZ	Multi-Time Zone Enhancement
RTESEL	Route Selector
SIP	Session Initiation Protocol
TOD	Time Of Day

Product = CS 2000

A00009129-- Controlled Hot SWACT

Functional Description

1: Applicable Solution(s)

PT-IP, Int'l PT-IP

1.1 Description

This feature introduces a controlled hot SWACT capability for the CS 2000 - Compact Call Agent to the same load on the inactive side. A controlled swact is defined as being initiated from the linux CCAMTC map level or system initiated following a REX test.

Prior to this feature, a controlled Swact of the CS 2000 - Compact Call Agent utilizes a warm restart with an associated denial of origination period of approximately 25 seconds. Existing calls are preserved.

This new controlled hot Swact capability significantly reduces the denial of origination period to less than 3 seconds. Existing calls are preserved.

With the significantly reduced denial of origination period, this feature will now initiate a SWACT following a full REX test.

This feature will also provide the ability to set the day of the full REX test. Prior to this feature, the day of the full REX test was hardcoded to Thursday. The time of the REX test is still set via the NODEREXCONTROL tuple in table OFCVAR.

1.2 Hardware Requirements or Dependencies

N/A

1.3 Software Requirements or Dependencies

The minimum software baseline for this feature is a cPCI SOS image based on CSP22 as well a linux ramdisk based on NCGL8.

1.4 Limitations and restrictions

1. The controlled hot swact introduced in this feature is only initiated in two scenarios. From the CCAMTC map and after a REX test. It does NOT include the following.

- SWACT due to hardware/software failure.
- SWACT due to locking of active card on the SAM21EM.
- SWACT initiated by using the SWACT FORCE option in CCAMTC.

2. The CCAMTC map will not display whether the switch is in warm sync or hot sync. This will only be displayed from the CAPCI tool within SOS.

1.5 Interactions

A new SOS CI called CMREXFUL will be created to allow setting the day the full REX will occur.

The SOS CAPCI output will be modified to reflect warm or hot sync state.

The warning message when the swact command is initiated from the linux CCAMTC map level will be modified.

1.6 Glossary

Term	Description
REX	Routine Exercise
SAM21EM	SAM21 Element Manager

Term	Description
SWACT	Switch Activity

Product = CS 2000

A00009153-- H.323 RLT Development

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

Release Link Trunk (RLT) is used to free unused call signaling paths that result from call path changes such as call forwarding and call transfers. RLT is a proprietary function to Nortel that was originally developed for PRI trunks. Therefore, the RLT functionality will only be used by Nortel H323 gateways such as CS 1000 (CS1K).

Since this feature does not address any new functionality for the CS2000 or CS2100, for the remainder of this document, the term CS2K will imply functionality for both CS2000 and CS2100.

Note: A 3rd party H323 Gateway does not use the RLT functionality.

1.1.1 RLT Capability

The RLT functionality and provisioning for CS1K are described outside the scope of this document in "*CS 1000 RLT FS*". The following steps are needed to configure the "*RLT on NI-1 PRI"* capability in the CS2K.

SOC option can be set and verified as shown in the steps below:

```
>soc; soc debug; select option NI000024; (RLT on NI-1 PRI)

>assign rtu <Pass Code> to NI000024
>assign state on to NI000024
OPTION    NAME                                RTU   STATE
     USAGE  LIMIT   UNITS  LAST_CHG
NI000024  RLT on NI-1 PRI        Y     ON       -
     -        -             04/11/17
```

1.1.2 RLT Trunk Provisioning

Each trunk group may be provisioned for RLT capability using the existing MRLT option in the TRKGRP table that was developed for NTNA PRI.

Add the MRLT option to the TRKGRP table.

```
>table trkgrp; format pack ; pos <h323-clli> ; change
     (option set to MRLT)
<h323-clli> PRA 0 NPDGP NCRT ASEQ N (ISDN 100) $ (MRLT ) $
```

1.1.3 RLT of NTNA PRI trunks

The following section was taken from *NTNA PRI Specification* (NIS A211-1). The H323 RLT functionality is identical to the RLT functionality described in the NTNA PRI specification.

RLT is a feature available on an optional basis which optimizes the usage of NTNA PRI trunks. The following is a typical usage for RLT. Please note that many other scenarios are possible. In this scenario, User A calls User B. This call is referred to as Call 1. Call 1 is routed through the DMS-100 to the PBX. User B then forwards or transfers the call to User C, requesting RLT.

This call (Call 2) is routed through the same DMS-100 as shown in the following figure.

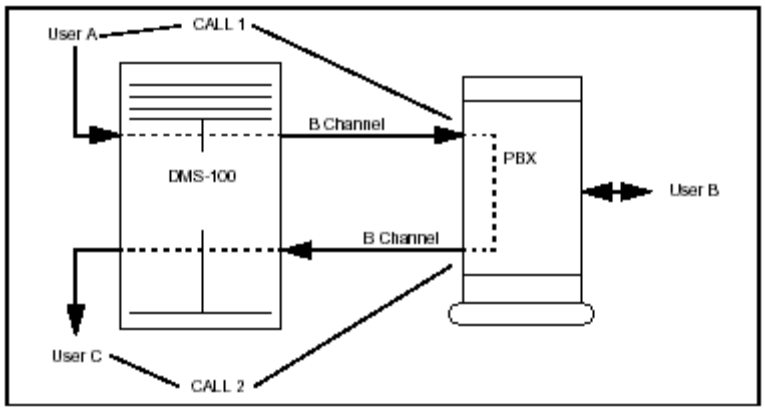


Figure 1: Typical Usage of RLT

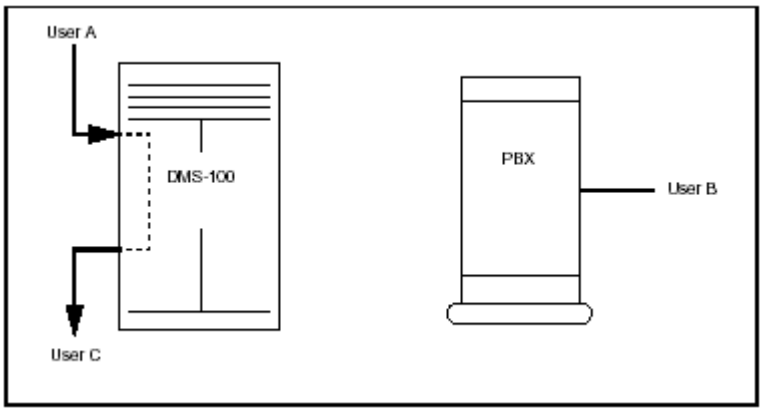


Figure 2: Result of Invoking RLT

When the call to User C is connected, RLT is invoked. The call is bridged between User A and User C at the DMS-100 and the PRI trunks to the PBX are released as shown in Figure 2: Result of Invoking RLT. Any CPE device may be used with this feature if it follows the same user side RLT protocol as described in "NTNA PRI Specification Chapter 5-12: Release Link Trunk (RLT)".

An example of the Q.931 message flow for RLT is shown in the following figure.

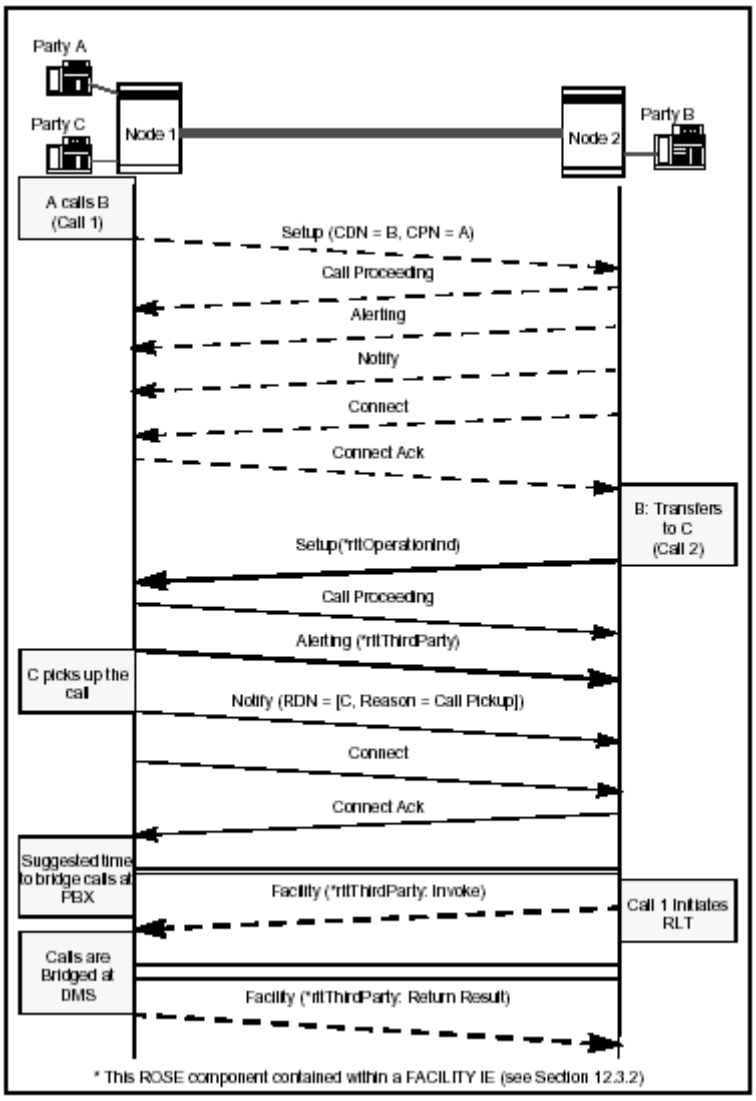


Figure 3: RLT with Call Transfer

1.1.4 Functional Behavior

Assuming RLT functionality has been provisioned in the CS2K and applied to all the H323 NTNA PRI trunk groups, there are two major behavior scenarios.

- "User Side" RLT capability
- "Network Side" RLT capability

1.1.4.1 User Side RLT

The first scenario is shown in the following figure. In this figure, CS1K A is calling CS1K B, and CS1K B call forwards to CS1K C. The invocation of RLT by CS1K B allows the CS2K to bridge the calls, making a new call from CS1K A through the CS2K to CS1K C. This invocation frees up the signaling path

between CS1K B and the CS2K. Note that all signaling paths are through the CS2K, since it is the H323 Gate Keeper in this network.

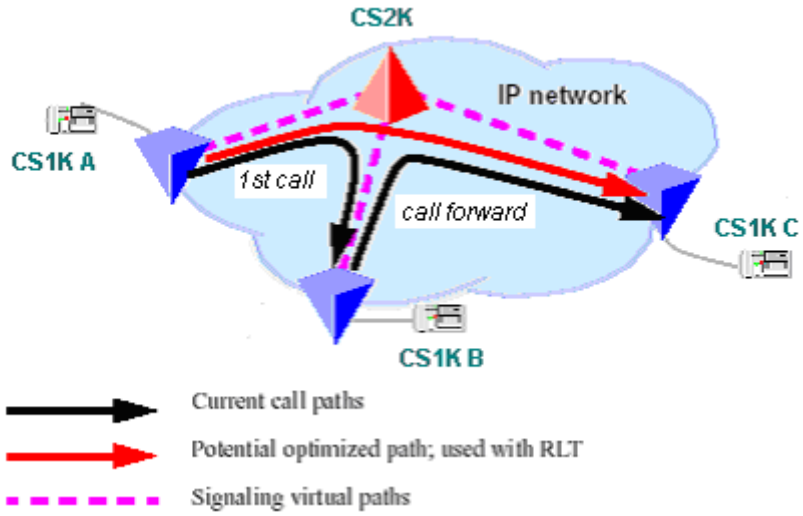


Figure 4 "User Side" RLT Functional Behavior

This scenario will also apply to call transfer in the CS1K. The CS2000 is only capable of processing RLT that is initiated by another H323 gateway such as CS1K; therefore, it is only capable of user side RLT.

1.1.4.2 Network Side RLT (CS 2100 only)

The second scenario is shown in the following figure. In this figure, CS1K A is calling an H323 gateway connected to the CS2100, and CS2100 call forwards to CS1K C. The invocation of RLT by CS2100 allows the CS1K A to bridge the call, making a new call from CS1K A to CS1K C. This invocation frees up the signaling path between CS2100 and the CS1K C.

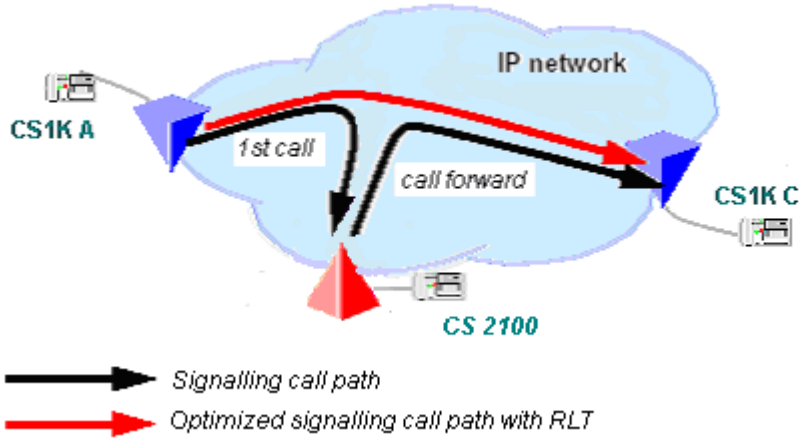
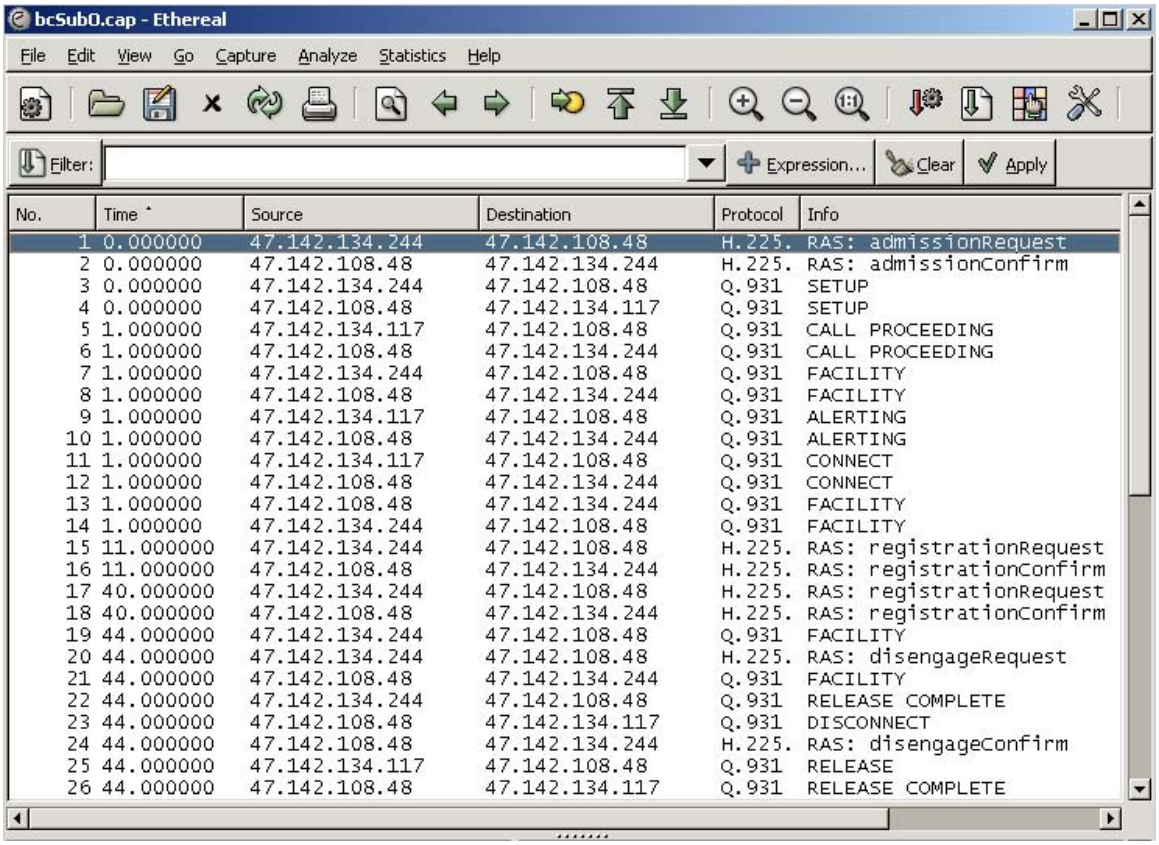


Figure 5 "Network Side" RLT Functional Behavior

This scenario will also apply to call transfer in the CS 2100. Since the CS2100 is the initiator of the RLT, it is performing the Network side RLT function.

1.1.5 H323 and Q.931 messaging

The H323 call processing messaging uses Q.931 within the H323 message. To demonstrate this, the packet capture tool in the GWC was used to capture packets from the H323 Gateway and packets formatted as Q.931 to send to CS2K. H323 Gateway: IP 47.142.134.244, GWC IP: 47.142.108.48 and CS2K IP: 47.142.134.117.

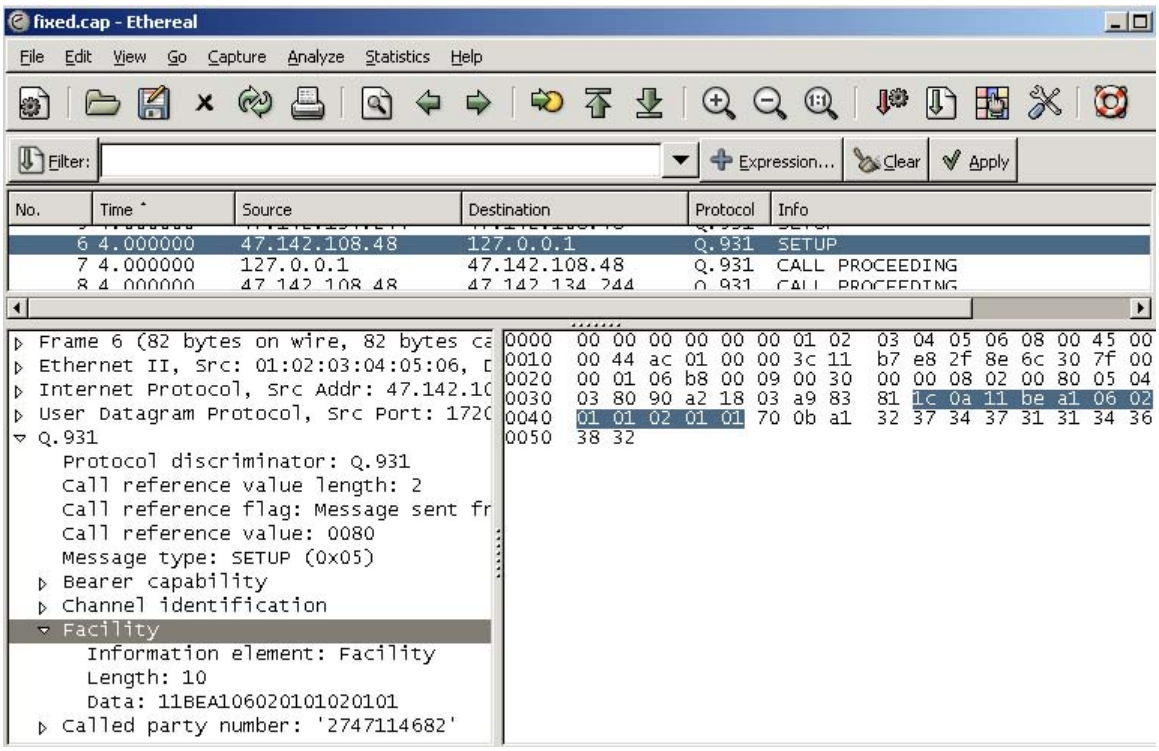


No.	Time	Source	Destination	Protocol	Info
1	0.000000	47.142.134.244	47.142.108.48	H.225.	RAS: admissionRequest
2	0.000000	47.142.108.48	47.142.134.244	H.225.	RAS: admissionConfirm
3	0.000000	47.142.134.244	47.142.108.48	Q.931	SETUP
4	0.000000	47.142.108.48	47.142.134.117	Q.931	SETUP
5	1.000000	47.142.134.117	47.142.108.48	Q.931	CALL PROCEEDING
6	1.000000	47.142.108.48	47.142.134.244	Q.931	CALL PROCEEDING
7	1.000000	47.142.134.244	47.142.108.48	Q.931	FACILITY
8	1.000000	47.142.108.48	47.142.134.244	Q.931	FACILITY
9	1.000000	47.142.134.117	47.142.108.48	Q.931	ALERTING
10	1.000000	47.142.108.48	47.142.134.244	Q.931	ALERTING
11	1.000000	47.142.134.117	47.142.108.48	Q.931	CONNECT
12	1.000000	47.142.108.48	47.142.134.244	Q.931	CONNECT
13	1.000000	47.142.108.48	47.142.134.244	Q.931	FACILITY
14	1.000000	47.142.134.244	47.142.108.48	Q.931	FACILITY
15	11.000000	47.142.134.244	47.142.108.48	H.225.	RAS: registrationRequest
16	11.000000	47.142.108.48	47.142.134.244	H.225.	RAS: registrationConfirm
17	40.000000	47.142.134.244	47.142.108.48	H.225.	RAS: registrationRequest
18	40.000000	47.142.108.48	47.142.134.244	H.225.	RAS: registrationConfirm
19	44.000000	47.142.134.244	47.142.108.48	Q.931	FACILITY
20	44.000000	47.142.134.244	47.142.108.48	H.225.	RAS: disengageRequest
21	44.000000	47.142.108.48	47.142.134.244	Q.931	FACILITY
22	44.000000	47.142.134.244	47.142.108.48	Q.931	RELEASE COMPLETE
23	44.000000	47.142.108.48	47.142.134.117	Q.931	DISCONNECT
24	44.000000	47.142.108.48	47.142.134.244	H.225.	RAS: disengageConfirm
25	44.000000	47.142.134.117	47.142.108.48	Q.931	RELEASE
26	44.000000	47.142.108.48	47.142.134.117	Q.931	RELEASE COMPLETE

The GWC receives the H323 messages and creates new Q.931 messages to send to the CS2K. When the GWC receives the CS2K response, it will create a new H323 message from the content of the received message. Therefore, data does not pass from the H323 interface to the CS2K interface transparently. Every component of the Q.931 message is examined and a decision is made within the GWC whether to pass this data. For example, a CS2K DISCONNECT message is translated to a RAS message for H323.

For each message, the content can be viewed using the Ethereal built in decipher of Q.931 as shown in the example below for the SETUP message. In this example, the deciphered message contains the RLT Facility, being sent from the H323 Gateway, forwarded to the CS2K. It is also interesting to note

that the call reference value is a 2 byte field on GWC to H323 messages but only one byte is used for the GWC to CS2K.

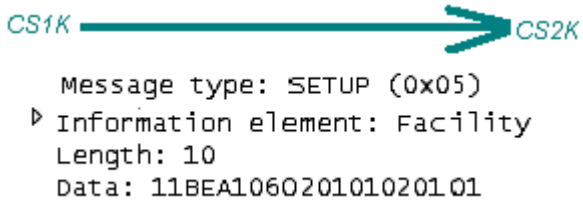


1.1.6 RLT message components

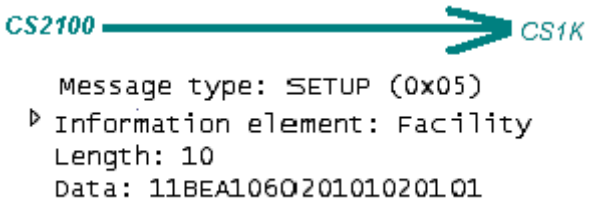
The RLT functionality is accomplished by adding a message component to the SETUP and ALERT messages and uses a new the FACILITY message to invoke RLT.

1.1.6.1 SETUP Message

CS1K SETUP messages for new calls will all contain the facility RLT.

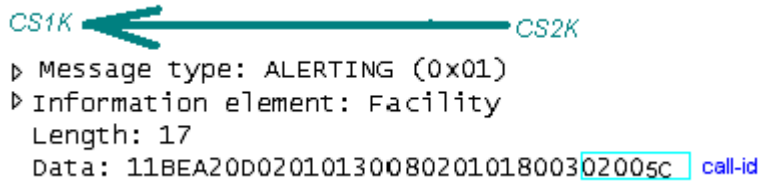


CS2100 SETUP messages for call forward or call transfer will contain the same facility RLT.

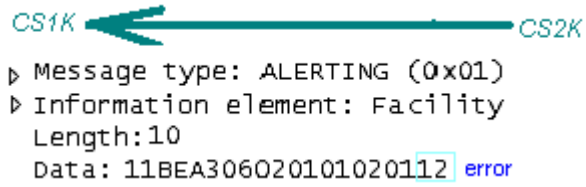


1.1.6.2 ALERT from CS2K

When CS2K is RLT provisioned and it receives an RLT Facility in the SETUP message, CS2K ALERT response messages will have the call-id in the facility RLT.

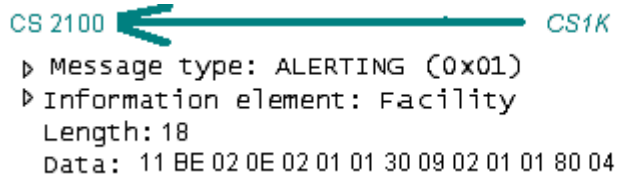


When CS2K is NOT RLT provisioned and it receives an RLT Facility in the SETUP message, CS2K ALERT response message will have and error indicating no RLT support.

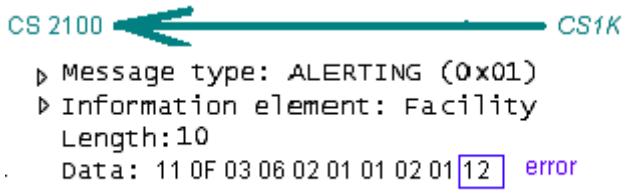


1.1.6.3 ALERT from CS1K

When CS2K sends an RLT Facility in the SETUP message, if CS1K is RLT provisioned, it will send an ALERT response messages with the call-id in the facility RLT.



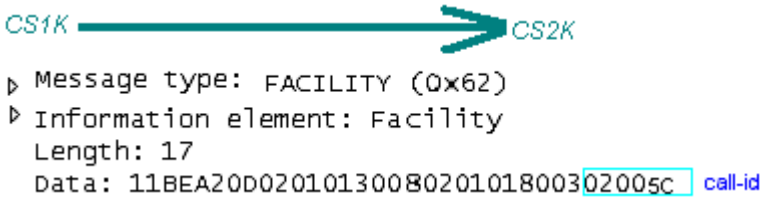
When CS2K sends an RLT Facility in the SETUP message but the CS1K is NOT RLT provisioned it will receive an ALERT response message with error indicating no RLT support.



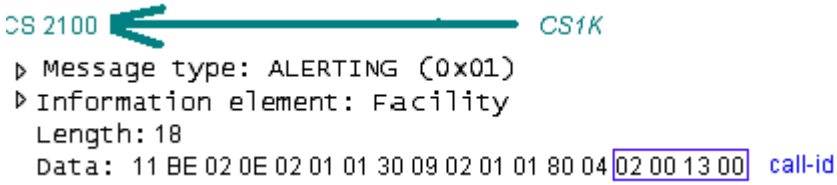
1.1.6.4 FACILITY RLT

After a successful call forward or call transfer, the FACILITY RLT message is used to free up the signaling links. The FACILITY RLT message contains the data returned in the ALERT message. Therefore, a FACILITY RLT message will can only be performed when the CS2K is properly provisioned for RLT on the particular trunk group.

The CS1K will send the FACILITY RLT message with the information it receives from the CS2K ALERT message.

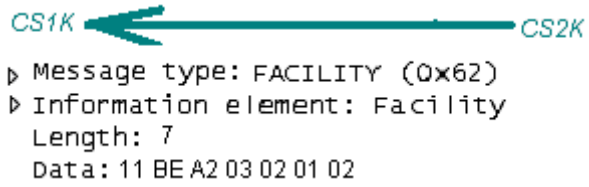


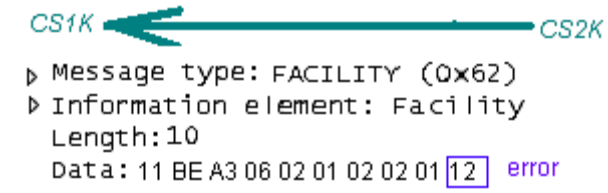
The CS 2100 will send the FACILITY RLT message with the information it receives from the CS1K ALERT message.



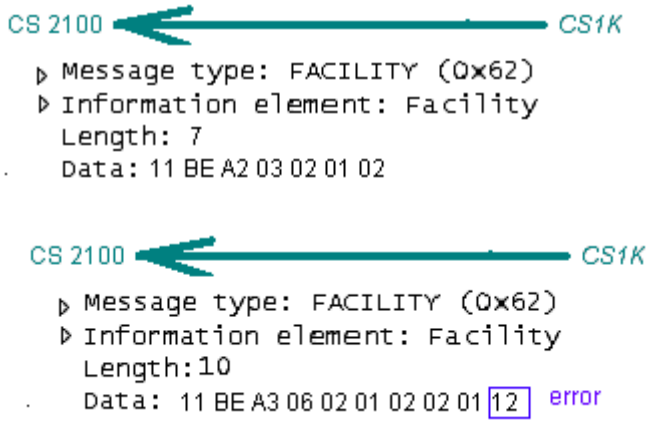
1.1.6.5 FACILITY RLT Response

The CS2K will send a response for the FACILITY RLT success or it will send an error indication.





CS1K response for FACILITY RLT message is the same as the CS2K.



1.2 Hardware Requirements or Dependencies

The H323 RLT capability is a software only component for GWC.

1.3 Software Requirements or Dependencies

The H323 RLT software requirements for the CS1K are described outside the scope of this document in CS1K feature DE2302. Since RLT is requested by the H323 Gateway, the GWC will not perform any RLT action without a Nortel H323 Gateway, such as the CS1K.

1.4 Limitations and restrictions

The CS2K will provide the RLT functionality described in *NTNA PRI Specification* (NIS A211-1).

1.5 Interactions

The RLT functionality is independent of the MCDN tunneling component of the H323.

Product = CS 2000

A00009190-- Universal Carrier Protocol (UCP) C7UPTMR Enhancements

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

This activity in SN09 provides provisionable timer support on a per trunk basis for UCP Trunks. This is accomplished by

- Provisioning timers in table C7UPTMR for UCP protocol.
- Provisioning the C7UPTMR index in table TRKSGRP
- This feature will be tracked by Track SOC UCSB0001.

When there is no C7UPTMR index provisioned in table TRKSGRP, the default timer values are used.

Currently, the XPM patch XIX20, is used to hardcode the ACM timer value to 20 secs for UCS trunks. When the switch is upgraded to SN09 core load, this patch XIX20 will be Obsoleted. New patch, XHW10 for DTC should be applied to support provisionable timers on a per trunk basis for UCP Trunks. When trunks hosted on DTCs are used, this patch will allow the datafilled ISUP timer value to be used during CallP.

- Datafill table C7UPTMR for UCP Potocol with the required timer value.
- Datafill TRKSGRP to change the TMRNAME field to the datafilled C7UPTMR index.

1.1.1 Provisioning Table C7UPTMR

Table C7UPTMR provides the ability to provision various ISUP timer values on a per-protocol and direction basis. The ISUP (ISDN User Part) timer values that can be provisioned in table C7UPTMR are dependent on the protocol. This activity supports provisioning of timers for UCP protocol. The new UCP timer implementation is modeled after the existing provisionable timers for the Q764 protocol. Refer to the following figure for a sample UCP C7UPTMR datafill.

Figure 1 Examples of the C7UPTMR Datafill

```
TABLE C7UPTMR
UCP2W 2W UCP 13 2 30 6 60 10 180 20 200 13 60 2 $
UCPIC IC UCP 13 6 60 20 200 13 60 $
UCPOG OG UCP 2 25 6 60 10 180 13 60 2 $
```

Refer to the following table for a brief description of the UCP timers, range and default values.

Table 1: UCP Timer Description

Timer Name ANSI	Timer Name Bellcore	Table C7UPTMR Field Name	Timer Range (Secs)	Default Value (Secs)	Direction Applicable	Description
COT	$T_{ccr,r}$	COT	10 to 15	13	IC, 2W	When responding to a continuity check request (CCR), awaiting a Continuity Test message (COT) or Release (REL)
T21	T_{cot}	TONE	2 to 2	2	OG, 2W	When responding to a continuity check in an Initial Address Message (IAM), awaiting return of suitable tone
ACM	T_{iam}	ACM	20 to 30	25	OG, 2W	When sending Initial Address Message IAM, awaiting Address Complete Message (ACM), Answer (ANM) or Release (REL).
REL	T_{rel}	RLCSREL	4 to 15	6	IC, OG, 2W	When sending REL, awaiting Release Complete (RLC); shorter timer used for retransmission
RLC	$T_{rel,l}$	RLCLREL	60 to 60	60	IC, OG, 2W	When sending REL, awaiting RLC; longer timer used for abnormal procedures
T7	unnamed	IRETEST	1 to 10	10	OG, 2W	Wait before initial COT retest
T8	unnamed	SRETEST	60 to 180	180	OG, 2W	Wait before subsequent COT retest
T11	$T_{cot,r}$	ICCR	16 to 20	20	IC, 2W	When receiving first COT coded “failed”, awaiting receipt of CCR
T13	$T_{cot,l}$	SCCR	180 to 300	200	IC, 2W	When receiving subsequent COT coded “failed”, awaiting receipt of CCR
T15	T_{rsc}	RLCSRSC	4 to 15	13	IC, OG, 2W	When sending Reset Circuit message (RSC), awaiting RLC; shorter timer used for retransmission
T16	$T_{rsc,l}$	RLCLRSC	60 to 60	60	IC, OG, 2W	When sending RSC, awaiting RLC; longer timer used for abnormal procedures

Table 1: UCP Timer Description

Timer Name ANSI	Timer Name Bellcore	Table C7UPTMR Field Name	Timer Range (Secs)	Default Value (Secs)	Direction Applicable	Description
T20	T_{ccr}	LPA	2 to 2	2	OG, 2W	When sending a CCR, awaiting receipt of Loop Back Acknowledgement

This feature will be tracked by Track SOC UCSB0001.

1.1.2 Provisioning Table TRKSGRP

Table TRKSGRP provides the ability to provision C7UPTMR index per trunk subgroup basis in field TMRNAME. The provisioned timers values are used for UCP call processing.

Figure 2 Example of the TRKSGRP Datafill

```
TABLE TRKSGRP
LOOP3IMT2WS7A 0 DS1SIG C7UP 2W N N EXTERNAL NONE UCP THRH 0 DMSNODE
$ UCP2W CIC
```

Once TMRNAME field is updated in the Table TRKSGRP, BSY; RTS the trunk to make sure that the C7UPTMR INDEX for the trunk is reflected at the peripherals (GWC/XPM/SPM).

1.2 Hardware Requirements or Dependencies

None

1.3 Software Requirements or Dependencies

None

1.4 Limitations and restrictions

None

1.5 Interactions

None

1.6 Glossary

Term	Description
CCR	Continuity Check Request
COT	Continuity Test
IAM	Initial Address Message
ISUP	ISDN User Part
RLC	Release Complete Message
REL	Release Message
RSC	Reset Circuit Message
UCP	Universal Carrier Protocol

Product = CS 2000

A00009200 -- Packet Trunking Trunk Test: Milli-watt Tone Swap

Functional Description

1: Applicable Solution(s)

PT-IP

1.1 Description

The purpose of this feature is to provide the customer the capability to perform a function known as Milli-watt Tone Swap from the MAPCI TTP interface on a Gateway TDM trunk circuit in the Succession XA-Core non-hybrid and Compact CS2K platforms. The new command is supported for all fabrics where the AudioCodes Media Server 2000 series media servers are supported, which includes AAL2, AAL5, and IP. The AAL1 solution is not being considered at this time (as no AudioCodes Media Server is supported in that solution) and no verification is being planned. This feature utilizes the combined capabilities of the XA-Core, Audio Controller (AC) and AudioCodes Media Server (AMS).

Milli-watt Tone Swap is defined as passing a well-known tone, the milli-watt tone of 1004 Hz., at a selectable power level, over a DS-0 trunk circuit on a Gateway TDM trunk, to a far-end switch wherein the amount of transmission loss can be measured. Simultaneously and independently, the far-end switch will pass the same 1004 Hz. tone back over the same trunk circuit wherein the

amount of transmission loss can then be measured by the near-end switch. This operation permits the customer to ensure two-way voice path is present and verify trunk padding is set correctly.

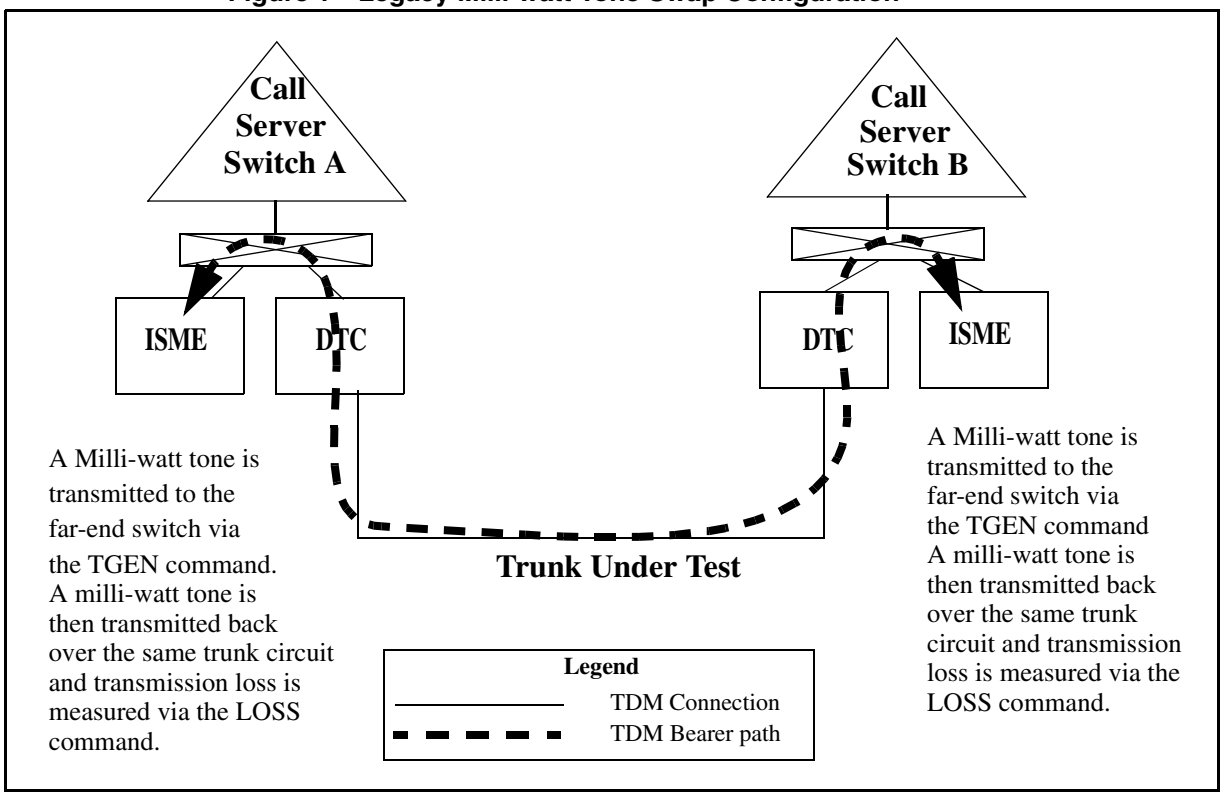
This feature introduces a new command, MWTSwap, from the MAPCI TTP interface, available only on the Succession CS2K & Compact CS2K platforms. The hardware required to perform the test will reside in the AudioCodes Media Server 2000 Series products.

1.2 Configuration Overview

1.2.1 Legacy DMS Milli-watt Tone Swap Configuration

In a conventional DMS configuration Milli-watt tone swapping can be performed via the combination of the TGEN and LOSS commands located on the MAPCI TTP interface. The user must perform each function of the Milli-watt tone swap separately, once to generate the desired milli-watt tone with the TGEN command, followed by a loss measurement with the LOSS command while the far-end is generating the tone. This command implementation does not permit the user to perform both functions simultaneously. Milli-watt tone swap in legacy is executed using special hardware in the Integrated Service Module Equipment or ISME connected to the ENET. Both command requests are originated by the user from the MAP interface. Connections are created between the Trunk Under Test and the appropriate trunk testing hardware resident on a local ISME. In order to perform Milli-watt tone swap a coordinated effort must be made between craft persons at both switches.

Figure 1 Legacy Milli-watt Tone Swap Configuration

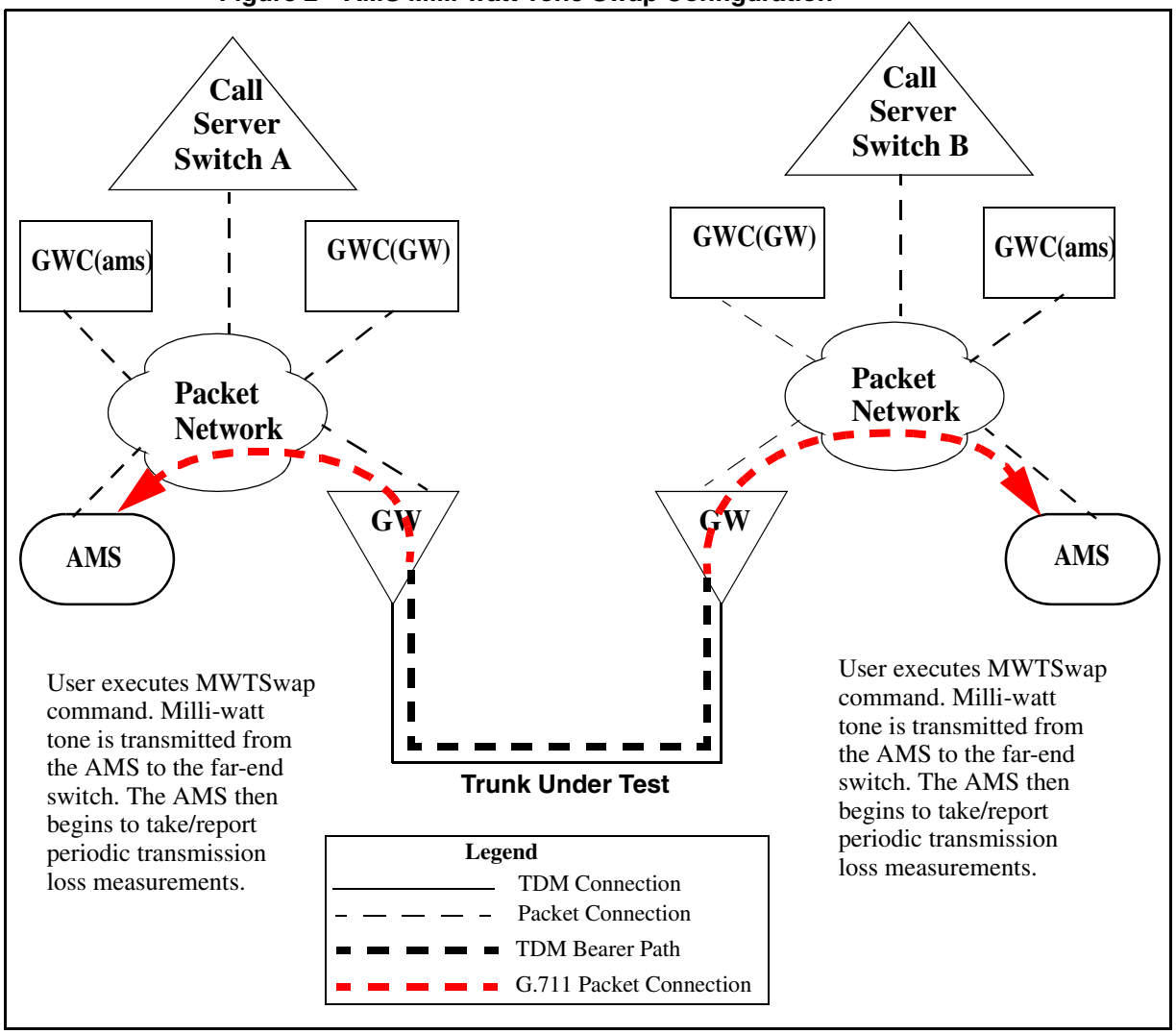


1.2.2 Packet Milli-watt Tone Swap Configuration

The implementation of this feature offers a new method of conducting milli-watt tone swapping via the DSP hardware resident in the AudioCodes Media Server (AMS) 2000 series products. This configuration has the capability of operating without the need for an ENET or ISME. A new command will be introduced at the MAPCI TTP interface called MWTSwap. This new command will perform both the tone generation and loss measurement functions simultaneously.

When the crafts-person invokes the new command, connections are established between the AMS and the Gateway TDM Trunk Under Test. A milli-watt tone is then generated towards the far-end switch. Simultaneously, transmission loss measurements will be taken, on a periodic basis, on the same trunk circuit and displayed on the MAP screen. In order to perform Milli-watt tone swap a coordinated effort must be made between craft persons at both switches, but because the two functions are executed together the coordination required is less.

Figure 2 AMS Miili-watt Tone Swap Configuration



1.3 Functional Overview

As mentioned earlier this feature will introduce a new command at the MAPCI TTP level interface. The new command, MWTSwap, will appear on the TTP level screen only when the office parameter EXTERNAL_GATEWAY_TEST_LINES is set to ‘Y’ in table OFCVAR. This office parameter determines which test head will be used for hardware based TTP/ATT level trunk testing. The default is ‘N’ which indicates that tests will use the existing hardware located in the ISM/MTM peripheral. When set to ‘Y’, all testing currently supported will be performed via the AudioCodes Media Server (AMS) 2000 series products.

Please note: AMS based testing is only supported on Gateway TDM trunks. No support is currently available for legacy peripheral TDM trunks.

The following is an example of the new command on the MAPCI TTP level interface.

```
 XAC      MS     IOD     Net      PM     CCS     Lns     Trks    Ext     APPL
Baseln  01SBPT  DLOG E   LOAD    1 DPT     .    SYSB     22C..   1Crit   SDM
  M                                *C*            *C*     *C*     *C*     M
  MANUAL
 0 QUIT       POST    23  DELQ            BSYQ          DIG
 2 Post_      TTP 27-0002
 3 MWTSwap    CKT TYPE      PM NO.          COM LANG      STA S R  DOT TE  RESULT
 4            2W S7 S7 GWC   9     1  H248ISUPITOG    1                    No Tn
 5 BSY                                                                    1004Hz
 6 RTS
 7 TST        EML  0.0 DB
 8 Noise      PAD PC 0 TE 0
 9 OP_
10 TDet
11 Hold       MWTSwap  f 1004 p 0 d 60
12 NEXT
13 RLS
14 HSet
15 Jack_
16 SGNL
17
18 CallTrf
  BRIAN
Time  10:46
```

When the ofcvar EXTERNAL_GATEWAY_TEST_LINES is activated the MWTSwap command will appear as a menu item to the crafts person. Note that the commands TGEN and Loss will be removed as menu items since they are currently not supported in the XA-Core non-hybrid and compact CS2K solution.

The following steps are performed to execute the command MWTSwap from the MAPCI TTP MANUAL level interface both on a Succession XA-Core non-hybrid or Compact CS2K platform.

1. Crafts person posts a trunk circuit which will be tested at the MAPCI TTP level interface.
2. The crafts person enters the MANUAL level.
3. The command MWTSwap is executed with the optional parameters to specify the tone frequency, power level, and test duration. If no optional parameters supplied, the default parameters are used, which are 1004 Hz. at 0 dB for 60 seconds.

   Please note although the command line interface provides for entering a tone frequency, only the 1004 Hz. frequency is supported for this feature. If a frequency other than 1004 Hz. is entered, the crafts person will be alerted with an error message.

4. Trunk is seized and connections established between the AMS and Gateway TDM trunk, the AMS is sent a request to perform the test.
5. Tone is generated on the outgoing Gateway TDM trunk, at the same time the AMS begins taking loss measurements and reporting them back to the CS2K.
6. The MAPCI TTP level interface is updated with the loss measurements on a periodic basis (every few seconds).
7. After the test duration completes the AMS will time out and release the connection and terminate the test.
8. The MAP screen will be cleared and the trunk reverts to its original state prior to the test being invoked.

Parameter	Range
Tone frequency	Currently only supports 1004 Hz.
Tone power level	-60 to 0 dB
Test Duration	1 to 240 seconds

1.4 MWTSwap frequency error message

This feature supports the generation of a tone frequency of 1004 Hz. If a crafts person enters any other frequency (1005 Hz in the example below) the following error message will be provided:

```
MWTSwap  f 1005
USING DEFAULT POWER LEVEL (0 DB)
USING DEFAULT DURATION (60 SECS)
Action not supported - invalid frequency entered.
Frequency is currently restricted to 1004 Hz for MWTSWAP command.
```

Other command level errors are documented in the CI section of this feature documentation as well as applicable Nortel NTP documentation.

1.5 Hardware Requirements or Dependencies

AudioCodes Media Server 2000 Series (MS2010, MS2020)

1.6 Software Requirements or Dependencies

This functionality will be available in SN09.

1.7 Limitations and restrictions

1. Tone frequency generation limited to 1004 Hz..

2. Loss measurement requires presence of Milli-watt tone. AMS will provide loss measurement data if 1004 Hz. tone is received. If no tone is present or if tone received is not 1004 Hz. the craftsperson will be alerted with an informational message of "No Tn" on the MAPCI display in place of the loss reading.
3. 32 Simultaneous MWTSwap commands can be conducted per AMS.
4. In SN09 only ISUP trunk types are supported for the MWTSwap command. PTS and PRI trunk types are blocked to prevent the command from being run on them.

1.8 Applicable customer facing sections

Fault Management

Logs	___N___
Alarms	___N___

Configuration

Data Schema	___N___
User Interface	___Y___
Element Management	___N___
Security	___N___
Service Order	___N___
Office Parameters	___N___

Accounting (includes AMA billing)	___N___
Performance (includes operational measurements)	___N___

1.9 Glossary

Term	Description
AMS	AudioCodes Media Server
GWC	Gateway Controller
AC	Audio Controller
MTM	Maintenance Trunk Module
ISME	Integrated Services Module Equipment
PVG	Passport Voice Gateway

1.10 T105 NT Responder Variant Support

The purpose of this section is to reference an additional part of this feature to provide the additional sub-test called “NT” to the T105 responder test capabilities of the AudioCodes Media Server 2000 Series (AMS) products. Today, the AMS currently supports the Nortel standard T105 test which is comprised of the following sub-tests:

a. L - Two-way loss measurement at 1004 Hz. and 0 dBm.

b. N - Far-end noise measurement with C-msg filter.

c. RN - Near-end noise measurement with C-msg filter.

d. LSC - Far-end loss self check with 1004 Hz. and 0 dBm.

e. NSC - Far-end noise self check with C-msg filter.

This support is made available for the Compact CS2K and non-hybrid CS2K configurations in which there is no ISM/MTM present which houses the traditional DMS test trunk hardware. The AMS provides a limited replacement for trunk testing to the ISM/MTM in these configurations.

The “NT” test is defined via the AT&T Technical Advisory No. 17 section CB106 as:

NT - Two-way noise measurement C-msg filter with tone at 1004 Hz. and -16 dBM.

The AMS provides the “NT” sub-test to the T105 responder functionality in the AMS. A far-end switch signaling to perform an “NT” test as a part of aT105 request can now be handled by the AMS. No development was required by Nortel for this feature. All development effort was performed by AudioCodes. The AMS support for the “NT” sub-test is limited to the responder or terminating side. A T105 test originating on an AMS will not request an “NT” sub-test.

2: Configuration for A00009200

2.1 Hardware and Software Requirements

For the MWTSwap command to be usable there needs to be a third party test equipment box installed. In SN09 the only supported third party test box that can run MWTSwap is the AudioCodes Media Server (AMS) series products. Once the AMS is installed, the office parameter “EXTERNAL_GATEWAY_TEST_LINES” in table OFCVAR should be set to “Y”. If this office parameter is set to “N” then it is assumed that the MTM is being used for test equipment and the MWTSwap command will be rejected.

2.2 User interface changes

2.2.1 Directory: MAPCI;MTC;TRKS;TTP;MANUAL

2.2.1.1 Directory description

This MAP level contains the TTP commands for manual trunk test position tests like TGEN, LOSS, etc.

2.2.1.2 Accessing directory: LEVEL MAN

2.2.1.2.1 Access to directory or MAP level and return to CI

To access the MANUAL level of the MAP enter "MAPCI;MTC;TRKS;TTP;LEVEL MAN" at the CI.

To return to the CI level enter "QUIT ALL" or simply "QUIT" to move up to the next higher level (the TTP level in this case).

2.2.2 Command: MWTSwap

2.2.2.1 Command type: Listed MENU and Unlisted MENU

The MWTSwap command is available at the general TTP level command directory as soon as the TTP level is entered. At the TTP level the command is an Unlisted Menu command. The MWTSwap command is also a Listed Menu command at the MANUAL level under the TTP level. Once the MANUAL level is entered the MWTSwap command appears in the menu.

Note: The MWTSwap command visibility at the MANUAL level is conditional on the value of the office parameter EXTERNAL_GATEWAY_TEST_LINES in table OFCVAR. If this office parameter is "Y" (Yes) then the MWTSwap command will be visible in the menu, and the commands "LOSS" and "TGEN" will be removed from the menu (although will still be Unlisted Commands). When the office parameter is "N" (No) then the MWTSwap command will not be visible in the menu, but will still be an Unlisted command at the MANUAL level.

2.2.2.2 Command target: All

2.2.2.3 Command availability: RES

2.2.2.4 Command description

MWTSwap is a new command implemented as a single command that combines the functionality of the TGEN and LOSS commands. The new command causes a 1004 Hz tone to be generated towards the far-end switch on the posted trunk, while at the same time measuring the loss on an incoming 1004 Hz tone from the far-end switch on the selected trunk. The command should be used in a coordinated fashion with a craftsperson on the far-end switch such that the far-end switch is also generating a 1004 Hz tone at the

same time so that a valid loss measurement can be taken by the near-end switch. If no tone detectable on the incoming circuit then the MAP display will indicate this through the text “No Tn” in the results area of the MAP.

The MWTSwap command supports 3 command line parameters, a frequency between 0 and 4000 Hz, a power level between -60 dB and 0 dB (in increments of 1 dB), and a test duration between 1 and 240 seconds. If no command line parameters are present the defaults of 1004Hz, 0 dB, and 60 seconds are used.

Note: Although the frequency range allowed on the command line is between 0 and 4000 Hz, the only supported frequency at this time is 1004 Hz. If any other frequency is given on the command line the command will fail with an appropriate error message.

When the MWTSwap command is entered the MAP is updated to display the frequency of the tone being generated as well as loss measurement information. The loss measurement information is updated on a regular basis (every few seconds) based on data sent from the third party test equipment. The MWTSwap command acts slightly differently from the TGEN and LOSS commands in that it runs for a specified time limit, during which time the user does not have the ability to invoke any other commands. Once the test completes it will return control to the crafts person. The upper limit on the length of the test is 4 minutes (240 seconds), with the default being 60 seconds. The upper limit was considered to be sufficiently long to allow coordination between the near-end and far0end switches in starting the test and long enough to get a stable loss reading on the trunk.

2.2.2.5 Command syntax

Table 1 MWTSwap command parameters and variables

Command	Parameters and variables
MWTSwap	Frequency, Power Level, and Test Duration
MWTSwap	F <Frequency> (0 to 4000) P <Power Level> (-60 to 0) D <Test Duration> (1 to 240)
Parameters and variables	Description
Frequency	Optional parameter. The frequency in Hz of the tone to be generated. Default is 1004 if not present on the command line.
Power Level	Optional Parameter. The power level (in decibels) of the tone to be generated. Default is 0 dB if not present on the command line.
Test Duration	Optional Parameter. The length of the test in seconds, ranging from 1 to 240 seconds. Default duration is 60 seconds if not specified on the command line.

The following is the command syntax as displayed to the user at the MAP:

```
help mwtswap
MWTSWAP-- MILLIWATT TONESWAP - GEN TONE AND MEASURE LOSS
Parms: [<FREQUENCY> {F <Frequency in Hz> {0 TO 4000}}]
       [<POWER LEVEL> {P <Power in dB> {-60 TO 0}}]
       [<TEST DURATION> {D <Duration in seconds> {1 TO 240}}]
```

Note that each of the command line parameters must be prefaced with the appropriate letter to indicate which option is being specified. For example, to specify a frequency of 1004 Hz, a power level of -6 dB and a duration of 120 seconds the command would be as follows:

```
MWTSWAP F 1004 P -6 D 120
```

It is possible to specify as many or as few options as needed on the command line. The only restriction on the optional parameters is that they must appear in the order specified in the syntax specified above. For example, the following command would be invalid and would generate the error shown:

```
MWTSWAP P -6 F 1004 D 30
USING DEFAULT FREQUENCY (1004 HZ)
EITHER incorrect optional parameter(s) OR too many parameters.
```

This is invalid as the frequency option “F” must be the first command line option if it is to be specified. Once the command interpreter sees the power level option “P” it assumes that the frequency will be the default value of 1004 Hz, and the F option is then treated as being an additional unnecessary parameter on the command line.

If no options are specified on the command line then the command will be executed with all the default values. An example of this is:

```
MWTSwap
USING DEFAULT FREQUENCY (1004 HZ)
USING DEFAULT POWER LEVEL (0 DB)
USING DEFAULT DURATION (60 SECS)
```

2.2.2.6 Qualifications and warnings

As noted above, the frequency is restricted to only 1004 Hz tones in SN09. Even though the frequency can be specified on the command line, any entry other than 1004 Hz will be rejected with an appropriate error message as follows:

```
MWTSWAP F 1005
USING DEFAULT POWER LEVEL (0 DB)
USING DEFAULT DURATION (60 SECS)
Action not supported - invalid frequency entered.
Frequency is currently restricted to 1004 Hz for MWTSWAP command.
```

2.2.2.7 Responses

2.2.2.7.1 Responses

Table 2 MAP outputs with associated meanings and actions

Command MWTSwap
"NOT ALLOWED": Error response **Meaning:** This response informs users that this command is not allowed on the posted trunk. This will occur when the office parameter "EXTERNAL_GATEWAY_TEST_LINES" in table OFCVAR is set to "N" and the MWTSwap command is executed. **System or user actions:** Check the value of the office parameter. If it is "N" then the office is not setup to use third party test equipment that supports the MWTSwap command.
"MWTSwap f 4001 Out of range: <Frequency in Hz> {0 TO 4000} Enter: <Frequency in Hz> [<POWER LEVEL>] [<TEST DURATION>]": Error response **Meaning:** The frequency parameter was entered incorrectly on the command line. **System or user actions:** Ensure that a valid frequency is entered on the command line. The allowable range is "0 to 4000".
"MWTSwap f 1005 USING DEFAULT POWER LEVEL (0 DB) USING DEFAULT DURATION (60 SECS) Action not supported - invalid frequency entered. Frequency is currently restricted to 1004 Hz for MWTSWAP command.": Error response **Meaning:** The frequency parameter was entered incorrectly on the command line. **System or user actions:** Ensure that a valid frequency is entered on the command line. In SN09 the only allowable frequency value is 1004 Hz even though the rage for the parameter is shown as 0 to 400 Hz.
"MWTSwap p 10 USING DEFAULT FREQUENCY (1004 HZ) Out of range: <Power in dB> {-60 TO 0} Enter: <Power in dB> [<TEST DURATION>]": Error response **Meaning:** The power level parameter was entered incorrectly on the command line. **System or user actions:** Ensure that a valid power level is entered on the command line. The valid range for power level is between -60 and 0 dB in steps of 1 dB.

Table 2 MAP outputs with associated meanings and actions

Command MWTSwap
"MWTSwap d 250 Wrong type: <Power in dB> {-60 TO 0} Enter: <Power in dB> [<TEST DURATION>]": Error response **Meaning:** The test duration parameter was entered incorrectly on the command line. **System or user actions:** Ensure that a valid test duration is entered on the command line. The valid range for test duration is between 1 and 240 seconds.
"POST A CIRCUIT AND TRY AGAIN": Error response **Meaning:** The command was entered without a trunk circuit posted at the MAP. **System or user actions:** Ensure that a trunk circuit is posted at the MAP and re-execute the command.
"TESTTRKANN OOS": Error response **Meaning:** The command was entered while the test trunk announcement are out of service.. **System or user actions:** Post the test trunk announcement at the MAP and take any corrective action required to bring the announcement to an IDL state.
"TEST COMPLETE": Valid response **Meaning:** The test has completed successfully with no errors. **System or user actions:** None.

2.2.2.8 Example

Table 3 Usage examples for MWTSwap command

Description of task:	Generate a 1004 Hz tone at 0 dB for 60 seconds and measure loss on a trunk circuit
Command: MAP response:	Example: MWTSwap Example: USING DEFAULT FREQUENCY (1004 HZ) USING DEFAULT POWER LEVEL (0 DB) USING DEFAULT DURATION (60 SECS) TEST COMPLETE
Description of task:	Generate a 1004 Hz tone at -6 dB for 60 seconds and measure loss on a trunk circuit
Command: MAP response:	Example: MWTSwap P -6 Example: USING DEFAULT FREQUENCY (1004 HZ) USING DEFAULT DURATION (60 SECS) TEST COMPLETE

Table 3 Usage examples for MWTSwap command

Description of task:	Generate a 1004 Hz tone at 0 dB for 120 seconds and measure loss on a trunk circuit
Command: MAP response:	Example: MWTSwap D 120 Example: USING DEFAULT FREQUENCY (1004 HZ) USING DEFAULT POWER LEVEL (0 DB) TEST COMPLETE
Description of task:	Generate a 1004 Hz tone at -20 dB for 240 seconds and measure loss on a trunk circuit
Command: MAP response:	Example: MWTSwap P -20 D 240 Example: USING DEFAULT FREQUENCY (1004 HZ) TEST COMPLETE

Product = CS 2000

A00009204-- Call Agent Customer Visible Capacity Tools

Functional Description

1: Applicable Solution(s)

PT-IP, PT-AAL2

1.1 Description

This feature covers the changes required to the Customer Visible Capacity Tools for the SOS Call Agent blade on Siren. The Capacity Tools covered by this feature are:

- CAPCI tool
- CAPACITY MAP levels

1.1.1 CAPCI CI Command

The following figure is a prototype of the output of the CAPCI CI command.

Figure 1 CAPCI Command Output

```
>capci
CAPCI -- 2004/12/13 12:42:24.018
CATMP/HR UTIL ENGCATMP ENGLEVEL MAXCATMP SYNC OVRLD IDLE COMPLEX
 1200000  50%  2400000    BELOW  2600000 +HOT   OFF  YES    1140
```

```
>query capci
```

```
CAPCI -- Display status of switch activity
Parms: [<option> {PARMS,
                  SCHEDMAP,
                  ALL}]
```

The output of the CAPCI ALL CI will output all the options available for CAPCI. The order of the output is CAPCI + SCHEDMAP + PARMS.

The following figure is a prototype of the output of the CAPCI ALL CI command.

Figure 2 CAPCI ALL Command Output

```
 >capci all
CAPCI -- 2004/12/13 12:42:24.018
CATMP/HR UTIL ENGCATMP ENGLEVEL MAXCATMP SYNC OVRLD IDLE COMPLEX
 1200000  50%  2400000    BELOW  2600000 +HOT   OFF  YES    1140

SCHED  FORE  MAINT   DNC  AUXCP    OM  GTERM    BKG   NETM   SNIP
  87%   10%    80%   83%     0%   81%    66%    62%     0%    66%

    Guaranteed_Terminal_CPU_Share = 0.0%
    AUXCP_CPU_Share               = 1.0%
    CC_Englevel_Warning_Threshold = 100%
    NETM share setting            = 0.0%
    DNC share setting             = 0.0%
    SNIP share setting            = 0.0%
    1% CPU allocation             = 10581 CATMP/HR
```

1.1.2 CAPACITY Map Level

This MAPCI level is accessed from >mapci;mtc;capacity. The CAPACITY MAPCI level output has been modified to match the CAPCI command.

The following figure is a prototype of the CAPACITY MAPCI display.

Figure 3 CAPACITY MAPCI Display

```
 CAPACITY
 0 Quit      CATMP/HR UTIL ENGCATMP ENGLEVEL MAXCATMP SYNC OVRLD IDLE COMPLEX
 2 Parms      1200000  50%  2400000    BELOW   260000  HOT   OFF  YES    1140
 3 SchedMap
 4           CAPACITY:
 5
 6
 7
 8
 9
10
11
12
13
14
15
16
17
18
```

1.2 Hardware Requirements or Dependencies

None.

1.3 Software Requirements or Dependencies

This feature requires the Siren Release 1.0 Call Agent platform.

1.4 Limitations and restrictions

This feature requires the Siren Release 1.0 Call Agent platform.

1.5 Interactions

Changes are being made to the current CAPACITY MAPCI level

Changes are being made to the CAPCI CI command.

1.6 Applicable customer facing sections

Fault Management

- Logs __NA___
- Alarms __NA__

Configuration

- Data Schema __NA__
- User Interface __NA__
- Element Management __NA__
- Security __NA__
- Service Order __NA__
- Office Parameters __NA__

Accounting (includes AMA billing) __NA__

Performance (includes operational measurements) __NA__

1.7 Glossary

Term	Description
New term	Definition

Product = CS 2000

A00009207 -- DPT Trunk Testing Support

Functional Description

1: Applicable Solution(s)

PT-AAL1

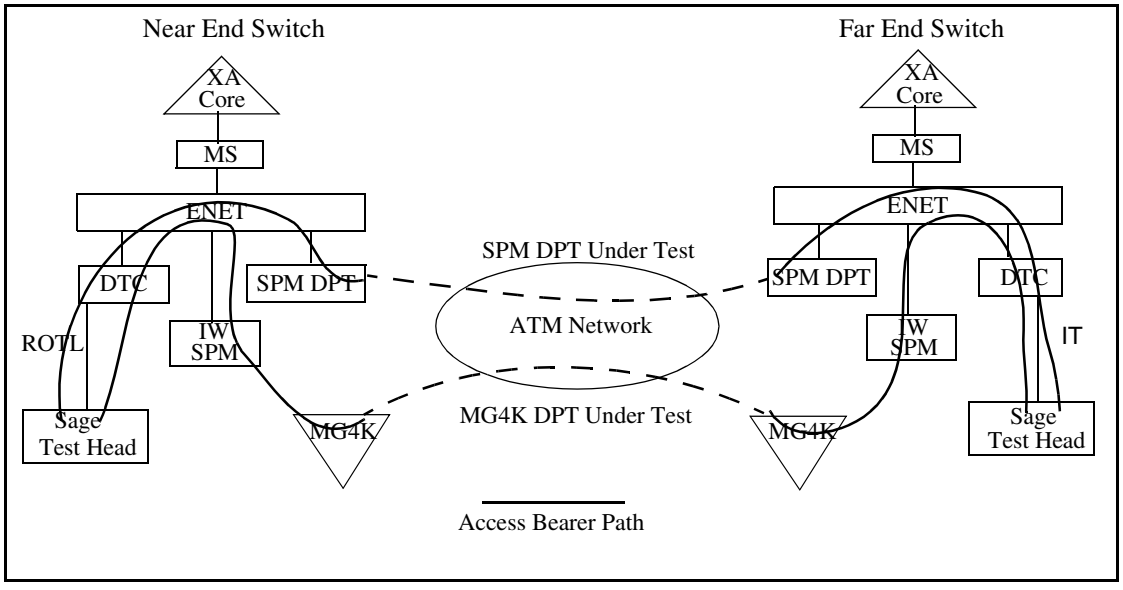
1.1 Description

This activity enhances the Digital Remote Office Test Line (ROTL) trunk interface to allow for the selection of a DPT node and Terminal Identifier (TID) if that DPT is hosted by a Spectrum Peripheral Module(SPM) or MG4K. In addition this feature allows the customer to select which SPM or MG4K to direct all incoming DPT test calls.

Digital ROTL is an existing DMS feature to remotely test trunks via a digital, four wire, E&M trunk. This CAS trunk interface permits a test head to be connected to the CS2K and, via a maintenance dial plan, select an outgoing trunk to be tested. A test head is connected to the CS2Kby a T1, on which several channels are provisioned with a ROTL trunk type. Test calls can then be outpulsed from the test head over the ROTL trunk members using a defined maintenance dial plan which instructs the CS2K software to select an outgoing trunk circuit and generate a test call to the far-end switch. A connection is then established between the test equipment and the trunk circuit being tested. Once all connections have been made the test head conducts the desired trunk test.

This feature enhances the Digital ROTL functionality to permit test connections over DPTs hosted by an SPM DPT or MG4K. The customer will be able to directly select the DPT group, node and TID to test.

Figure 1 Configuration Diagram



1.2 Digital ROTL Origination Feature Description

A test head in conjunction with the Digital ROTL feature permits the selection of an outgoing trunk to test via a maintenance dial plan outpulsed into the switch over a T1 interface. The group of digits in the dial plan which identify the outgoing trunk is known as the Port Identification Number. The current Digital ROTL Port Identification Number for TDM trunk selection is defined as the following:

KP + Test Line Id + ADNUM + Trunk Member + Testline Number + ST

KP - Key Pulse digit
Test Line Id - the code of the desired test (e.g. 05 = ROTL_105 testline id)
ADNUM - value from table CLLI represents the trunk group to be tested
Trunk Member - Member of the trunk from table TRKMEM
Testline Number - DN being outpulsed to the far end switch
ST - Stop or cut-through digit

With the introduction of DPT support by this feature, the existing TDM Port Identification Number portion of the maintenance dial plan is modified to select based on node and terminal number rather than trunk member. The new Port Identification Number will be defined as the following:

KP + Test Line Id + ADNUM + Node + Terminal + Testline Number + ST

KP - Key Pulse digit

Test Line Id - here new ids will be defined which will indicate trunk selection via the new node and terminal dial plan (#80 ROTL_100, #82 ROTL_102 and #85 for ROTL_105)

ADNUM - ADNUM from table CLLI represents the trunk group the DPT terminal will be assigned to.

Node - the node which the DPT terminal is allocated

Terminal - the DPT which will be tested

Testline Number - DN being outpulsed to the far-end switch

The CS2K software will parse this new Port Identification Number and a selection of the desired outgoing DPT terminal will be performed. A connection between the selected DPT terminal and the test head will then be made. Once established the desired trunk test will be performed by the test head.

1.2.1 Find the node number of the SPM

The NODENO command provides the number of the node to dial for testing the outgoing call. The command also prints a reminder of the valid DPT terminal number range for the SPM. The valid terminal ranges are:

- DPT SPM: 1 to 2016
- MG4000: 2079 to 4094

Finding the node number
At the MAP terminal
1. Access the DPT info debug tools by typing
```
>dptinfo
```
DPTINFO:

2. Enter the node number command
```
>nn node_type device_class device_no
```
Note: The short form for the nodeno command is "nn". where
node_type
for any SPM, node_type is "spm"
device_class
for any SPM, device_class is "spm"
device_no
is the SPM number found in table MNMODE.

Example
```
> nn spm spm 1
NODENO=70
This node has DPT terminals 2079-4094
>
```

1.3 DPT Test Call Termination Feature Description

In conjunction with the design to provide DPT test support via the Digital ROTL interface, incoming DPT test calls will have the capability to be routed to a desired DPT node. This selection will be data fillable, and once set, all incoming DPT calls flagged as a test call will terminate on the provisioned SPM (either DPT SPM or MG4K).

1.3.1 New office parameter DPT_BICC_TEST_NODE

This activity introduces a new office parameter, DPT_BICC_TEST_NODE in the table OFCVAR which will identify the particular node to which all incoming DPT test calls will be routed. This office parameter contains two fields, first PMTYPE and the second is SPM node number. Currently, the implementation of this office parameter will be limited to only the SPM node type. In addition, a check is place to ensure that the node number entered is supports DPT.

Note: During an ONP, if this new parameter exists in a previous software load, it will be propagated forward. If the office parameter does not exist in the previous load, the entry will be created in table OFCVAR with the default values of NIL_PMTYPE and '0'.

1.3.2 Set the CPC (Calling Party Category) in the ISUP IAM Message

A DPT test call IAM (Initial Address Message) initiated by the Digital ROTL feature is being modified to set the Calling Party Category (CPC) field to ISUP_CPC_TEST_CALL. At present this CPC field is set to the default of CPC_UNKNOWN. The CPC field will be used to identify if an incoming DPT call is considered to be a test call.

1.3.3 Move the incoming DPT Test Call to the provisioned terminating node

The incoming DPT test call will be moved to the desired SPM node based on the following:

- The call will be identified as a test call via the CPC field in the IAM message of ISUP_CPC_TEST_CALL.

- A look-up will be performed on the office parameter DPT_BICC_TEST_NODE and the provisioned SPM node will be returned.

- The incoming test call will then be moved to the desired node.

Note: Provisioning a desired terminating node effects test calls generated via the MAPCI;DPTTRKS level OP (Outpulse) command. Since a test call associated with this command sets the CPC of the IAM to ISUP_CPC_TEST_CALL.

1.4 Hardware Requirements or Dependencies

This feature enhances the existing Digital ROTL interface for trunk selection. A test head is required to perform the actual trunk test.

1.5 Software Requirements or Dependencies

Core: SN09 or greater.

SOC option BAS00050 56Kb/sTrk Tst prt must be activated.

1.6 Limitations and restrictions

1. The T1 interface to the test head equipment will not be supported on an MG4K node type because the MG4K does not currently support the ROTL trunk type.

2. This activity supports DPT terminals hosted by an SPM or MG4K. No official support is made for GWC DPT terminals. However, no enforcement will be provided by this feature.

1.7 Interactions

Not applicable

1.8 Glossary

Term	Description
DPT	Dynamic Packet Trunk
ROTL	Remote Office Test Line
TID	Terminal Identifier
PTS	Per Trunk Signaling
SPM	Spectrum Peripheral Module
MG4K	Media Gateway 4000
DMS	Digital Multiplex System
ONP	One Night Process
CPC	Calling Party Category
IAM	Initial Address Message
CS2K	Call Server 2000

2: Configuration for A00009207

2.1 Hardware and Software Requirements

This activity requires the following:

- SOC option BAS00050 56Kb/sTrk Tst prt must be turned on

- This activity provides interface support for a new Port Identification Number in the Digital ROTL maintenance dial plan. A third party test head is required to use this interface to perform testing on DPT terminals. An example test head is the SAGE Instruments 945RTS test unit.

2.2 Initial Configuration

- SOC option activation
- Third party test head initialization

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

2.3.1 New/modified office/subnet parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/ CHANGED/ DELETED/	Domain (CM or Subnet Management
OFCVAR	DPT_BICC_TEST_NODE	NEW	CM

2.3.2 Parameter information

2.3.2.1 DPT_BICC_TEST_NODE

DPT_BICC_TEST_NODE

2.3.2.1.1 Functional description

This parameter identifies the node to which incoming DPT test calls are moved.

The purpose of this feature is to provide an interface to third party test heads to permit testing of Dynamic Packet Trunks(DPT), if that DPT is hosted by a SPM or MG4K. This interface allows the user to generate a test call over a desired DPT terminal to a remote switch. Since an incoming DPT call can be terminated on any available DPT node, provisioning of this parameter provides the node information to allow the test call to be terminated to a specified peripheral. This permits the customer to have a known path when conducting a test.

2.3.2.1.2 Provisioning rules

When an incoming DPT call is flagged as a test call from the data in the ISUP IAM message, if the user would like to specify which DPT node they would like to route call to, they can provision this information in this new parameter. The parameter accepts a node type and a node number. Currently, the node type will be limited to SPM and only for an SPM node type that supports DPT terminals.

2.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default

2.3.2.1.4 Activation

Enter a PMTYPE type of SPM and a valid node number within the range 0 to 85. If that SPM node exists and supports DPT terminals, then the parameter will be activated. The activation of this office parameter is immediate.

2.3.2.1.5 Dependencies
None.

2.3.2.1.6 Consequences
If the user enters an valid SPM node number but the SPM does not support DPT terminals, the following response will be provided:

'This node does not have DPT terminals allocated.'

If the user enters a node number out of range, the following response will be provided:

'Not a valid SPM number.'

2.3.2.1.7 Verification
A DPT group hosted by the SPM node provisioned in the office parameter can be posted at the DPTTRKS level and incoming DPT test calls will show active terminals.

2.3.2.1.8 Memory requirements
No memory impact.

2.3.2.1.9 Parameter release history update
Parameter DPT_BICC_TEST_NODE is new in this release.

2.4 Upgrade Considerations
No impact.

Product = CS 2000

A00009208 -- SN09 180K Lines Support
Functional Description

1: Applicable Solution(s)
UA-IP, IAW, IAC

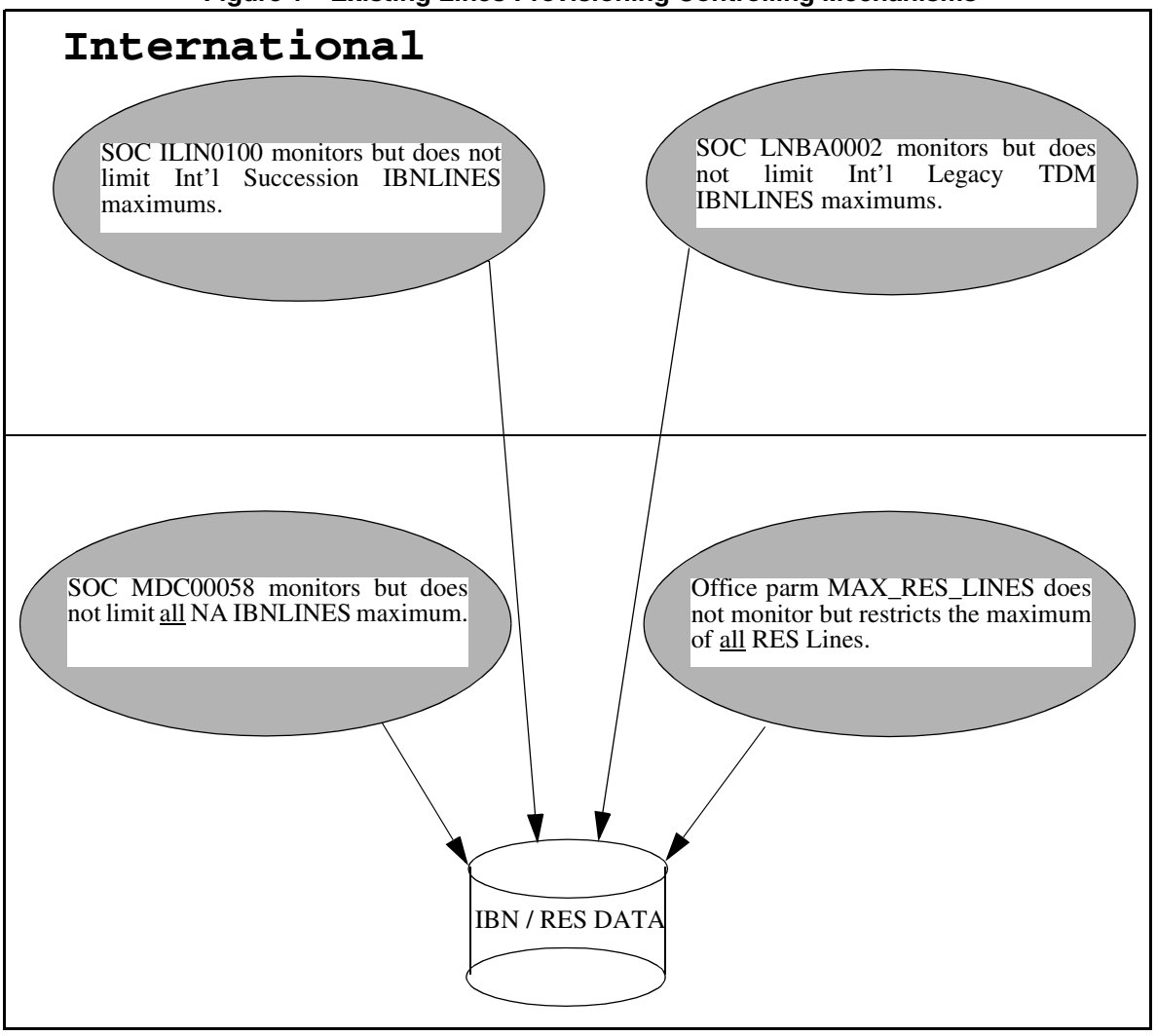
1.1 Description
The purpose of this feature is to increase the provisioning limits for lines globally from its current limit of 150k to 180k. The feature provides the ability to:

- provision a total of 180,000 RES lines for the North American market

- provision a total of 180,000 IBN lines for the International market
- perform Call Processing on each of these lines

There are no new SOCs or Office Parms introduced to activate the new provisioning limits. The capability is built into the SN09 load. The customer will use the existing mechanisms to allow provisioning of RES/IBN lines to these new limits. Refer to the following figure.

Figure 1 Existing Lines Provisioning Controlling Mechanisms



The specific SOCs mentioned in Figure 1are soft SOCs which means they monitor limits. Customers are allowed to go beyond their initial limit without Nortel intervention. For details on SOCs, please refer to the Maintenance and Operations Manual NTP 297-9881-500. This feature does not impact/change how these SOCs function.

The MAX_RES_LINES Office Parameter in Table OFCOPT does limit the maximum number of all RES lines provisioned. The range for this office parameter is increased from 1500 to 1800, and activation is immediate. For details on office parameters, please refer to the Office Parameters Reference Manual NTP-297-8021-855. This feature does not impact/change how this office parameter functions.

1.2 Hardware Requirements or Dependencies

There are no hardware dependencies required to execute this feature.

1.3 Software Requirements or Dependencies

Software Dependencies:

— CORE - SN09 release or later

Firmware Dependencies:

— None

1.4 Limitations and restrictions

This feature is applicable to:

- North American and International software releases
- the CS2000 and CS2000-Compact configurations
- the AAL1 and IP solutions

This feature restrictions are:

- Does not change the Engineered maximum number of GWCs supported in an Office, currently at 60.
- Does not change the Engineered maximum number of lines supported per GWC, currently at 6400.
- Does not change or implement any new SOC controls for line capacities
- Does not increase current TDM limit of 150K lines
- Does not address the MG9000 Manager limit of 110K native lines. (ABI-based lines are not included in the 110,000 MG 9000 Manager limit)
- The current core BHCA capacity is not a limiting factor for the line access call models.
- Does not impact the ACD limit which is changing from 30K to 99,999 with SN09 feature A00009085.
- Does not increase Call Processing Feature limits:
  — Current line service capacity limits apply (e.g., 50K Speed Call Long Lists)

— No more than 45% penetration of voice mail service (requiring CFW and MWT)

- Does not increase current Cable line capacity limit of 150K lines. 180K lines is possible with a combination of the current 150K Cable lines (with a maximum of 115K MTAs when RMGC is employed) and 30K TDM or other allowable non-Cable packet lines.

1.5 Interactions

The following are the feature interactions for A00009208 feature:

- Features which A00009208 is dependant on:
  — none
- Features which are dependant on A00009208:
  — none

1.6 Applicable customer facing sections

Fault Management

Logs ___n/a___

Alarms ___n/a___

Configuration

Data Schema ___n/a___

User Interface ___n/a___

Element Management ___n/a___

Security ___n/a___

Service Order ___n/a___

Office Parameters ___n/a___

Accounting (includes AMA billing) ___n/a___

Performance (includes operational measurements) ___n/a___

1.7 Glossary

Term	Description
SOC	Software Optionality Control

Product = CS 2000

A00009235 -- TLS for SIP
Functional Description

1: Applicable Solution(s)

PT-IP, IAC

TLS = Transport Level Security, a security protocol that enables secure data transmission between two communicating applications.

SIP = Session Initiation Protocol

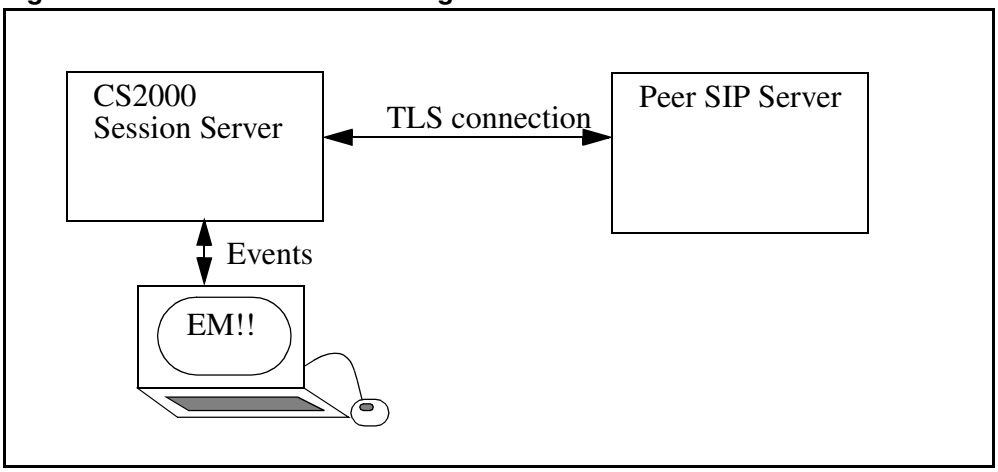
1.1 Description

The TLS for SIP feature will provide robustness improvements over the SN08 functionality, as well as provide compliance to specified Packet Cable requirements.

The peer-to-peer scenario is the focus of this feature. The peer SIP servers that the CS2000 Session Server connects to need to be authenticated, a TLS cipher must be selected, and the connection must be monitored, all to ensure the security of the connection and the validity of the messages being passed between the two peers. Most of this functionality has been delivered already, however some items remain (for example, FQDN/IP address mapping from the certificate, to ensure that FQDN's can be verified in the SIP messages).

Additional robustness improvements on the local CS2000 Session Server to alert the craft to issues in the system are required, and added flexibility to system/threshold settings are desired as well.

Figure 1 Functional Behavior Diagram



1.2 Hardware Requirements or Dependencies

No new hardware dependencies are introduced in SN09.

1.3 Software Requirements or Dependencies

This feature requires the standard SN09 load.

1.4 Limitations and restrictions

The following limitations exist for this feature:

Provisioning

- CS2000 Session Server Call Processing must be restarted anytime a new server certificate is provisioned (Call Processing is not required to be restarted if remote servers' certificates are provisioned).
- CS2000 Session Server Call Processing must be restarted for the following security parameters to take effect:
  ExitOnFailTLSInitialization
  MaxTLSSessions
  localTLSport
- Self-Signed Certificates from other servers must be data filled on the CS2000 Session Server in order to have the CS2000 Session Server recognize those certificates.
- Any Self-Signed Certificate from the current CS2000 Session Server must be data filled on other CS2000 Session Servers -- and other SIP servers in general -- in order to have the remote servers recognize those certificates.
- Restarting CS2000 Session Server Call Processing means restarting the SIP gateway application.

Performance

- Client-side session caching will be supported on the CS2000 Session Server. Server-side session-caching is already supported. However, the session cache exists only in memory. During a Dead-Office Recovery (DOR) new TLS sessions will require a full handshake.
- The maximum number of supported simultaneous TLS connections is limited to 400. The provisionable parameter 'MaxTLSSessions' controls this maximum number, and any connection attempts beyond the provisioned maximum will be rejected.

Cryptography

- Only RSA/DHE_RSA and AES/3DES ciphers will be enabled for use on the CS2000 Session Server by default. These will be the only ciphers supported by Nortel on the CS2000 Session Server. Specifically, the supported ciphers will be:
  TLS1_TXT_RSA_WITH_AES_128_SHA,

TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS1_TXT_RSA_WITH_AES_256_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA and
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.

- RSA keys used on the CS2000 Session Server will require a minimum of 1024 bits. RSA keys of smaller sizes are generally considered to be vulnerable to cracking.
- AES keys used on the CS2000 Session Server will require a minimum of 128 bits.
- Imported certificates will be expected to be in X509 version 3 PEM format,, in order to be imported for use by the CS2000 Session Server.

Licensing

- Licenses apply to certain open-source code (OpenSSL, Cryptlib) that are used in the CS2000 Session Server implementation of TLS. Terms of use require acknowledgement of the various authors in customer documentation materials etc. Please see appendix for full licenses of open-source code used within this product.

Certificate

- In this activity if the certificate and key files is changed in one NGSS, during initialization the mate host will be notified. If the mate host has not been updated with the new certificate and key files an alarm will raise. The limitation here is the application is not copying the certificate and key files over the mate host and by a craft person should do it.
- If the Common Name of the certificate contains an FQDN, it must match the Remote SIP Server name as provisioned in the Remote SIP Server web page. This FQDN must be less than 64 characters in length.
- Remote SIP Server Cluster configurations in which a single Remote SIP Server has been datafilled with multiple IP addresses must ensure that the Common Name of the certificate presented from any one of the IP addresses in the list matches either the IP address of the originator, or the FQDN as presented as the name of the Remote SIP Server.

1.5 Interactions

1.6 Glossary

Term	Description
TLS	Transport Level Security, a security protocol that enables secure data transmission between two communicating applications.
SIP	Session Initiation Protocol
DOR	Dead-Office Recovery, the term used to describe the complete loss, then recovery, of an entire office.

1.7 Appendix

- Open SSL license

```
//* ====================================================================
* Copyright (c) 1998-2004 The OpenSSL Project.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
*    notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
*    notice, this list of conditions and the following disclaimer in
*    the documentation and/or other materials provided with the
*    distribution.
*
* 3. All advertising materials mentioning features or use of this
*    software must display the following acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit.  (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
*    endorse or promote products derived from this software without
*    prior written permission. For written permission, please contact
*    openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
*    nor may "OpenSSL" appear in their names without prior written
*    permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*    acknowledgment:
*    "This product includes software developed by the OpenSSL Project
*    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
*
====================================================================
```

```
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com).  This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).

*
*/
```

- Eric Young's License

```
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
```

- Brian Gladman's License

```
---------------------------------------------------------------------------
Copyright (c) 2002, Dr Brian Gladman <brg@gladman.me.uk>, Worcester, UK.
All rights reserved.

LICENSE TERMS

The free distribution and use of this software in both source and binary
form is allowed (with or without changes) provided that:

  1. distributions of this source code include the above copyright
     notice, this list of conditions and the following disclaimer;

  2. distributions in binary form include the above copyright
     notice, this list of conditions and the following disclaimer
     in the documentation and/or other associated materials;

  3. the copyright holder's name is not used to endorse products
     built using this software without specific written permission.

ALTERNATIVELY, provided that this notice is retained in full, this product
may be distributed under the terms of the GNU General Public License (GPL),
in which case the provisions of the GPL apply INSTEAD OF those given above.

DISCLAIMER

This software is provided 'as is' with no explicit or implied warranties
in respect of its properties, including, but not limited to, correctness
and/or fitness for purpose.
---------------------------------------------------------------------------
Issue Date: 26/08/2003
```

- Peter Gutmann's License

```
/* The random pool handling code in this module and the misc/rnd*.c modules
   represent the cryptlib continuously seeded pseudorandom number generator
   (CSPRNG) as described in my 1998 Usenix Security Symposium paper "The
   generation of practically strong random numbers".

   The CSPRNG code is copyright Peter Gutmann (and various others) 1995-2002
   all rights reserved.  Redistribution of the CSPRNG modules and use in
   source and binary forms, with or without modification, are permitted
   provided that the following conditions are met:

   1. Redistributions of source code must retain the above copyright notice
          and this permission notice in its entirety.

   2. Redistributions in binary form must reproduce the copyright notice in
        the documentation and/or other materials provided with the distribution.

   3. A copy of any bugfixes or enhancements made must be provided to the
          author, <pgut001@cs.auckland.ac.nz> to allow them to be added to the
          baseline version of the code.

   ALTERNATIVELY, the code may be distributed under the terms of the GNU
   General Public License, version 2 or any later version published by the
   Free Software Foundation, in which case the provisions of the GNU GPL are
   required INSTEAD OF the above restrictions.

   Although not required under the terms of the GPL, it would still be nice
   if you could make any changes available to the author to allow a
   consistent code base to be maintained */
```

2: Fault Management for A00009235

2.1 Fault management strategy

The TLS security feature for the SIP Gateway application on the CS2000 Session Server includes new logs and alarms to be defined. This section details the logs and alarms that the TLS security feature has defined.

An alarm monitoring process will be used to compare thresholds values with current operating conditions. As alarmable conditions occur, the process will ensure that the appropriate alarm is raised.

2.2 Fault management tools and utilities

This feature utilizes the current log and alarm display mechanisms in use by the SS-Trunks. There will be new alarms and logs defined, but there will not be any new display mechanisms. Refer the to documented activity (in pls fmdoc) A00003933 (Succession Communication Server (SCS) 2000 - Session Server Manager 2000 - SIP Gateway application) for the overall log and alarm tools and utilities.

This feature generates logs and alarms under the purview of the SIP Gateway application Call Processing. These logs and alarms are only generated and reported on the SIP Gateway application.

They can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server Manager - SIP Gateway application web page. The body of log formats shown in this document are the format for the Session Server logs if viewed from the IEMS (Integrated Element Manager System). Log formats may differ if logs are viewed from the Session Server Web Interface. The content will not differ, just the format and/or the headers.

References to TLS-based logs and alarms not found in this document will be found in the documentation to feature A00006893 in PLS FMDOC.

2.3 Logs

All logs and associated alarms will have the name start with SIPS (for SIP Security).

The following new logs have been created/modified:

- SIPS608 - TLS Certificate Policy failure (new).
- SIPS609 - Security Parameter Changed (new).
- SIPS604 - TLS Initialization Logs (changed).

The following new alarm related logs have been created/modified:

- SIPS303 - Certificate Mismatch in Server Certificate
- SIPS305 - TLS Initialization Failure (changed from previous release)
- SIPS308 - Failed Certificate Policy Check

2.3.1 SIPS608 - TLS Certificate Policy failure log

2.3.1.1 Formats

2.3.1.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS608 <Severity> <Type> TLS ^M Certificate Policy failure, <IP Address>:<Port>^M

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <Severity>: The Severity of the log (MINOR).
- <Type>: The type of log (INFO)
- <DeviceName>: The name assigned to the Session Server
- <IP Address> : The IP address of the remote side of the connection
- <Port> : The port number of the connection

Example:

```
 Mar 2 09:53:57 NGSS sipgwyappln: SIPS608 MINOR INFO TLS Certificate Policy
failure, 172.16.172.104:55263
```

2.3.1.2 Explanation

The SIPS608 log is generated when the remote side of the connection presents a certificate that does not conform to the selected local certificate policy.

2.3.1.3 Field descriptions

Table 2: Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	MINOR	Severity level of the log
<Type>	INFO	informational or initialization log.
<IP Address>	<a>.<b>.<c>.<d>	IP address of remote side of connection
<Port>	<xxx>	The Port number of the connection

2.3.1.4 Action

There are two courses of action. The first would be to remove the certificate policy that is preventing the certificate from the Security Parameters Configuration Web Page on the SS-Trunks. The second course of action (and the preferred one) would be to enforce the local certificate policy throughout the network (forcing the Remote SIP Server to present a certificate that conforms to the certificate policy).

See “Certificate Policy Check Failure Alarm” on page 1217 for more details.

2.3.1.5 Associated Operational Measurements or Performance Measurements

None for this log.

2.3.1.6 Additional information

None.

2.3.2 SIPS609 - TLS Security Parameter Changed log

2.3.2.1 Formats

2.3.2.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS609 <Severity> <Type> TLS ^M Security Parameter <SecParmName> updates^M OLD: <OldText>^M NEW: <NewText>

Following are values/explanations of the variable values presented above:

<Date>: Current date

<Time>: Current time

<DeviceName>: The name assigned to the Session Server

<Severity>: The Severity of the log (NONE).

<Type>: The type of log (“TLS”)

<process>: process class that raised the log (either sipgwyappln: or certClass:)

<Unit#>: The unit number assigned (either 0 or 1)

<SecParmName>: One of:

- "MaxTLSSessions",
- "localTLSport",
- "numOfTLSEngines",
- "SessionCachingEnabled",
- "SessionCacheValidDuration",
- "SessionCacheSize",
- "SelfSignedCertificatesAllowed",
- "TLSAllowedCipherSuites",
- "TLSServerCertPath",
- "TLSServerKeyPath",
- "TLSTrustedCertsPath",
- "ThrottleEnabled",
- "ThrottleBurstDurationinSecs",
- "ThrottleSustainedDurationinSecs",
- "ThrottleBurstEventThreshold",
- "ThrottleSustainedEventThreshold",
- "TlsEnabled",
- "ExitOnFailTLSInitialization",

- "RequireLocalCertificatePolicy",
- "RequirekeyUsage",
- "RequireauthorityKeyIdentifier",
- "RequiresubjectKeyIdentifier",
- "RequireprivateKeyUsagePeriod",
- "RequiresubjectAltName",
- "RequireissuerAltName",
- "RequirebasicConstraints",
- "RequireextKeyUsage",
- "AlarmMinimumDisplayTimeMinutes",
- "AlarmThresholdDroppedConnections",
- "AlarmThresholdAuthenticationFailure",
- "AlarmThresholdCertExpiryDays",
- "AlarmThresholdLocalCertificatePolicy"

<OldText>: One of

- For the non-AlarmThreshold logs: “<value>”, where:
  - <value>: the old value of the entry
- For the AlarmThreshold logs: “Minor = <min>, Major = <maj>, Critical = <crit>”, where:
  - <min>: the old minor threshold value
  - <maj>: the old major threshold value
  - <crit>: the old critical threshold value

<NewText>: One of

- For the non-AlarmThreshold logs: “<value>”, where:
  - <value>: the new value of the entry
- For the AlarmThreshold logs: “Minor = <min>, Major = <maj>, Critical = <crit>”, where:
  - <min>: the new minor threshold value
  - <maj>: the new major threshold value
  - <crit>: the new critical threshold value

Example:

```
Mar 11 12:31:12 NGSS sipgwyappln: SIPS609 NONE      TLS Security Parameter
AlarmThresholdAuthenticationFailure updated OLD: Minor = 2, Major = 4, Critical =
6 NEW: Minor = 2, Major = 4, Critical = 5
```

```
Mar 11 12:31:37 NGSS sipgwyappln: SIPS609 NONE      TLS Security Parameter
ExitOnFailTLSInitialization updated OLD: 1 NEW: 0
```

2.3.2.2 Explanation

The SIPS609 logs are generated whenever a TLS Security Parameter is changed by the user.

2.3.2.3 Field descriptions

Table 3: Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	CRIT	Severity level of the log
<Type>	“ “	Informational log
<SecParmName>	<SecParmName>	Name of the parameter as seen from the Security Parameters Configuration web page.
<OldText>	<OldText>	The text representation of the old value of the parameter(s)
<NewText>	<NewText>	The text representation of the new value of the parameter(s)

2.3.2.4 Action

None. Informational log only.

2.3.2.5 Associated Operational Measurements or Performance Measurements

None.

2.3.2.6 Additional information

None.

2.3.3 SIPS604: Certificate Information Logs

These logs were originally implemented in SN08. The Certificate Effective Date log is the new content being documented here. Everything else remains the same as in SN08.

2.3.3.1 Formats

2.3.3.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS604 <Severity> <Type> TLS <Log Message>

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <Severity>: The Severity of the log (NONE).
- <Type>: The type of log (INFO)
- <Log Message>: one of:
  - — none/info: "^M Local Certificate Effective: Year=<YYYY>, Month = <MM>, Day = <DD>^M"
  - — none/info: "^M Local Certificate Expires: Year=<YYYY>, Month = <MM>, Day = <DD>^M"

Examples:

```
Oct  8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS604 NONE INFO TLS ^M    Local
Certificate Effective: Year=2004, Month = 10, Day = 8^M

Oct  8 15:17:07 comit.ngss.unit1 sipgwyappln: SIPS604 NONE INFO TLS ^M    Local
Certificate Expires: Year=2005, Month = 10, Day = 8^M
```

2.3.3.2 Explanation

The SIPS604 log is generated twice during the initialization of the Call Processing application (i.e. during the unlock). These logs indicates when the current local certificate will become effective, and when it will expire.

2.3.3.3 Field descriptions

Table 4: Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.

Table 4: Field descriptions

Field	Value	Description
<Severity>	NONE	Severity level of the log
<Type>	INFO	informational.
<Log Message>	see bulleted list	Log message text.

2.3.3.4 Action

On an info log, no immediate action is required.

2.3.3.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

2.3.3.6 Additional information

None.

2.3.4 SIPS303 - TLS Certificate Mismatch alarm log

2.3.4.1 Formats

2.3.4.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS303 <Severity> <Type> TLS ^M Certificate Mismatch in Server Certificate NCGL=<DeviceName>;Unit=<UnitNumber>;SIPS = Certificate Mismatch in Server Certificate ^M

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <Severity>: The Severity of the log (CRITICAL).
- <Type>: The type of log (INFO)
- <DeviceName>: The name assigned to the Session Server
- <UnitNumber>: The node {0 or 1} where the alarm was generated.

Example:

```
Apr  7 16:38:21 yang alarmd: SIPS303 CRIT TBL  Certificate Mismatch in Server
Certificate NCGL=yang;Unit=0;SIPS = Certificate Mismatch in Server Certificate
```

2.3.4.2 Explanation

Every minute, the SS-Trunks compares the data in the certificate and key files on the active side, to those on the inactive side. The SIPS303 log is generated if the two sets of files do not match each other. An alarm is also raised.

If the two files do not match each other, a number of consequences may occur, depending on the nature of the changes made to the files.

Effects may include:

- Inability to use the EM Web Server after the next swact or reboot.
- Inability to run TLS-based calls after the next swact or reboot.
- Dropping of all TLS-based calls after the next swact.

Needless to say, this is a log/alarm that should be acted on immediately. See the "Action" section below for more details.

2.3.4.3 Field descriptions

Table 5: Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	CRITICAL	Severity level of the log
<UnitNumber>	0 or 1	which one of the two units generated the log.
<Type>	INFO	informational or initialization log.

2.3.4.4 Action

The proper certificate and key files must be restored to their place on both the active and inactive nodes. Check to ensure that the Certificate and Key provided to the call processing application are in the correct directory (as pointed to by the Database entry). It may be that the database entry is incorrect or corrupt.

The location of the files for the certificate and key are specified by the values stored in the database.

Root access to the SS-Trunks is normally required to correct this condition. This is because the server.key file is readable and writeable only by root.

Obtain the backup copies of these files made during install or upgrade, or during certificate replacement. Install them on *both* nodes using the cert_mgnt tool. Details on the backup/restore using cert_mgnt or other means can be found in the CN for this feature or the SS-Trunks install/upgrade NTP NN10346-611.

If the backup copies are not immediately available, it may be possible to copy the files from one node to the other. The sipgwyappln application must be running in a normal state on the node with the complete fileset for this to happen. Details on copying files between nodes can be found in the CN for this feature or the NTP quoted above.

In the worst case, if no backup copies exist, the user may wish to create or import an entirely new set of certificate and key files. Be warned: creating new self-signed certificates will likely require datafilling of the certificate on every peer SIP server in the network. And it will require the user to restart CallP on both nodes during a maintenance window.

The user will want to determine who has damaged or removed these files, because this may be the result of a security breach in the user's network.

The SS-Trunks produces CRT700 and CRT701 customer logs that are produced when the system cert_mgnt tool creates these files; look for these logs to determine if someone has made recent changes.

The user will want to ensure that the certificate and key files are meant to be together (by running the cert_mgnt tool).

2.3.4.5 Associated Operational Measurements or Performance Measurements

None for this log.

2.3.4.6 Additional information

None.

2.3.5 SIPS305 - TLS Engine failure log

These logs are output by TLS when it fails to initialize, and by the TLS alarm code when an alarm is raised to flag TLS initialization failure.

2.3.5.1 Formats

2.3.5.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS305 <Severity> <Type> NCGL=<DeviceName>;Unit=<UnitNumber> TLS <Log Message>

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <DeviceName>: The name assigned to the Session Server
- <Severity>: The Severity of the log (CRIT).
- <Type>: The type of log (INIT)
- <UnitNumber>: The number {0,1} of the SS-Trunks.
- <Log Message>:
  - crit/init: “^M TLS Local Key and Cert do not match^M”
  - crit/init: “^M TLS Failed client init^M”
  - crit/init: “^M TLS Failed Server init^M”
  - crit/init: “^M TLS Failed to load Certificate^M”
  - crit/init: “^M TLS Failed to load Key^M”
  - crit/init: “^M TLS Failed to Init^M”
  - crit/init: “^M TLS Failed to get pointer^M”
  - crit/init: “^M TLS Failed to create thread^M”
  - crit/init: “^M TLS Failed Local Certificate Policy^M”
  - crit/init: “^M TLS is Not Enabled NCGL=<DeviceName>;Unit=<UnitNumber> TLS is Not Enabled^M” where <UnitNumber> is the number of the unit where the alarm was generated.

Examples:

```
Mar  1 10:06:53 NGSS sipgwyappln: SIPS305 CRIT INIT TLS ^M    TLS Failed Local
Certificate Policy^M
Mar  1 10:06:53 NGSS alarmd: SIPS305 CRIT TBL  TLS is Not Enabled
NCGL=NGSS;Unit=0;SIPS TLS is Not Enabled
```

2.3.5.2 Explanation

The SIPS305 log is generated during the initialization of the Call Processing application (i.e. during the unlock). If one of the critical logs come out, it means that there is a problem with the initialization, and the application is unable to start.

2.3.5.3 Field descriptions

Table 6: Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	CRIT	Severity level of the log
<Type>	INIT or TBL	initialization log / trouble log.
<UnitNumber>	0 or 1	which one of the two units generated the log.
<Log Message>	see bulleted list	Log message text.

2.3.5.4 Action

On a critical severity log, check to ensure that the Certificate and Key provided to the call processing application are in the correct directory (as pointed to by the Database entry). Then ensure that the Certificate and Key files themselves are not corrupted or tampered with. Ensure that the certificate and key files are meant to be together (by running the cert_mgnt tool). See “SIPS604: Certificate Information Logs” on page 1205 for more information.

Alternatively contact the next level of support.

Once the problem is resolved, and the user ‘unlocks’ the application again, there will be 3 logs indicating resolution.

- SIPM500

```
Feb  9 13:15:40 comit.ngss.unit1 sipgwymtc: SIPM500 NONE INFO SIP Gateway
Application Maintenance State Change ^M       [Administrative : Locked        ->
Unlocked      ]^M       [Operational    : Enabled        -> Enabled       ]^M
[Control        : Not Suspended   -> Not Suspended  ]^M        [Procedural     :
Not Terminating -> Not Terminating]^M     [User Requested : Yes]^M     [Reason
: Unlock command issued]^M        [Web User ID    : mtc]^M
```

- SIPS605
- SIPS604 (2 of them: one for certificate effective date; one for certificate expiry date)

2.3.5.5 Associated Operational Measurements or Performance Measurements

Not applicable to this log.

2.3.5.6 Additional information

Normally, the cert_mgnt CLI will provision the certificate and key files properly. If this interface has not been run prior to the attempt to bring the call processing application in service, or has been run improperly, unexpected results could occur. Extra information as to the cause of the problem will likely reside in the initialization trace logs provided in the /opt/apps/logs directory (look for siptrace.<date>.server.<pid>).

2.3.6 SIPS308 - Failed Certificate Policy Check Alarm Log

2.3.6.1 Formats

2.3.6.1.1 Syslog

Following is the format of the log:

<Date> <Time> <DeviceName> sipgwyappln: SIPS308 <Severity> <Type> ^M TLS Local Certificate Policy Mismatch NGSS=NCGL;Unit=<UnitNumber>;SIPS Failed <count> certificate policy checks.^M

Following are values/explanations of the variable values presented above:

- <Date>: Current date
- <Time>: Current time
- <Severity>: The Severity of the log.
- <Type>: The type of log (INFO)
- <DeviceName>: The name assigned to the Session Server
- <UnitNumber>: The number {0,1} of the SS-Trunks.
- <count>: The number of certificate policy checks that have failed.

Example:

```
Mar  2 14:44:46 NGSS alarmd: SIPS308 MINOR TBL  TLS Local Certificate Policy
Mismatch NCGL=NGSS;Unit=0;SIPS Failed 1 certificate policy checks
```

2.3.6.2 Explanation

The SIPS308 log is generated when enough certificate policy failures have occurred to generate an alarm. See 2.4.3 “Certificate Policy Check Failure Alarm” on page 1217 for more information.

2.3.6.3 Field descriptions

Table 7: Field descriptions

Field	Value	Description
<DATE>	<Mon> <DD>	Current date when the log occurred.
<Time>	<HH>:<MM>:<SS>	Current time when the log occurred.
<DeviceName>		Name of the session server.
<Severity>	MINOR	Severity level of the log
<UnitNumber>	0 or 1	which one of the two units generated the log.
<Type>	INFO	informational or initialization log.

2.3.6.4 Action

There are two courses of action. The first would be to remove the certificate policy that is preventing the certificate from the Security Parameters Configuration Web Page on the SS-Trunks.

The second course of action (and the preferred one) would be to enforce the local certificate policy throughout the network (forcing the Remote SIP Server to present a certificate that conforms to the certificate policy).

2.3.6.5 Associated Operational Measurements or Performance Measurements

None for this log.

2.3.6.6 Additional information

None.

2.4 Alarms

The following list of alarms has been created or changed for this feature:

- Fail to construct TLS client or server engine (changed).
- Certificate mistmatch between active/inactive host (new).
- Failed Certificate Policy Check (new).

The following alarms have not changed in SN09, but now have provisionable alarm thresholds. Consult this feature's CN document for more details.

- Connection Requests Dropped Alarm.
- Connection Handshake Failure Alarm.
- TLS Local Certificate Expiration Alarm.

2.4.1 Certificate Mismatch Alarm

Many of the details on this alarm and the appropriate response are documented in section 2.3.4 “SIPS303 - TLS Certificate Mismatch alarm log” on page 1207.

2.4.1.1 Integrated Element Manager GUI Fields

Table 8: IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE, or CRIT
Category	*Certificate Mismatch*
LogName	SIPS
LogNumber	303
EventType	TBL
EventLabel	TBL
ProbableCause	*versionMismatch*
SpecificProblem	TLS Certificate Mismatch
BodyText	Certificate Mismatch in Server Certificate

The original alarm log is not refreshed.

2.4.1.2 Explanation

Description: The SIPS303 log is generated whenever the certificate or private key files on the SS-Trunks do not match between the active and inactive nodes .

Severity: Critical. A certificate mismatch means that a SWACT could lead to the dropping of TLS calls, or that TLS CallP may not be active on the next reboot. It may also mean that the EM web server is inoperative, or will become inoperative on the next SWACT or node reboot. See 2.3.4.2 “Explanation” on page 1208 for more information.

2.4.1.3 Action

See 2.3.4.4 “Action” on page 1208 for detailed instructions on how to respond.

2.4.1.4 Corresponding Clear Log

Log Title: SIPS303 with severity NONE.

2.4.2 TLS Engine Failure Alarm

This alarm has been changed in SN09; it was first implemented in SN08. Please reference feature documentation for A00006893 for details on the SN08 implementation.

2.4.2.1 Integrated Element Manager GUI Fields

Table 9: IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE or CRIT
Category	*TLS Engine Failure*
LogName	SIPS
LogNumber	305
EventType	TBL
EventLabel	TBL
ProbableCause	*fileError*
SpecificProblem	TLS has failed to initialize properly, and needs to be restarted.
BodyText	TLS is Not Enabled

2.4.2.2 Explanation

The TLS Engine has failed to initialize when SS-Trunks CallP started. This may or may not have resulted in the termination of CallP on the SS-Trunks.

The SIPS305 customer log is generated during the alarming of TLS Engine failure. This log will inform the user of the exact reason that the TLS engine failed to start.

This alarm will only occur when the exitOnFailTLSinitialization security parameter is set to ‘N’. We recommend that exitOnFailTLSinitialization always be set to ‘Y’, and ‘Y’ is the default value.

2.4.2.3 Action

It is recommended that exitOnFailTLSinitialization be set to ‘Y’. After that parameter is set to ‘Y’, this alarm will not occur in future cases of TLS initialization failure. Instead, the CallP application will not run if TLS cannot initialize properly.

The text of the associated SIPS305 customer log dictates the action.

The following error messages may be output in the SIPS305 customer log:

1. "TLS Failed to load Key"
2. "TLS Failed to load Certificate"
3. "TLS Failed Server init"
4. "TLS Local Key and Cert do not match"
5. "TLS Failed client init"
6. "TLS Failed to create thread"
7. "TLS Failed to get pointer"
8. "TLS Failed to Init"
9. "TLS Failed Local Certificate Policy"

The appropriate actions for these messages are as follows:

For messages 1, 2, and 4:

a. Check for the existence and validity of the certificate and key files. Restore these from backup if necessary. See 2.3.4.4 "Action" on page 1208 for a detailed method of validating these files.

b. If CallP is running, and the exitOnFailTLSinitialization security parameter is set to 'N', then: Change the value of parameter TlsEnabled to "Y" on the SecurityParmConfig EM web page. This will attempt a restart of TLS.

c. Else: Manually suspend/lock (if required) and unsuspend/unlock CallP from the Maintenance EM web page.

d. If the alarm is not cleared after this, contact Nortel Technical Support.

For messages 3, 5, 6, 7, and 8:

a. If CallP is running, and the exitOnFailTLSinitialization security parameter is set to 'N', then: Change the value of parameter TlsEnabled to "Y" on the SecurityParmConfig EM web page. This will attempt a restart of TLS.

b. Else: Manually suspend/lock (if required) and unsuspend/unlock CallP from the Maintenance EM web page.

c. If the alarm is not cleared after this, contact Nortel Technical Support.

For message 9, there are two alternatives:

a. Set the "RequireLocalCertificatePolicy" parameter on the SecurityConfigParms EM web page to "N". This is a stopgap measure that will allow TLS to come up even if the certificate defies the local certificate policy.

i. If CallP is running, and the exitOnFailTLSinitialization security parameter is set to 'N', then: Change the value of parameter TlsEnabled to "Y" on the SecurityParmConfig EM web page. This will attempt a restart of TLS.

ii. Else: Manually suspend/lock (if required) and unsuspend/unlock CallP from the Maintenance EM web page.

b. Provision a new certificate that follows the established security policy. This is usually the preferred option, but may take a significant amount of time to accomplish, depending on the Public Key Infrastructure policy of the customer.

i. If the customer allows self-signed certificates, a new self-signed certificate may be provisioned on this SS-Trunks using the cert_mgnt tool. However, this new self-signed certificate will have to be provisioned as a trusted certificate on all the SS-Trunks's peer SIP servers.

ii. If CallP is not running: Manually suspend/lock and unsuspend/unlock CallP from the Maintenance EM web page.

iii. If CallP is running: Change the value of parameter TlsEnabled to "Y" on the SecurityParmConfig EM web page. This will attempt a restart of TLS.

c. If steps a and/or b do not work, contact Nortel Technical Support

2.4.2.4 Corresponding Clear Log

Log Title: SIPS305 with severity NONE.

2.4.3 Certificate Policy Check Failure Alarm

2.4.3.1 Integrated Element Manager GUI Fields

Table 10: IEMS Alarm GUI Field descriptions

Field	Value
Severity	NONE, MINOR, MAJOR, or CRIT
Category	*Certificate Policy Check Failure*
LogName	SIPS
LogNumber	308
EventType	TBL
EventLabel	TBL
ProbableCause	*thresholdCrossed*

Table 10: IEMS Alarm GUI Field descriptions

Field	Value
SpecificProblem	A number of certificates violating the provisioned certificate policy on the SS-Trunks have been submitted by peer SIP servers.
BodyText	Failed <certificate_count> certificate policy checks <updatetext>

BodyText explanation: The BodyText entry for the log will contain “Failed <number> certificate policy checks”. However, over time, other events may occur, and the alarm BodyText will be updated with “Failed <number> certificate policy checks in the last minute<updatetext>”, where <updatetext> is one of:

- “, <numberminor> Minor events since alarm creation” for Minor alarms
- “, <numbermajor> Major, <numberminor> Minor events since alarm creation” for Major alarms or
- “, <numbercritical> Critical, <numbermajor> Major, <numberminor> Minor events since alarm creation” for Critical alarms.

The original alarm log is not refreshed.

2.4.3.2 Explanation

The customer has the option of setting requirements on TLS certificates submitted by other servers, using certain parameters provisionable on the SecurityParmsConfig web page on the EM.

If certificates are submitted by remote SIP servers that violate the policy set by the customer, the remote servers’ certificates will be rejected, and calls from that server will not be allowed.

If a certain number of remote servers’ certificates are failed, an alarm is generated. The number of failures that trigger an alarm is provisionable via the AlarmThresholdLocalCertificatePolicy parameter on the SecurityParmsConfig web page.

The default provisioned values for this alarm are minor=1, major=2, critical=5.

The log/alarm will be raised at least 30 minutes, and if the problem has ceased, the clear alarm log will be generated.

2.4.3.3 Action

The customer has two options here:

1. Disable the certificate policy restrictions set on the SecurityParmsConfig web page. The policy restrictions can be turned off by setting the RequireLocalCertificatePolicy parameter to 'N'.
   a. This option is intended as a stopgap, so that the customer can permit calls from offending servers while new certificates are issued to those servers.
2. Provision new certificates on the offending servers, that meet the customer's certificate policy. If self-signed certificates are used on the offending servers, the certificates will require datafilling on multiple peer SIP servers.
   a. This is the preferred option, but it may take significant time to complete this task.

2.4.3.4 Corresponding Clear Log

Log Title: SIPS308 with severity NONE.

2.5 Related documentation

NTP NN10346-611.

A00006893 FM section.

A00009235 CN section.

3: Configuration for A00009235

3.1 Hardware and Software Requirements

Nothing required outside of the normal SN09 software load on the appropriate hardware platform.

3.2 Initial Configuration

SN09

3.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

3.4 Upgrade Considerations

If a Session Server is to be placed in a Packet Cable environment, extra steps will be required after the upgrade is complete.

From 07 to 09 upgrade in the case of CA-signed certificate, the customer must execute the procedure "Prepare to validate" which is run on the 07 in order to ensure that cert_mgnt in 09 will be successful if the customer is importing a CA-signed certificate from 07 to 09. This is documented in the NTP. If the certificates are nearing expiry during the upgrade or shortly after the upgrade,

the customer is recommended to replace the certificates prior to upgrade in order to avoid downtime once the system is running the 09 load.

From 07 to 09 upgrade in the case of self-signed certificates, the customer will have to generate new certificates.

From 08 to 09 upgrade, running cert_mgnt is not required. If the certificates are nearing expiry during the upgrade or shortly after the upgrade, the customer is recommended to replace the certificates prior to upgrade in order to avoid downtime once the system is running the 09 load.

3.4.1 Dump and Restore (CM)

None.

3.4.2 Element Management Upgrade

None.

3.4.3 Downgrade impact

None.

3.5 Data schema (DS) (CM, MIBS, RDB)

Not applicable.

3.6 Service Orders (SO) (CM & SESM)

Not Applicable.

3.7 Software optionality control (SOC)

Not Applicable.

3.8 Element Management

3.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
CS2000 Session Server Tomcat Web Server	Changed

3.8.2 GUI information

3.8.2.1 GUI name: Session Server Tomcat Web Server

This GUI is a CS2000 Session Server-specific management tool.

The changes made to this GUI consist of:

- Additions to the Security configuration parameters web page with new parameters
- Modification of an existing parameter to the security configuration parameters web page.

3.8.2.1.1 Functional description

Changes to the CS2000 Session Server Tomcat Web Server GUI are as follows:

CS2000 Session Server Tomcat Web server security configuration parameters:

Ciphers. This field existed in SN08 and is modified to include new ciphers:

- TLSAllowedCipherSuites

Alarm threshold provisioning. These fields are new:

- AlarmThresholdDroppedConnections - Dropped connections alarm per loop time of 60 seconds
- AlarmThresholdAuthenticationFailure - Certificate Authentication failure alarm - per loop time of 60 seconds
- AlarmThresholdCertExpiryDays - Local certificate expiry alarm in days
- AlarmThresholdLocalCertificatePolicy - remote certificate policy failure alarm per loop time of 60 seconds
- AlarmMinimumDisplayTimeMinutes - Minimum time an alarm should be raised

Secretary options. This field is new:

- ExitOnFailTLSInitialization - Exit application if TLS fails to initialize

Certificate Policy options. These fields are new:

- RequireLocalCertificatePolicy
- RequireauthorityKeyIdentifier
- RequirebasicConstraints
- RequireextKeyUsage
- RequireissuerAltName
- RequirekeyUsage
- RequireprivateKeyUsagePeriod
- RequiresubjectAltName
- RequiresubjectKeyIdentifier

Additions for throttling are:

- ThrottleBurstDurationinSecs

- ThrottleBurstEventThreshold
- ThrottleEnabled
- ThrottleSustainedDurationinSecs
- ThrottleSustainedEventThreshold

Other parameters that are new in SN09 are:

- TlsEnabled

Other parameters that are changed from SN08 to SN09:

- MaxTLSSessions
- SessionCachingEnabled
- SessionCacheSize
- SessionCacheValidDuration

3.8.2.1.2 GUI usage and implications

The purpose of the new configuration parameters is to provide new functionality as well as increased robustness to the security component of the CS2000 Session Server.

3.8.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
GUI			Not applicable

3.8.2.1.4 GUI fields

The following table lists fields for the CS2000 Session Server Tomcat Web server Security Parameters GUI that have been added or changed.

Table 3 Security Parameters in Tomcat Web Server

Parameter	AlarmThresholdDroppedConnections	Type	Integer
Description	Number of dropped connections - Minor/Major/Critical alarm threshold value within 60 seconds. Related to SIPS600 log and applies to SIPS300 alarm. Note: 0 < Minor threshold < Major Threshold < Critical Threshold < 32767 The value is applied immediately.	Default Value	Minor - 10 Major - 50 Critical - 100
Effect of Change	Changes the threshold for activating alarm for dropped connections in CS2000 Session Server	New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**AlarmThresholdAuthenticationFailure**	Type	Integer
Description	Number of certificate authentication failures - Minor Threshold. Related to SIPS 601 log and applies to SIPS301 alarm. Note: 0 < Minor threshold < Major Threshold < Critical Threshold < 32767 The value is applied immediately.	Default Value	Minor - 1 Major - 2 Critical - 5
Effect of Change	Changes the threshold for activating alarm for certificate authentication failures in CS2000 Session Server	New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**AlarmThresholdCertExpiryDays**	Type	Integer
Description	Number of days until the local certificate expires. Applies to the SIPS302 alarm. Note: Modifying/replacing the local certificate requires a restart of the web services and the SIP application. Note: The SIPS604 log indicates the time and date from when and until when the local certificate is active. Note: This alarm remains raised until the event is no longer observed. Note: 32767 > Critical threshold > Major Threshold > Minor Threshold > 0 The value is applied immediately.	Default Value	Minor - 31 days Major - 15 days Critical - 5 days
Effect of Change	Changes the threshold for activating alarm for local certificate expiry in CS2000 Session Server	New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**AlarmThresholdLocalCertificatePolicy**	Type	Integer
Description	Number of certificate policy violations in 60 seconds. Related to the SIPS608 log and applies to the SIPS308 alarm. Note: 0 < Minor threshold < Major Threshold < Critical Threshold < 32767 The value is applied immediately.	Default Value	Minor - 1 Major - 2 Critical - 5
Effect of Change	Changes the threshold for activating alarm for certificate policy violations.	New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Parameter	**AlarmMinimumDisplayTimeMinutes**	Type	Integer
Description	The following alarms will remain raised when the event persists. This value indicates the number of minutes that the following alarms should remain raised when the event is no longer continuously observed. AlarmThresholdLocalCertificatePolicy AlarmThresholdAuthenticationFailure AlarmThresholdDroppedConnections The value is applied immediately.	Default Value	60 minutes Minimum value: 1 minute Maximum value: 32767 minutes
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ExitOnFailTLSInitialization**	Type	Boolean
Description	1) If the key file or certificate file is not present or corrupted, or 2) if the system is running out of memory and having trouble initializing TLS or 3) the certificate does not match the local policy, or 4) the key/certificate do not match, then this value indicates whether to exit the application or continue with the application initialization and attempt to service calls while the issue is resolved. Default is to exit the application because it may indicate issues with system memory or key/certificate files. Because the same key/certificate files are used to run the EM web servers, the recommended value for this parameters is Y. If the value is changed to 'N' (to allow application initialization), then TlsEnabled can be used to initialize TLS. This value is applied only on application restart.	Default Value	Y Recommended Value: Y
Effect of Change		new or changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireLocalCertificatePolicy**	Type	Boolean
Description	This parameter enables certificate policy checking. For Packet Cable conformance, this must be set to Y. The value is applied immediately.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			
Parameter	**RequireauthorityKeyIdentifier**	Type	Boolean
Description	This value ensures whether the authority key identifier is present in the X.509 version 3 certificate extensions. For Packet Cable conformance, this must be set to Y. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequirebasicConstraints**	Type	Boolean
Description	This value ensures whether the basic constraints is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireextKeyUsage**	Type	Checklist
Description	This value ensures whether the individual key usage settings are present in the X.509 version 3 certificate extensions. Possible values are none of the following, or any combination of the following: serverAuth clientAuth codeSigning emailProtection timeStamping OCSPSigning For Packet Cable conformance, this must be set to (serverAuth and clientAuth). This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	Empty set, See description.
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireissuerAltName**	Type	Boolean
Description	This value ensures whether the issuer alternative name is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequirekeyUsage**	Type	Checklist
Description	This value ensures whether the key usage settings is present in the X.509 version 3 certificate extensions. Possible values are none of the following, or any combination of the following: digitalSignature nonRepudiation keyEncipherment dataEncipherment keyAgreement keyCertSign cRLSign encipherOnly decipherOnly For Packet Cable conformance, this must be set to (digitalSignature and keyEncipherment). This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	Empty Set, see description
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequireprivateKeyUsagePeriod**	Type	Boolean
Description	This value ensures whether the private key usage field is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			
Parameter	**RequiresubjectAltName**	Type	Boolean
Description	This value ensures whether the subject alternative name is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**RequiresubjectKeyIdentifier**	Type	Boolean
Description	This value ensures whether the subject key identifier is present in the X.509 version 3 certificate extensions. This value is applied immediately and requires RequireLocalCertificatePolicy to be set to “Y” to have effect.	Default Value	N
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			
Parameter	**ThrottleBurstDurationinSecs**	Type	Integer
Description	The maximum number of TLS connections represented by ThrottleBurstEventThreshold that can be serviced in ThrottleBurstDurationinSecs seconds. ThrottleBurstDurationinSecs is recommended to be ThrottleSustainedDurationinSecs divided by 5. This value is applied immediately and requires ThrottleEnabled to be set to “Y” to have effect.	Default Value	1 Minimum 1 Maximum 10
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ThrottleBurstEventThreshold**	Type	Integer
Description	The maximum of number of TLS connections that can be serviced in ThrottleBurstDurationinSecs seconds. Recommended value 30 This value is applied immediately and requires ThrottleEnabled to be set to “Y” to have effect.	Default Value	30
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Parameter	**ThrottleEnabled**	Type	Boolean
Description	Enables or disables TLS connection throttling Recommended value Y.	Default Value	Y
Effect of Change		New or Changes	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ThrottleSustainedDurationinSecs**	Type	Integer
Description	The maximum number of TLS connections represented by ThrottleSustainedEvent-Threshold that can be serviced in Throttle-SustainedDurationinSecs seconds. ThrottleSustainedDurationinSecs is recommended to be ThrottleBurstDurationinSecs multiplied by 5. This value is applied immediately and requires ThrottleEnabled to be set to “Y” to have effect.	Default Value	5
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**ThrottleSustainedEventThreshold**	Type	Integer
Description	The maximum of number of TLS connections that can be serviced in ThrottleSustainedDurationinSecsseconds. Recommended value 100 This value is applied immediately and requires ThrottleEnabled to be set to “Y” to have effect.	Default Value	100
Effect of Change		New or Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**TlsEnabled**	Type	Boolean
Description	By default, TlsEnabled is “Y”. If the value is “Y” is cannot be modified. TlsEnabled is “N” in the following case: If ExitOnFailTLSInitialization is set to “N” and TLS fails to initialize. In that case, this boolean can be used to initialize TLS once the issue is resolved.	Default Value	Y
Effect of Change	The value cannot be changed if it is already set to Y. Changing this value from N to Y restarts TLS initialization. The key file and certificate file must be present in order for TLS initialization to be successful. Once successful, look for the SIPS 605 log. If memory allocation for TLS or the SIP application fails, then the SIP application will terminate.	New of Changed	New
Adverse Effects			
Countering Adverse Effects			

Table 3 Security Parameters in Tomcat Web Server

Parameter	**MaxTLSSessions**	Type	Integer
Description	The maximum number of TLS Sessions allowed. The default value is set to 256, maximum of 400.	Default value	Default 256, Minimum 10 Maximum 400.
Effect of Change	This is the maximum number of simultaneous TLS connections on the active unit.	New or Changed	Changed maximum value from SN08 to SN09.
Adverse Effects			
Countering Adverse Effects			

Table 4 Cipher Suites

Parameter	**TLSAllowedCipherSuites**	Type	Checklist
Description	The cryptographic ciphers that are supported in the TLS connection. The value is applied immediately. AES128-SHA is the minimum. Any combination of the following is also allowed: AES256-SHA DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA EDH-RSA-DES-CBC3-SHA DES-CBC3-SHA	Default Value	AES128-SHA at a minimum. See description.
Effect of Change	Selecting ciphers other than AES may cause performance degradation.	New or Changed	Changed from SN08
Adverse Effects			
Countering Adverse Effects			

All ciphers listed here support private key sizes of 1024, 1536, and 2048 bits, RSA authentication, and SHA (Secure Hash Algorith) as the HMAC (hashed message authentication code).

Cipher Name: TLS_RSA_WITH_AES_128_CBC_SHA
Short Name: AES128-SHA
Key Agreement: RSA
RSA/DSA Authentication: RSA
Encryption: AES_CBC, 128 bits

Cipher Name: TLS_RSA_WITH_AES_256_CBC_SHA
Short Name: AES256-SHA
Key Agreement: RSA
Encryption: AES_CBC, 256 bits

Cipher Name: TLS_RSA_WITH_3DES_EDE_CBC_SHA
Short Name: DES-CBC3-SHA
Key Agreement: RSA
RSA/DSA Authentication: RSA
Encryption: 3DES_EDE_CBC, 168 bits

Cipher Name: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
Short Name: DHE-RSA-AES128-SHA
Key Agreement: DHE
RSA/DSA Authentication: RSA
Encryption: AES_CBC, 128 bits
DHE Prime Size: 1024

Cipher Name: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Short Name: DHE-RSA-AES256-SHA
Key Agreement: DHE
RSA/DSA Authentication: RSA
Encryption: AES_CBC, 256 bits
DHE Prime Size: 1024

Cipher Name: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Short Name: EDH-RSA-DES-CBC3-SHA
Key Agreement: DHE
RSA/DSA Authentication: RSA
Encryption: 3DES_EDE_CBC, 168 bits
DHE Prime Size: 1024

Table 5 Session Caching Parameters

Parameter	**SessionCachingEnabled**	Type	Integer
Description	Defines whether session caching is enabled or disabled. Session caching improves performance over TLS connections where traffic is fairly low and over SWACT. It is recommended that all remote servers have TLS session caching functionality enabled. This value now enables or disables client side and server side session caching. Recommended value Y.	Default value	Y
Effect of Change	Turning off session caching does not clear the cache. Items are removed from the server side and client side cache when they are expired. Items may also be removed from the server cache when the server cache is full in order to make room for a new entry.	New or Changed	Changed scope to include client side caching in SN09.
Adverse Effects			
Countering Adverse Effects			

Parameter	**SessionCacheSize**	Type	Integer
Description	Defines the maximum size of the client and server side TLS session cache. Valid values: 10, 100, 1000, 2000, 3200 This recommended value is: (8 x the number of remote sip servers using TLS) <= NEW VALUE. This value should not normally be decreased.	Default value	10
Effect of Change	Increases or decreases the size of the client and server side TLS session cache.	New or Changed	Changed to include new values: 2000, 3200.
Adverse Effects			
Countering Adverse Effects			

Parameter	**SessionCacheValidDuration**	Type	Integer
Description	Defines the length of time a TLS session can be cached. Valid values are 24_Hours, 7_Days, 3_Months. Recommended value: 7_Days	Default value	7_Days
Effect of Change	Changing the values impacts all future TLS sessions, but does not impact entries already in the cache.	New or Changed	Changed to include additional value 3_Months
Adverse Effects			
Countering Adverse Effects			

3.8.2.1.5 Usage example

The following example shows sample datafill or menu selection for the CS2000 Session Server Tomcat Security Parameters Configuration Web Page GUI:

Example:

1. Customer enters the Succession Communication Server 2000 web page.
2. Customer enters the Succession Communication Server 2000 Session Server Manager webpage.
3. Customer clicks on the Provisioning Tab on the Menu Frame
4. Customer clicks on the Security Tab.
5. Customer clicks on the SIP Gateway Tab.
6. Customer clicks on the Security Config Data link, which brings up the Security Configurable Parameters page.
7. All of the parameters listed in See “Security Parameters in Tomcat Web Server” on page 1223. are available.

3.8.2.1.6 GUI release history update

See “Security Parameters in Tomcat Web Server” on page 1223. for parameters that are changed or new in SN09.

3.8.2.1.7 Context sensitive launching information

This GUI is accessed from a series of links starting on the CS2000 Session Server main web page. The normal instructions for launching the CS2000 Session Server Application Web Server can be followed for the new web pages described herein.

3.8.2.1.8 Supplementary information

Not applicable.

3.8.3 CLUI Interface

The Certificate Management Tool has changed slightly from SN08 to SN09.

The tool in its entirety is documented here.

3.8.3.1 Certificate Management Tool (cert_mgnt or cert_mgmt)

The certificate management tool is a customer-visible tool that provides a common interface for provisioning certficates for use by Apache, Tomcat, and the NGSS SIP application.

As of SN08, all three applications use the same certificate.

The certificate management tool is located in /sbin/cert_mgnt or /sbin/cert_mgmt, and is executable only by the root user. Since /sbin is in the path, cert_mgnt can be executed from anywhere.

The certificate management tool provides three functions

- Create a new self-signed certificate for the host
- Create a certificate signing request. The craftsperson would manually send the signing request to the Certificate Authority (CA) where it will be signed.
- Import key and certificate (including CA signed certificate).

The tool makes permissions on private key files and the certificate keystore file to be read/write by the root user.

As described in the SN08 documentation (A00006893), the server.crt contains the local server certificate. The trusted.crt file contains the certificate chain (for CA-signed certificates only) for the local server certificate. Both these files are are read/write by the root user and readable by other users.

Anytime the certificate management tool is run to successful completion, the host must be rebooted, or the three applications that use the certificate must be stopped/ started.

To reboot the host as a root user: at the command prompt: reboot

If rebooting is not appropriate, then stopping/starting each application is necessary.

To stop/start Apache: locate the executable “apachectl” in the directory structure and type: apachectl stop. Once this is successful, type apachectl start

To stop/start Tomcat: local the executable “tomcatd” in the directory structure and type: tomcatd stop. Once this is successful, type tomcatd start.

To stop the NGSS SIP application, the application must be locked and disabled and then enabled and unlocked using the NGSS GUI.

3.8.3.1.1 Certificate Management

Upon installation of the NGSS, the customer can either furnish their own certificates or use the certificate management tool.

If the customer furnishes their own certificates, they will be required to perform their own certificate management.

3.8.3.1.2 Files used by the Certificate Management Tool

The directory /opt/base/share/ssl is the recommended directory to store all certificates, keys, and related files. The cert_mgnt tool performs this automatically.

The tool is run only on 1 host, and the files are not synced/reflected to the other mate host in SN09. Therefore, the files must be manually copied to the other mate host using a secure method such as scp after the tool runs successfully.

server.crt - Only the local server certificate is in this file. In the self-signed certificate option, this file is created automatically by the tool. In the CA-signed option, this file will be provided by the customer, and placed in a temporary directory for import by the tool.

trusted.crt - The certificate chain leading up to the root CA certificate is placed in this file. This file is provided by the customer, and placed in a temporary directory for import by the tool.

server.key - This file contains the private key corresponding to the certificate in server.crt

certificate.keystore - This file contains an encoded version of the server.crt, trusted.crt, and server.key file. This file is created automatically by the tool and is used by Tomcat.

The directory /opt/base/share/ssl should be backed up on a regular basis using a secure method in a physically and logically secure environment. This will help prevent unauthorized access to the private keys.

There are two files (cert_gen.txt and assign_cert.txt) that are placed in the /opt/base/share/ssl directory. These files are used by the tool and should not be removed.

3.8.3.1.3 Certificate and Key revocation

Not applicable.

3.8.3.1.4 Self Signed Certificates

In this case, the craftsperson has chosen to use self-signed certificates.

1. In the case of self-signed certificates, the craftsperson selects option 1 in Figure 1 ”Choose a Certificate Type” on page 1249.
2. In order to proceed, the craftsperson must accept the disclaimer and the notice as indicated in:
   - Figure 2 ”Disclaimer for Self-Signed Certificates (1 of 4)” on page 1250,
   - Figure 3 ”Disclaimer for Self-Signed Certificates (2 of 4)” on page 1250,
   - Figure 4 ”Disclaimer for Self-Signed Certificates (3 of 4)” on page 1251, and
   - Figure 5 ”Disclaimer for Self-Signed Certificates (4 of 4)” on page 1251..

   A customer log is generated logging the user’s acceptance of the disclaimer.

3. Going back at any time will display the previous panel. Selecting proceed will only work if the craftsperson has entered the required information.
4. The craftsperson selects an RSA key size Figure 6 ”Select Key Size” on page 1252. The key size can be 1024/1536/2048 bits. The higher the key size, the stronger the private key. There may be a performance impact to using higher key sizes due to additional encryption requirements.
   - If the key already exists in the /opt/base/share/ssl/ directory, the tool will prompt to reuse it or delete it and recreate a new key.
   - If the craftsperson wishes to reuse the key, the tool will always accept the key’s current size. This is illustrated in Figure 7 ”Key Already Exists” on page 1252
   - If in Figure 7 ”Key Already Exists” on page 1252, the craftsperson select ‘n’ that they do not want to proceed, then the tool prompts for key deletion in Figure 8 ”Remove Existing Key” on page 1253.
   - If in Figure 7 ”Key Already Exists” on page 1252 , the craftsperson select ‘y’ that they do want to proceed, then the tool will reuse the existing key and move on to step 5.
   - If in Figure 8 ”Remove Existing Key” on page 1253, the craftsperson selects ‘n’ that they do want to proceed, the tool will then abort the current operation and return to the top of this step.
   - If in Figure 8 ”Remove Existing Key” on page 1253, the craftsperson selects ‘y’ that they do want to proceed, the tool will then make a backup of the existing key to another file in the same directory. A customer log is generated for this case.

5. The user must also select a length of time for which the certificate is valid. This is specified in Figure 9 ”Expiry Days” on page 1253. This is the number of days from the current date for which the certificate is valid.
6. The craftsperson selects a country, state, and city name in Figure 10 ”Country Name” on page 1254, Figure 11 ”State Name” on page 1254, Figure 12 ”Locality Name” on page 1255. These fields are optional. Although they are optional, they help to identify the NGSS to a remote entity.
7. The craftsperson selects an organizational name, and an organizational unit name in Figure 13 ”Organizational Name” on page 1255, and Figure 14 ”Organizational Unit Name” on page 1256. These fields optional. Although they are optional, they help to identify the NGSS to a remote entity.
8. In Figure 15 ”Common Name” on page 1256, the craftsperson identifies the mandatory common name. In the case of the NGSS, this must be the IP address of the active NGSS host. This is used for mutual authentication and is necessary for the correct operation of the NGSS. There is no validation at this stage of the common name.
9. In Figure 16 ”Email Address” on page 1257, the craftsperson identifies the optional email address of the local contact. There is no validation of the email address.
10. Once all the information is entered, the tool displays a summary in Figure 17 ”Summary for Self Signed Certificates” on page 1257. Selecting “proceed” will generate the self signed certificate. The following message will be displayed on success:

```
Exporting certificate/key pair to PKCS#12 keystore
Certificate/key pair has been successfully exported to PKCS#12 format
Changing permissions on key file
Changing permissions on keystore file
```

11. The user must then secure copy the necessary files from the unit where the cert_mgnt was executed to the mate unit.

For example:

```
cd /opt/base/share/ssl
scp * mtc@<mate host IP>:/users/mtc
```

12. The user log into the mate unit and change directory to the location where the certificate files are located. The user can then use the cert_mgnt tool option 3 to import the certificates and commit the files to /opt/base/share/ssl. This is documented in section 3.8.3.1.6 ”Import Certificates and Private Key” on page 1260.

Figure 1 Choose a Certificate Type

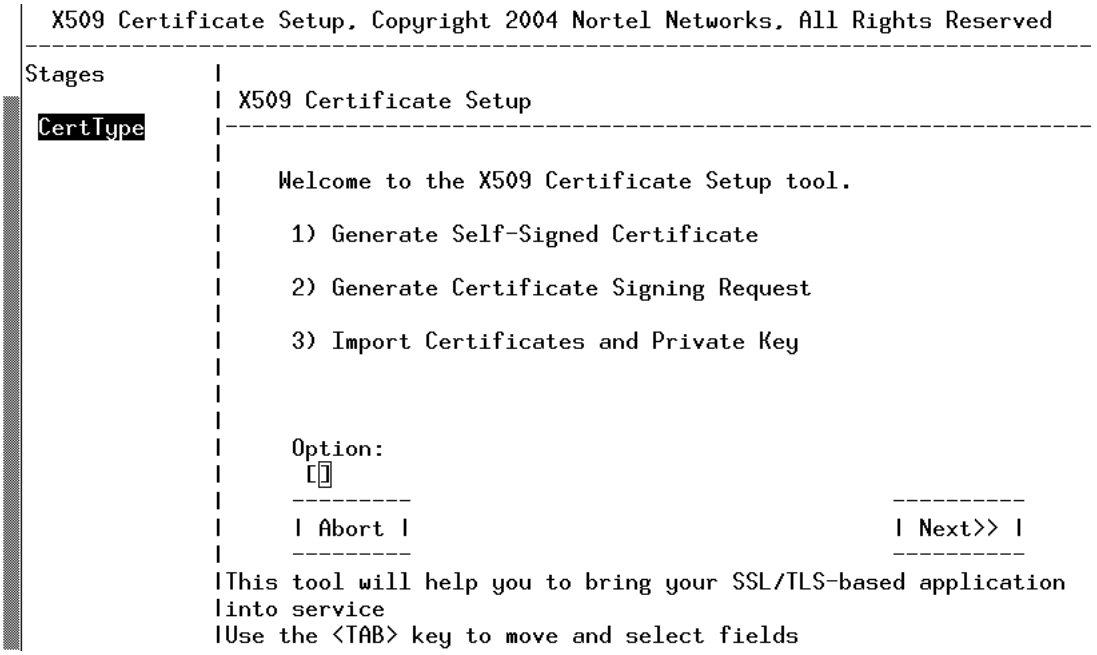


Figure 2 Disclaimer for Self-Signed Certificates (1 of 4)

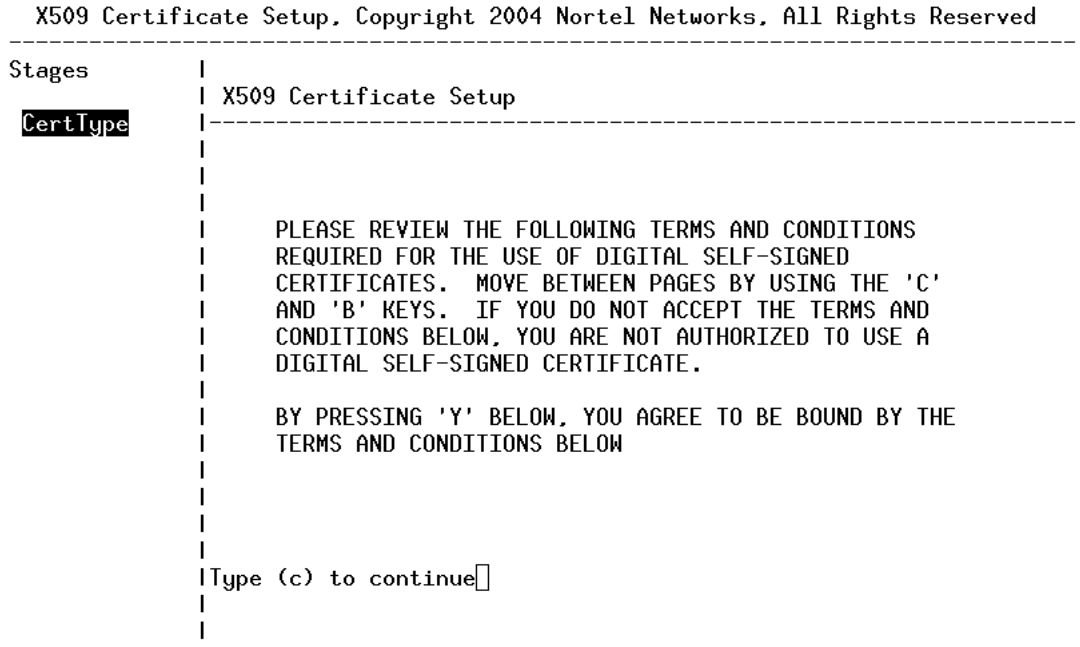


Figure 3 Disclaimer for Self-Signed Certificates (2 of 4)

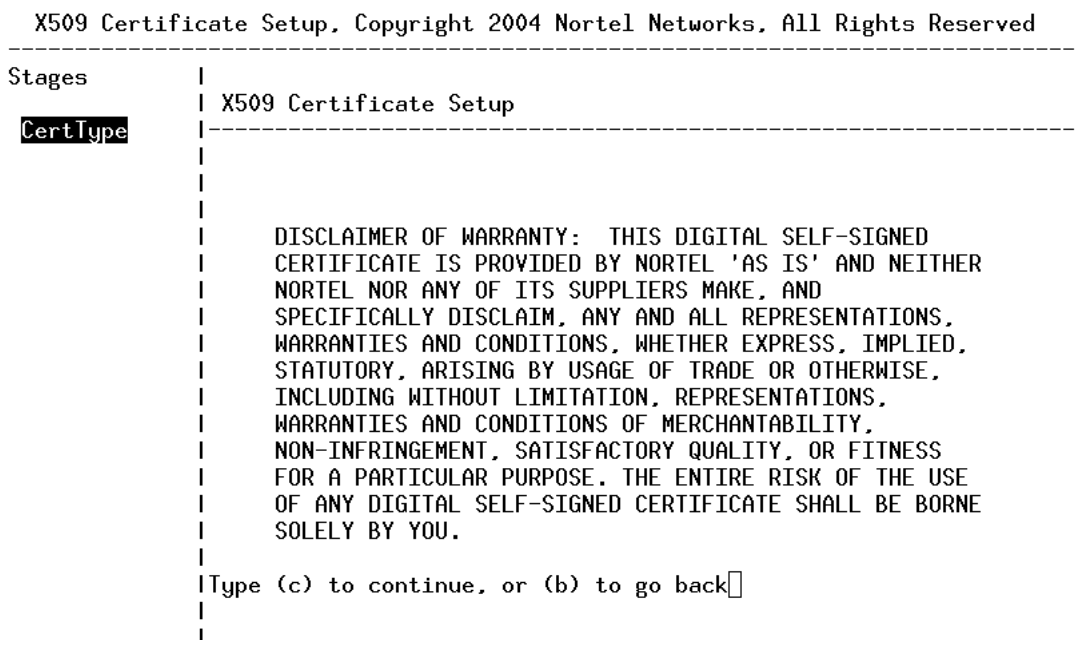


Figure 4 Disclaimer for Self-Signed Certificates (3 of 4)

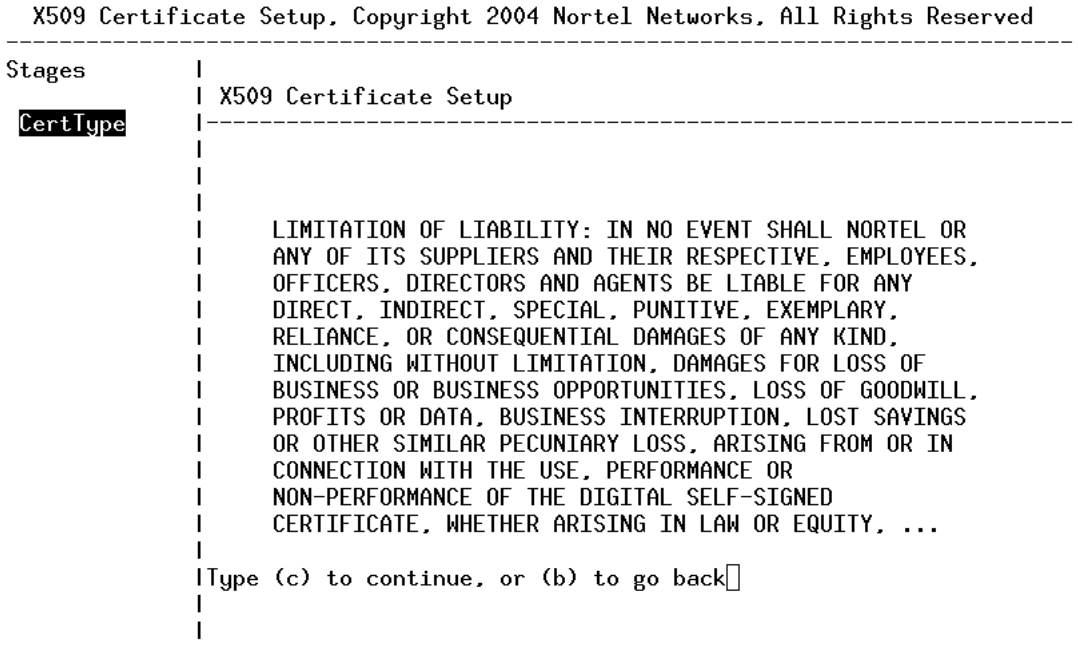


Figure 5 Disclaimer for Self-Signed Certificates (4 of 4)

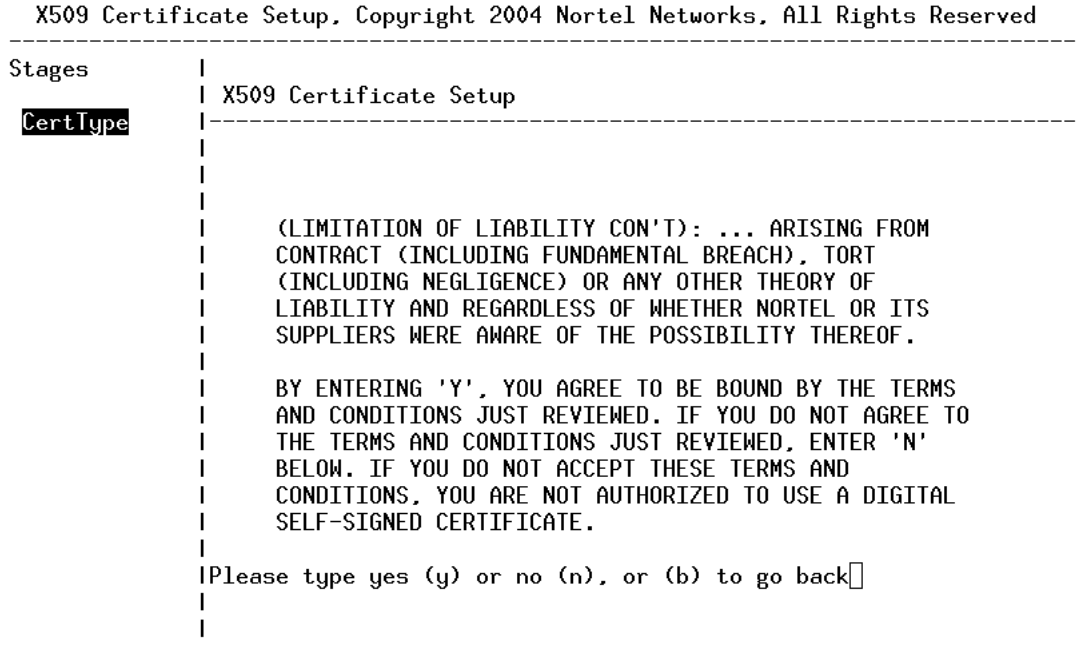


Figure 6 Select Key Size

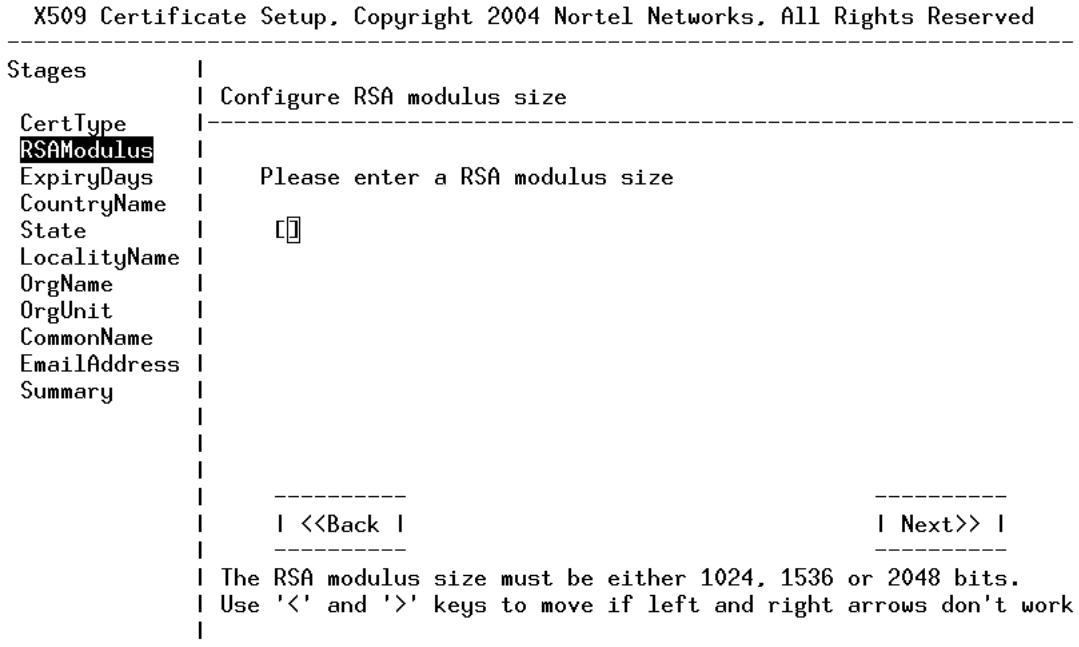


Figure 7 Key Already Exists

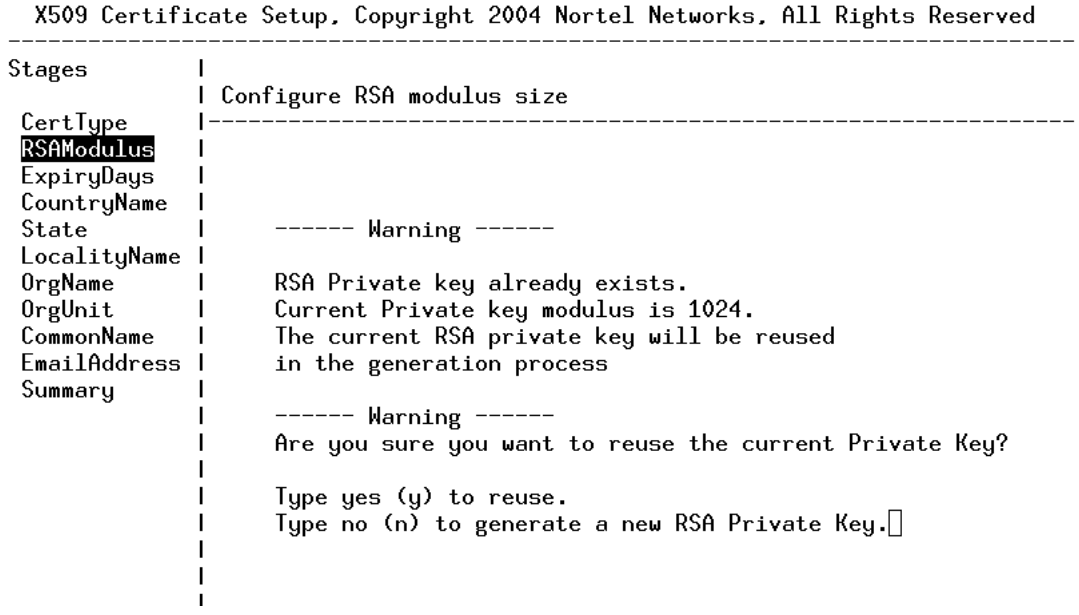


Figure 8 Remove Existing Key

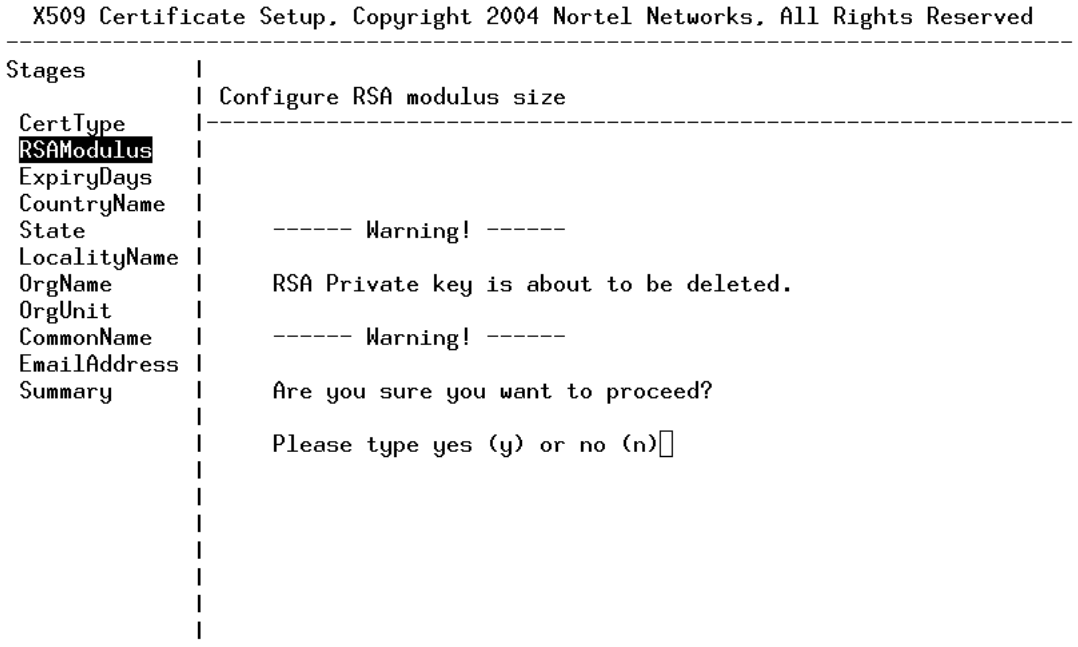


Figure 9 Expiry Days

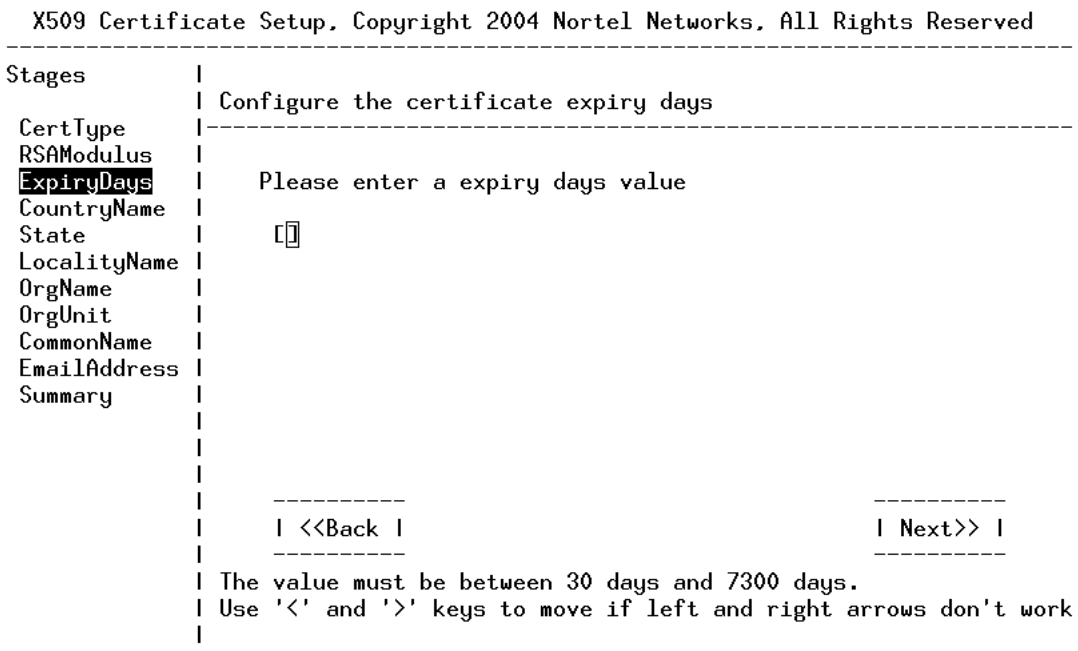


Figure 10 Country Name

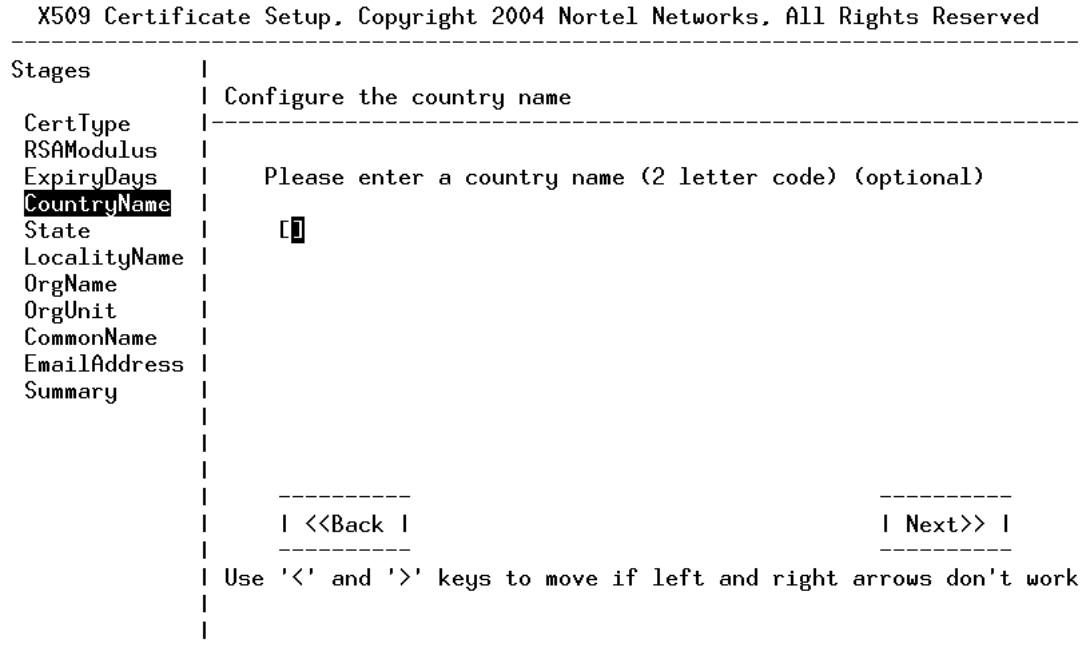


Figure 11 State Name

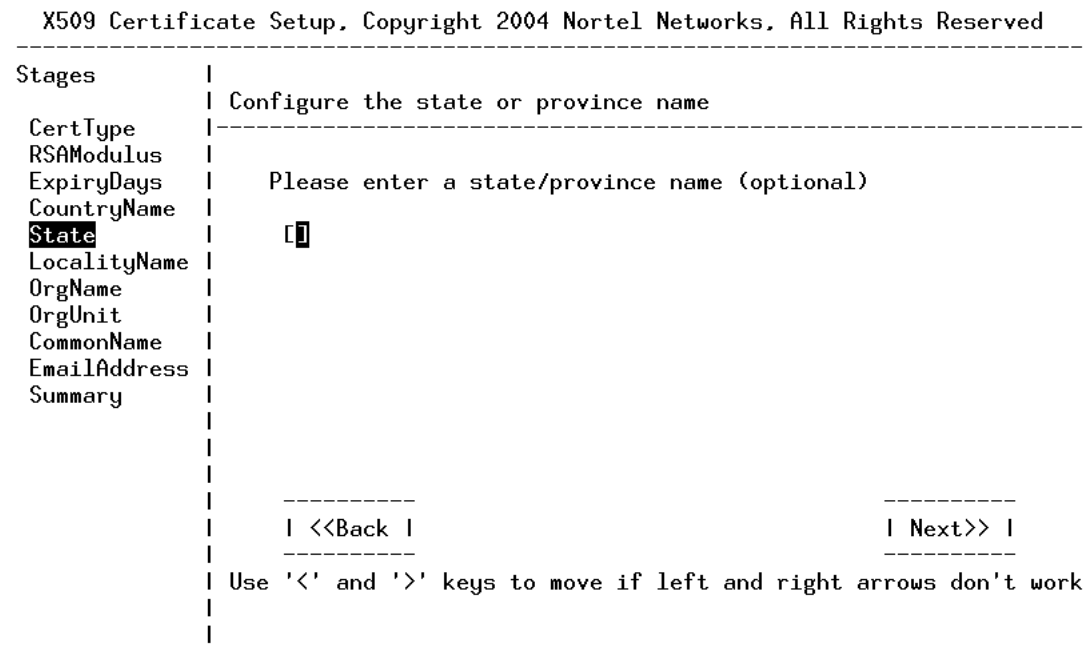


Figure 12 Locality Name

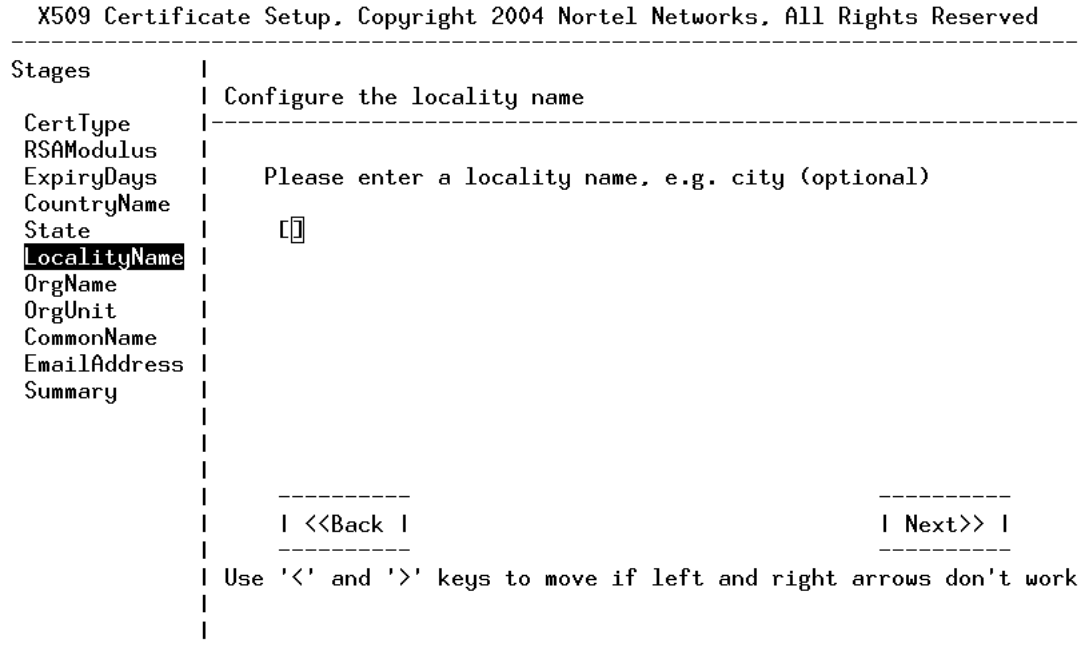


Figure 13 Organizational Name

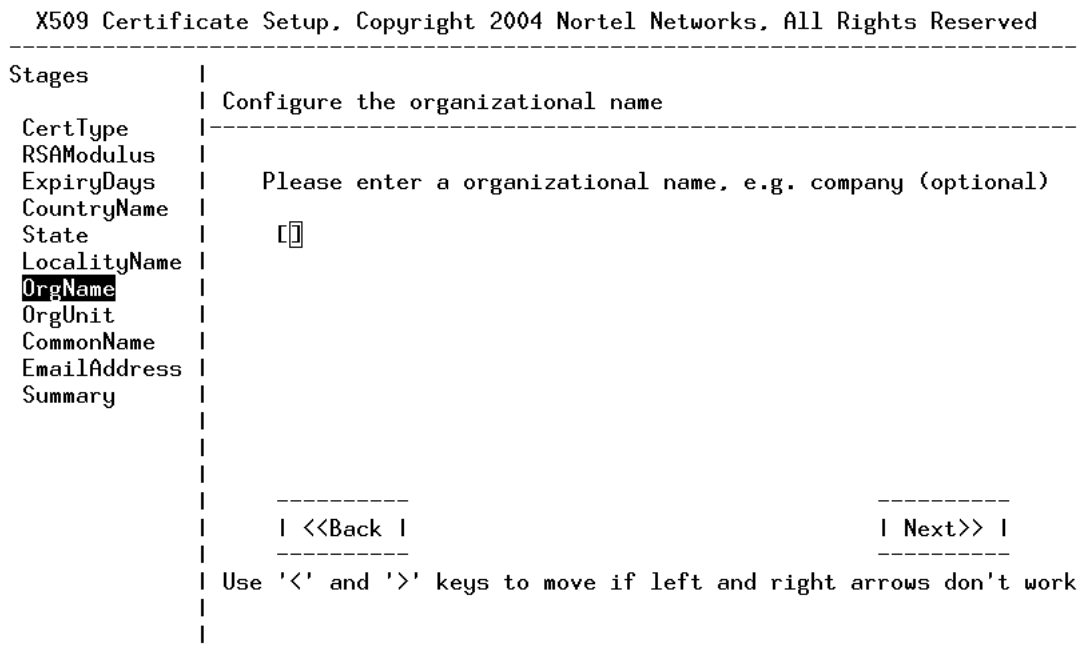


Figure 14 Organizational Unit Name

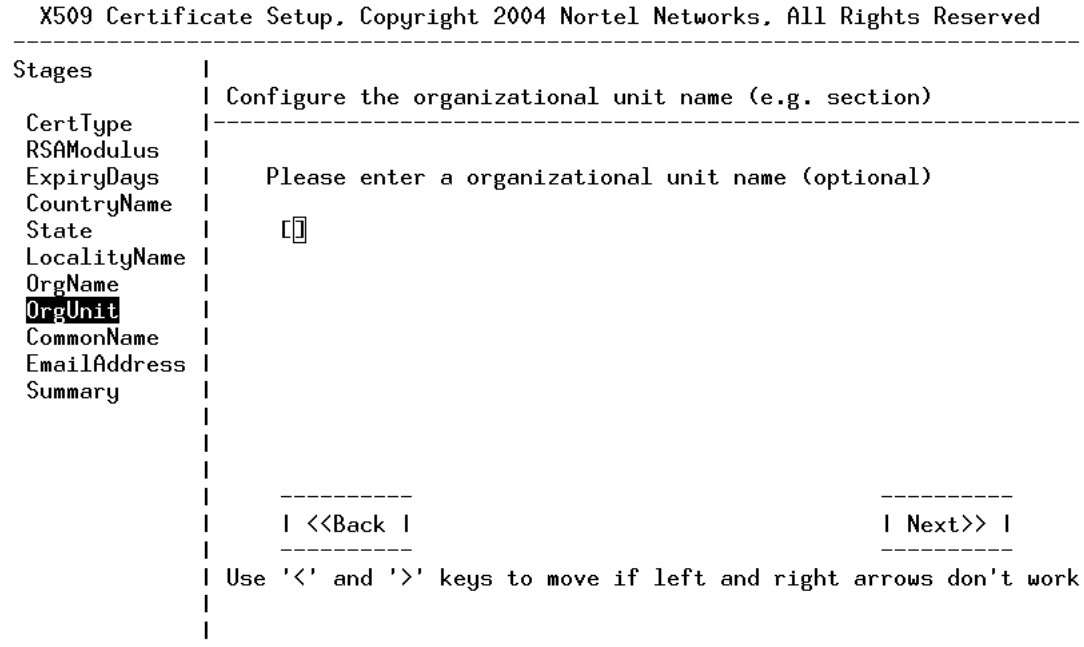


Figure 15 Common Name

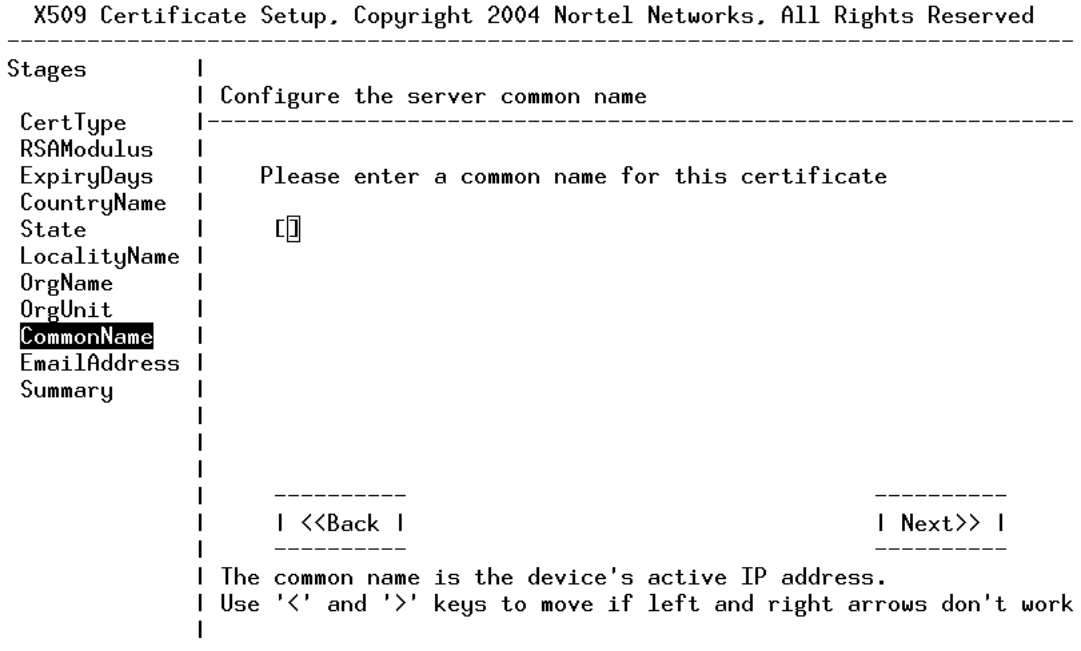


Figure 16 Email Address

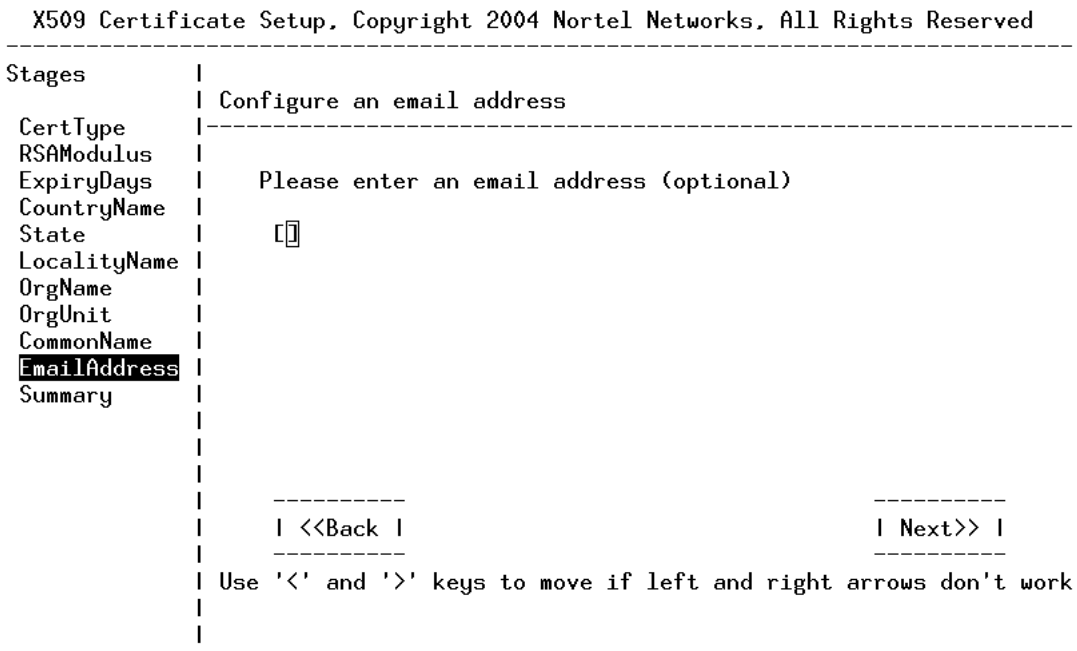
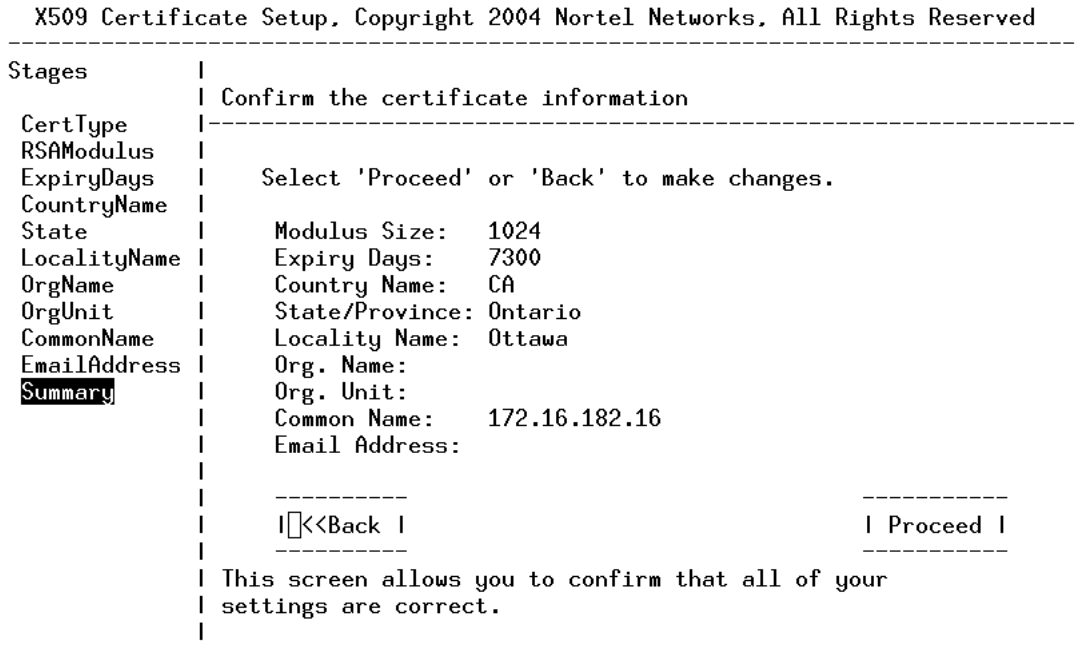


Figure 17 Summary for Self Signed Certificates



3.8.3.1.5 Certificate Signing Request

1. In the case of a certificate signing request, the craftsperson selects option 2 in Figure 1 ”Choose a Certificate Type” on page 1249.
2. Going back at any time will display the previous panel. Selecting proceed will only work if the craftsperson has entered the required information.
3. The craftsperson selects an RSA key size in Figure 6 ”Select Key Size” on page 1252. The key size can be 1024/1536/2048 bits. The higher the key size, the stronger the private key. There may be a performance impact to using higher key sizes due to additional encryption requirements.
   - If the key already exists in the /opt/base/share/ssl/ directory, the tool will prompt to reuse it or delete it and recreate a new key.
   - If the craftsperson wishes to reuse the key, the tool will always accept the key’s current size. This is illustrated in Figure 7 ”Key Already Exists” on page 1252
   - If in Figure 7 ”Key Already Exists” on page 1252, the craftsperson select ‘n’ that they do not want to proceed, then the tool prompts for key deletion in Figure 8 ”Remove Existing Key” on page 1253.
   - If in Figure 7 ”Key Already Exists” on page 1252, the craftsperson select ‘y’ that they do want to proceed, then the tool will reuse the existing key and move on to step 4.
   - If in Figure 8 ”Remove Existing Key” on page 1253, the craftsperson selects ‘n’ that they do want to proceed, the tool will then abort the current operation and return to the top of this step 3.
   - If in Figure 8 ”Remove Existing Key” on page 1253, the craftsperson selects ‘y’ that they do want to proceed, the tool will then make a backup of the existing key to another file in the same directory. A customer log is generated for this case.
4. The craftsperson selects a country, state, and city name in Figure 10 ”Country Name” on page 1254, Figure 11 ”State Name” on page 1254, Figure 12 ”Locality Name” on page 1255. These fields are optional. Although they are optional, they help to identify the NGSS to a remote entity.
5. The craftsperson selects an organizational name, and an organizational unit name in Figure 13 ”Organizational Name” on page 1255, and Figure 14 ”Organizational Unit Name” on page 1256. These fields optional. Although they are optional, they help to identify the NGSS to a remote entity.
6. In Figure 15 ”Common Name” on page 1256, the craftsperson identifies the mandatory common name. In the case of the NGSS, this must be the IP address of the active NGSS host. This is used for mutual authentication and is necessary for the correct operation of the NGSS. There is no validation at this stage of the common name.
7. In Figure 16 ”Email Address” on page 1257, the craftsperson identifies the optional email address of the local contact. There is no validation of the email address.
8. In Figure 18 ”Challenge Password” on page 1259, the tool queries for a challenge password. This password is used by the tool only.

9. Once all the information is entered, the tool displays a summary Figure 19 ”Certificate Signing Request Summary” on page 1260. Selecting “proceed” will generate the self signed certificate. The following message will be displayed on success.

```
Certificate Management:

Generating Certificate Signing Request
Generating a RSA Key
RSA private key has been successfully generated
Creating Certificate Signing Request
Certificate Signing Request has been successfully generated
-----BEGIN CERTIFICATE REQUEST-----

-----END CERTIFICATE REQUEST-----
Changing permissions on key file
Changing permissions on keystore file
```

10. The certificate signing request between the <BEGIN> and <END> delimeters is sent to the Certificate Authority for signing and certificate generation. Once that is done, the certificate authority’s certificate and the signed certificate are used to perform the function in section 3.8.3.1.6 ”Import Certificates and Private Key” on page 1260.

Figure 18 Challenge Password

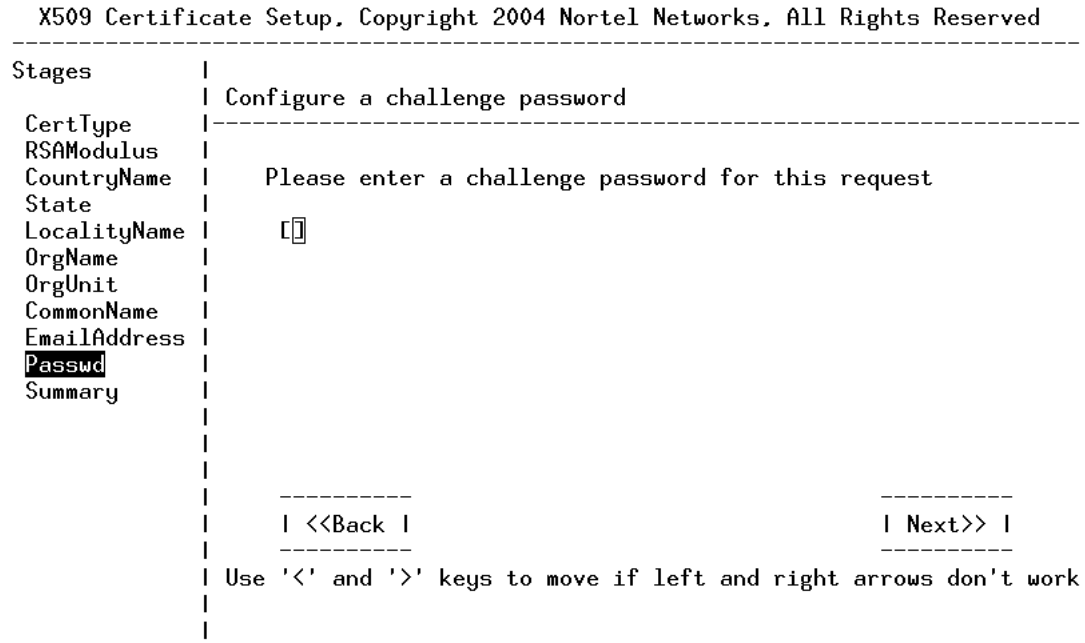
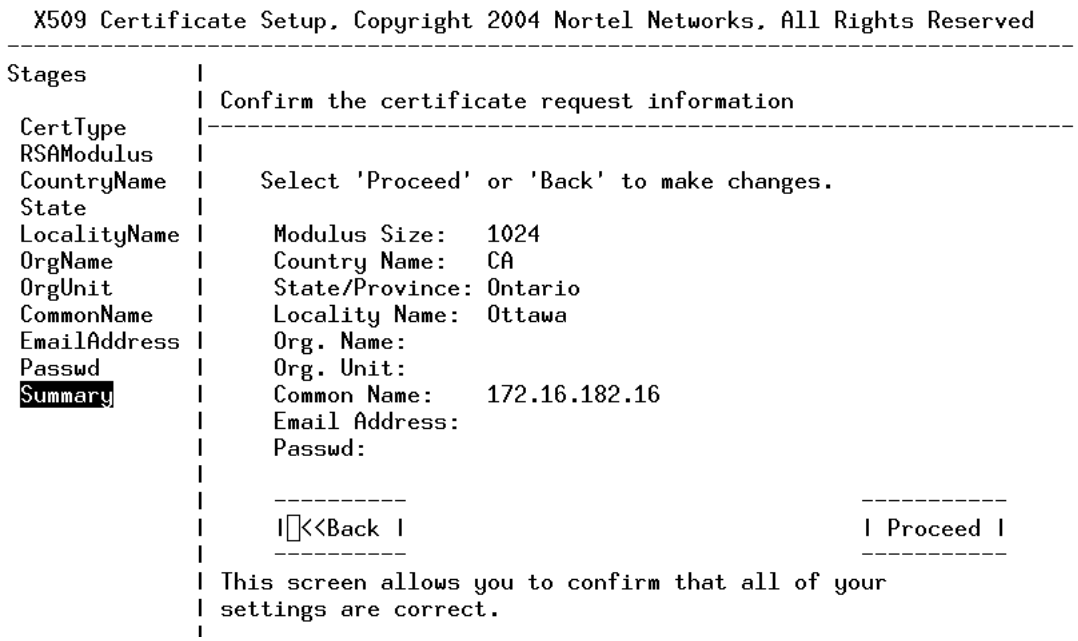


Figure 19 Certificate Signing Request Summary



3.8.3.1.6 Import Certificates and Private Key

It is recommended that this procedure NOT be executed from /opt/base/share/ssl nor is it recommended that the files be copied there prior to the execution of this procedure.

This procedure can be used to:

- Provision the self-signed certificate on the mate unit, and commit the files to /opt/base/share/ssl.
- Provision the CA-signed certificate from the signing request in option 2. The same private key that was generated in option 2 must be available.

1. Provide the CA certificates:
   - If this procedure is being used to provision the self-signed certificate on the mate unit, then, In Figure 20 , the craftsperson supplies the full path and filename where the self-signed certificate can be found. The tool will not proceed unless the file exists.
   - If this procedure is being used to import the CA-signed certificates, then, In Figure 20, the craftsperson supplies the full path and filename where the CA chain certificates can be found. The tool will not proceed unless the file exists.

2. Provide the server CA-signed certificate:

- If this procedure is being used to provision the self-signed certificate on the mate unit, then, In Figure 21 "Server Certificate - CA signed certificate" on page 1263, the craftsperson supplies the full path and filename where the self-signed certificate can be found. The tool will not proceed unless the file exists.
- If this procedure is being used to import the CA-signed certificates, then, In Figure 21 "Server Certificate - CA signed certificate" on page 1263, the craftsperson supplies the full path and filename where the CA signed certificate can be found.. The tool will not proceed unless the file exists.

3. Provide the private key. The craftsperson supplies the full path and filename where the private exists in Figure 22 "Provide the key" on page 1263.
4. Validation. In this step, the tool confirms the user input. By selecting "Proceed", the tool completes the import in Figure 23 "Import Summary" on page 1264.
5. If successful, the following messages are displayed (this example is for a self-signed certificate).

```
Provisioning CA Certificate
Verifying certificate/key pair
spawn openssl verify -CAfile server.crt server.crt
server.crt: OK
Certificate validation succeeded
Exporting certificate/key pair to PKCS#12 keystore
Committing trusted certificate to /opt/base/share/ssl
Committing server certificate to /opt/base/share/ssl
Committing private key to /opt/base/share/ssl
Certificate/key pair has been successfully exported to PKCS#12 format
Changing permissions on key file
Changing permissions on keystore file
```

Figure 20 CA Certificate - Trusted certificate

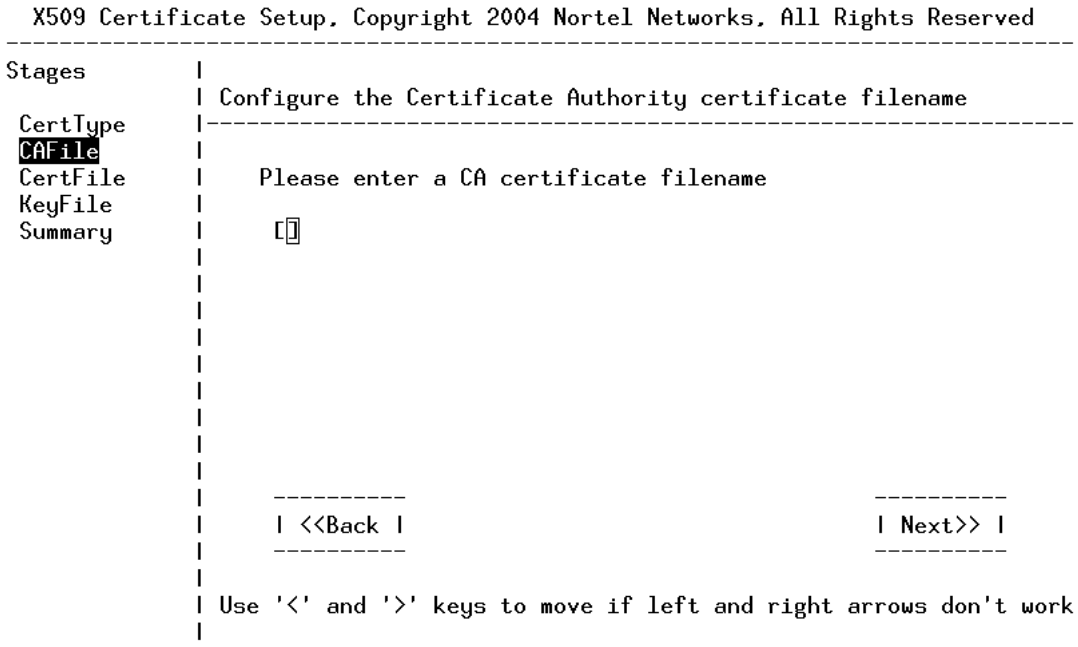


Figure 21 Server Certificate - CA signed certificate

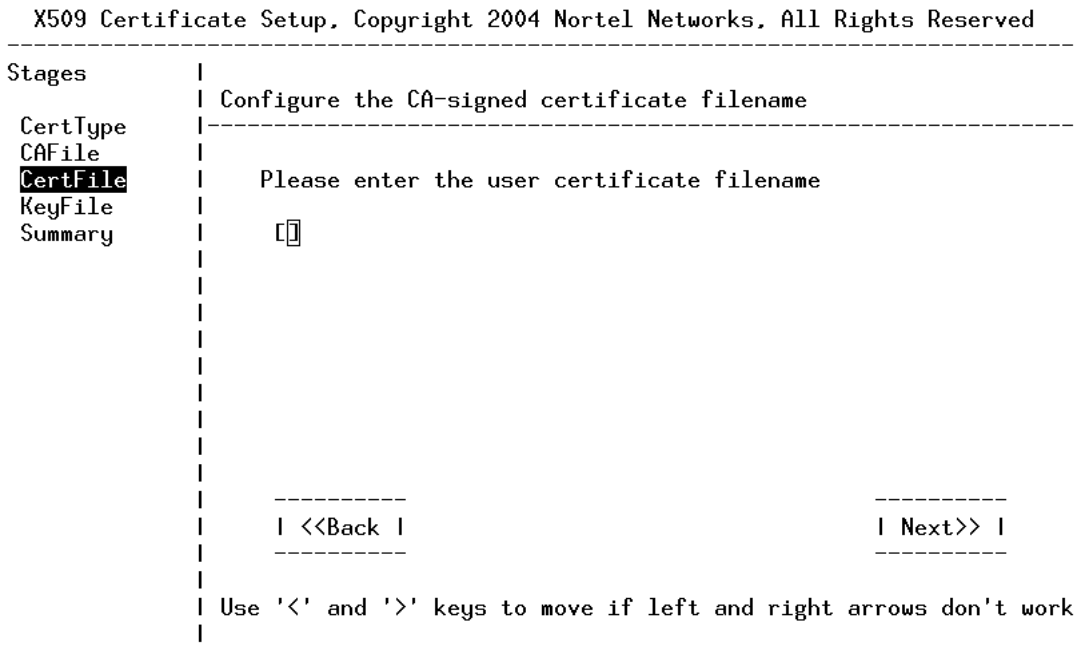


Figure 22 Provide the key

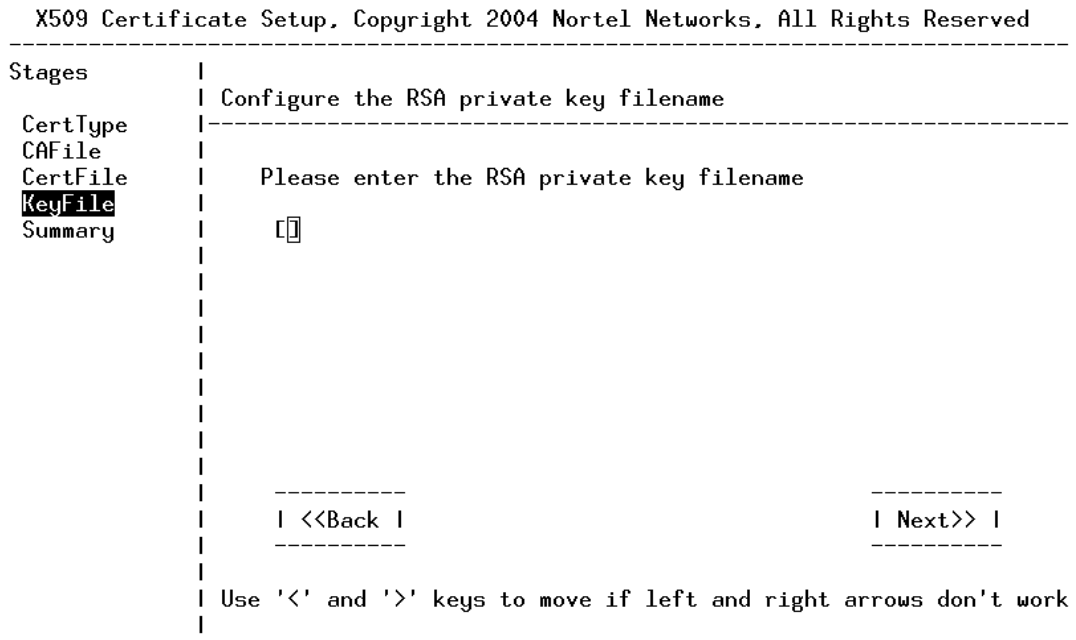
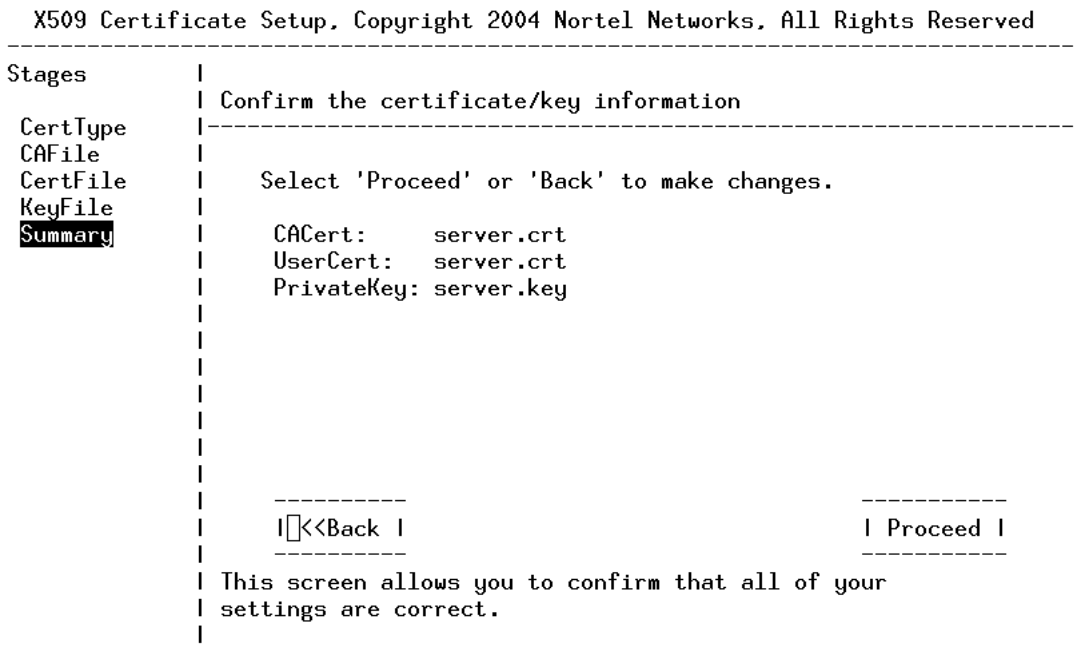


Figure 23 Import Summary



Import Summary shown above assuming a self-signed certificate import from the mate unit.

3.8.3.1.7 After provisioning a new certificate

Once the new certificate/key pair is in place, the Apache, Tomcat, and SIPGWYAPPLN applications must be restarted to ensure they are using the new certificate. This can be handled by rebooting the unit on which the new certificate was provisioned on, or by just stopping and starting the individual applications.

3.9 User interface changes

Not applicable.

3.10 OSSGate Interface Changes

Not applicable.

3.11 Security

3.11.1 Network configuration

Network configurations should not be changed as a result of this feature.

3.11.2 Key management

Key management will be done automatically as part of certificate management procedures. Keys will thus be managed internally by the CS2000 Session Server web server and/or CLI tools. No customer interface dealing with keys will be implemented.

3.11.3 Protocol

This activity is not making changes to protocols that are used to manage security.

3.11.4 Authentication

No change.

3.12 Configuration Walkthrough

See section 3.8 “Element Management” on page 1220.

Product = CS 2000

A00009252 -- Multi-Time Zone AMA Enhancements

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

In order to support networks that span Multiple Time Zones (MTZ) features in the Succession/CS2K products must be enhanced. Feature A59038784 introduced a framework to support MTZ and DST (Daylight Savings Times) for subscriber visible services. Feature A00009120 (done in parallel with this feature) extends this framework.

This feature allows the customer to record a corrected timestamp for billing records that originate on agents with the MTZ line option. The connect timestamp will be modified to the agent's time zone and this timestamp will be appended to the existing billing record in AMA using a module code and SMDR using an extension record.

Table AMAOPTS contains a new switch wide option (RECORD_MTZ) that will allow customers to use the MTZ option and decide whether or not they want to record the modified timestamp.

1.2 Software Requirements or Dependencies

SN09

1.3 Limitations and restrictions

The limitations and restrictions specified in activity A59038784 and A0009120 are also applicable to this activity.

In addition the following limitations and restrictions apply:

- This feature will not FORCE billing records, it will only append the information if a billing record exists.
- This Feature only modifies the Connect time stamp.
- Billable calls that terminate to an agent with the MTZ option will not generate a modified timestamp.

1.4 AMA

The addition of the MTZ line option and corresponding MULTITM datafill will append module code 611 (context ID 80200) that contains a modified connect time and date. The record will look as follows:

1.5 SMDR

1.6 Interactions

This feature interacts with the Multi-Time Zone feature, A59038784 and A0009120 Multi-Time Zone Enhancements.

1.7 Glossary

Term	Description
MTZ	Multi-Time Zone Enhancement
AMA	Automatic Message Accounting
SMDR	Station Message Detailed Recording

Product = CS 2000

A00009311-- SSPFS Dark Office backup

Functional Description

1: Applicable Solution(s)

UA-IP, PT-AAL2

1.1 Description

There is a critical need to allow customers to re-write the image and data on to the DVD more than one time without ejecting the DVD tray as it currently is done today. This limits the number of times someone has to go to the central office every time when backing up data is required or to put a DVD into the DVD tray every time its blanked.

With this feature, full system backups are schedulable to both active and inactive units and can re-use the same physical media (DVD-RW only) to rewrite over them. Alarms are raised when backups fail. System image size is limited to 4 Gig. A backup image can be restored to a fresh installed machine. The original media is required for a restore. A restore will either leave the non backed-up filesystems intact or create them if they do not exist.

Figure 1 illustrates a typical backup scenerio of how this feature is used

- User logs in either as a Super User or through the “Restricted Access Shell” feature in SN09 and be part of the “emsadm” group to have “su” access.

- User uses the SSPFS CLI (CLUI) to invoke the “Backup Configuration” settings menu and schedule a full system backup of the SSPFS box.
- On scheduled date and time, the bkfullsys backup command is called to backup the system and failures are reported northbound.

If the DVD disk is re-writable, no user intervention is required for this operation to happen and depending on what rules are defined for the DVD behavior, the DVD can be re-written over on the scheduled date and time automatically.

Three simple rules can be invoked through the “Backup Configuration” to define the backup behavior.

1 - When performing backup, eject DVD tray when done.

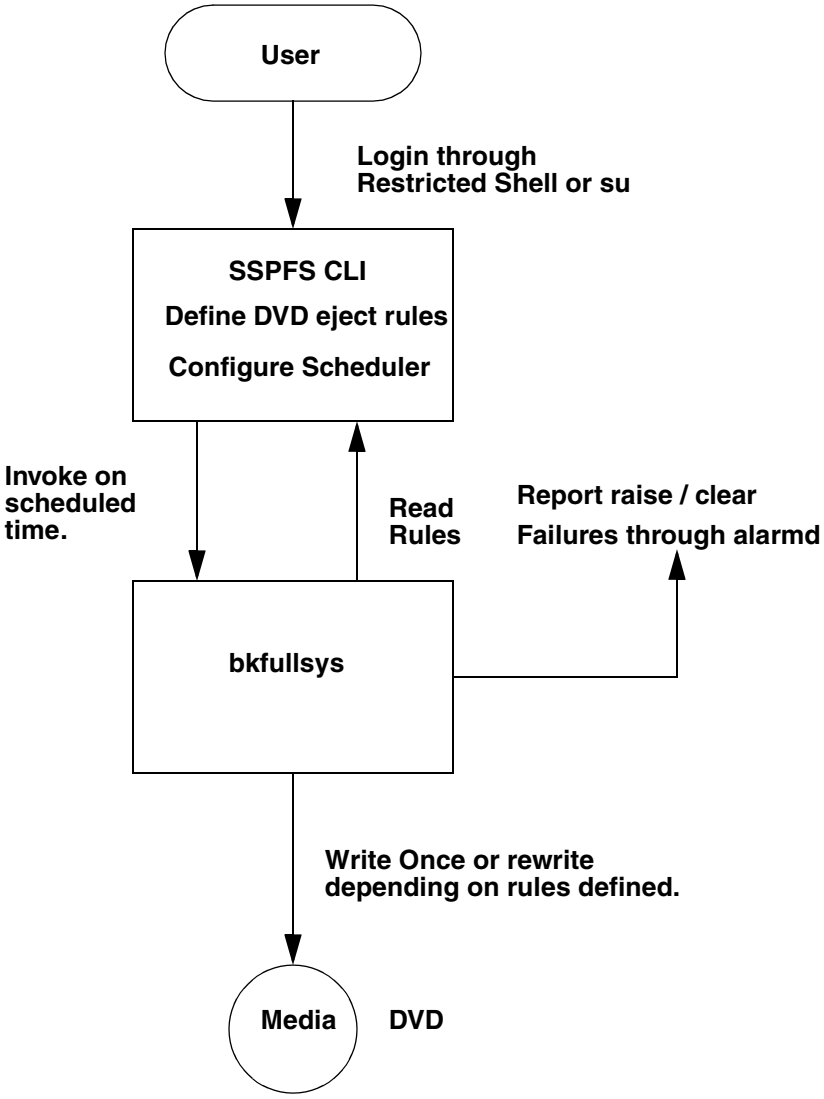
2 - When performing backup, do not eject DVD tray , subsequent backups will not overwrite previous data.

3 - When performing backup, do not eject DVD tray, subsequent backups will overwrite previous data.

The backup scripts (bkfullsys and bkdata) will also confirm to these rules if invoked manually, option 1 is default setting.

For backing up critical data which includes Oracle and critical application data, this feature provides you with an option that can be invoked through the “Backup Configuration” in SSPFS CLI called “***Copy last Oracle backup to DVD or tape”.*** This option will copy the last good Oracle backup from the “Syncronized Backup Manager” and burn it to DVD or tape. The “Syncronized Backup Manager” has its own scheduler for backing up the critical data at scheduled intervals and writes to disk. This option does not do the backup itself, it simply copies what was written to disk by the “Syncronised Backup Manager”.

Figure 1 Backup Flow Diagram



Full system Backup

1.2 Hardware Requirements or Dependencies

Not applicable

1.3 Software Requirements or Dependencies

Not applicable

1.4 Limitations and restrictions

Backup and Restore time depends on the I/O speed to the target media whether it is hard drive, tape drive, or DVD / CD burner.

1.5 Interactions

This feature interacts with the SSPFS backup and restore scripts for doing a full system backup and backing up of oracle and critical data that are part of the “Backup and Restore Enhancements” feature in SN09 which is called at scheduled intervals by the “Syncronized Backup Manager” which was first introduced in SN08.

This feature also interacts with the “Restricted Access Shell” feature to be able to schedule backups in a restricted shell environment.

1.6 Glossary

Term	Description
CLUI	Command Line User Interface
SSPFS	Succession Solution Platform Foundation Server
CLI	Command Line Interface

Product = CS 2000

A00009313 -- SSPFS SN09 Upgrades and ESD Support

Excerpts from the Design Summary

1: Applicable Solution(s)

UA-IP, PT-AAL2

1.1 Description

This feature will cover the SSPFS upgrade from SN07, or SN08 to the SN09 SSPFS release. The goal of this feature is primarily two areas: ESD support and greater robustness.

The intent is to upgrade SSPFS with a minimal of application downtime.

1.2 Design Component: ESD SSPFS SN09 Upgrade

It is very important to set the expectations of this feature. The goal of this feature is to provide SSPFS upgrades using electronic delivery of the ISO images instead of physical cdrom media.

The pre_upgrade.ksh upgrade script of SSPFS will create the location /Upgrade which will be the repository for the iso images. After the execution of the pre_upgrade script, the user is to place all 3 disk images in the /Upgrade

directory. If they all exist, the user will be prompted as to whether or not they intend to perform an ESD upgrade. If they respond positively, then the upgrade will begin in a similar fashion to the normal upgrade. However, the main difference is that the user will never be prompted for the insertion of the SSPFS cdrom disks. Therefore, it will continue unassisted until near the end of the SSPFS upgrade. There will be one point on cbm profiles, where the SSPFS upgrade will stop and we will prompt the user to upgrade the CBM application. Lastly, the user must choose to accept the upgrade or fallback just like the normal upgrade.

1.3 Design Component: pre_upgrade.ksh improvements

This design component is just being developed to document changes which will be placed into the pre_upgrade.ksh script for robustness.The pre_upgrade.ksh upgrade script of SSPFS will be enhanced to check the following additional system states prior to full upgrade execution:

- Ensure the required SSPFS disk mirrors exist and have all sub-mirrors attached.
- Ensure that /var has enough free space to hold the package spooling during the upgrade execution.

These enhancements will allow pre_upgrade to catch more failure cases prior to execution of the main upgrade script. Therefore, the user has a chance to fix system errors before attempting the upgrade again.

1.4 Glossary

N/A

Product = CS 2000

A00009315 -- Detect Failures from Syslog and Generate Alarms

Functional Description

1: Applicable Solution(s)

UA-IP, PT-AAL2

1.1 Description

Detect if the syslog system has failed to write logs and raise a major alarm. If and when the syslog system becomes operational, the alarm will be cleared.

Failure detection is not done on each write to the syslog stream, thus it's not 100% real-time. A ten minute audit is used instead. If the audit fails it will wait for one more failing audit before the alarm is raised.

The default timing interval for checking that the logs have stopped is 10 minutes. If a log was generated within the last 10 minutes then everything is working. If the log is older than 10 minutes the system will allow one more 10 minute interval to pass before rasing an alarm. The fastest that an alarm will be raised is 21 minutes and the slowest is 29 minutes.

Note, the timing interval is fixed and cannot be changed by the customer.

This facility will be provided on all profiles of SSPFS-based products, including CMT, MG9K EM, IEMS, MDM, and CBM.

The Fault Management section identifies the details of the new alarm.

1.2 Hardware Requirements or Dependencies

Not applicable.

1.3 Software Requirements or Dependencies

Not applicable.

1.4 Limitations and restrictions

Does not monitor each syslog write in real-time, and does not ensure reliable forwarding of syslog messages to a remote syslog daemon.

1.5 Interactions

Not applicable.

1.6 Glossary

Not applicable.

2: Fault Management for A00009315

2.1 Fault management strategy

ISSPFS will generate alarms for:

- Detect that the logging system is no longer writing logs

2.2 Fault management tools and utilities

The scope of this feature is to provide a mechanism to immediately notify, in real-time, the MSAP administrator (e.g., alarm) if the MSAP security log fails to record the events that are required to be recorded.

2.3 Logs

None

2.4 Alarms

2.4.1 Logging has stopped Alarm

```
Component Id     :
cbm850=wnc0s0rv;NODE=wnc0s0rv,CLASS=SYS,SYSTYPE=Syslog,File=monitor_syslog.csh
Severity         : Major
State            : ISTb
Report Name      : SPFS
Report Number    : 380
Application      : SSPFS_RES_MON
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : The Logging system is not writing logs
Specific Problem : syslogd not writing marklog logs
User Data        :
Recovery Action  :
Time When Raised : Wed Mar 2 11:51:28 2005
```

2.4.2 Logging has stopped Alarm Clearing

```
Component Id     :
cbm850=wnc0s0rv;NODE=wnc0s0rv,CLASS=SYS,SYSTYPE=Syslog,File=monitor_syslog.csh
Severity         : Cleared
State            : InSv
Report Name      : SPFS
Report Number    : 380
Application      : SSPFS_RES_MON
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : The Logging system is now writing logs
Specific Problem : syslogd is now writing marklog logs
User Data        :
Recovery Action  :
Time When Raised : Wed Mar 2 11:53:34 2005
```

2.5 Related documentation

N/A

Product = CS 2000

A00009332 -- P-Time and Codec Negotiation Selection Policy

Functional Description

1: Applicable Solution(s)

PT-AAL1, PT-IP, UA-IP, Int'l UA-IP

2: Description

This feature makes enhancements to the CS2M that allows the customer to choose codecs and packetization rates for IP and aal2 network bearer connections that were previously not available. The new P-times are p30ms and p40ms.

The CS2M now supports the following new codecs.

- G.723
- EVRC
- EVRC0
- G726-32
- ILBC
- BV16
- AMR
- G726-24

In addition to the above, further enhancements were made to the CS2M GUI. These enhancements were to display G.711A as PCMA and G.711U as PCMU.

Note: Codec ILBC should only be associated with packetization rates of 20ms or 30ms.

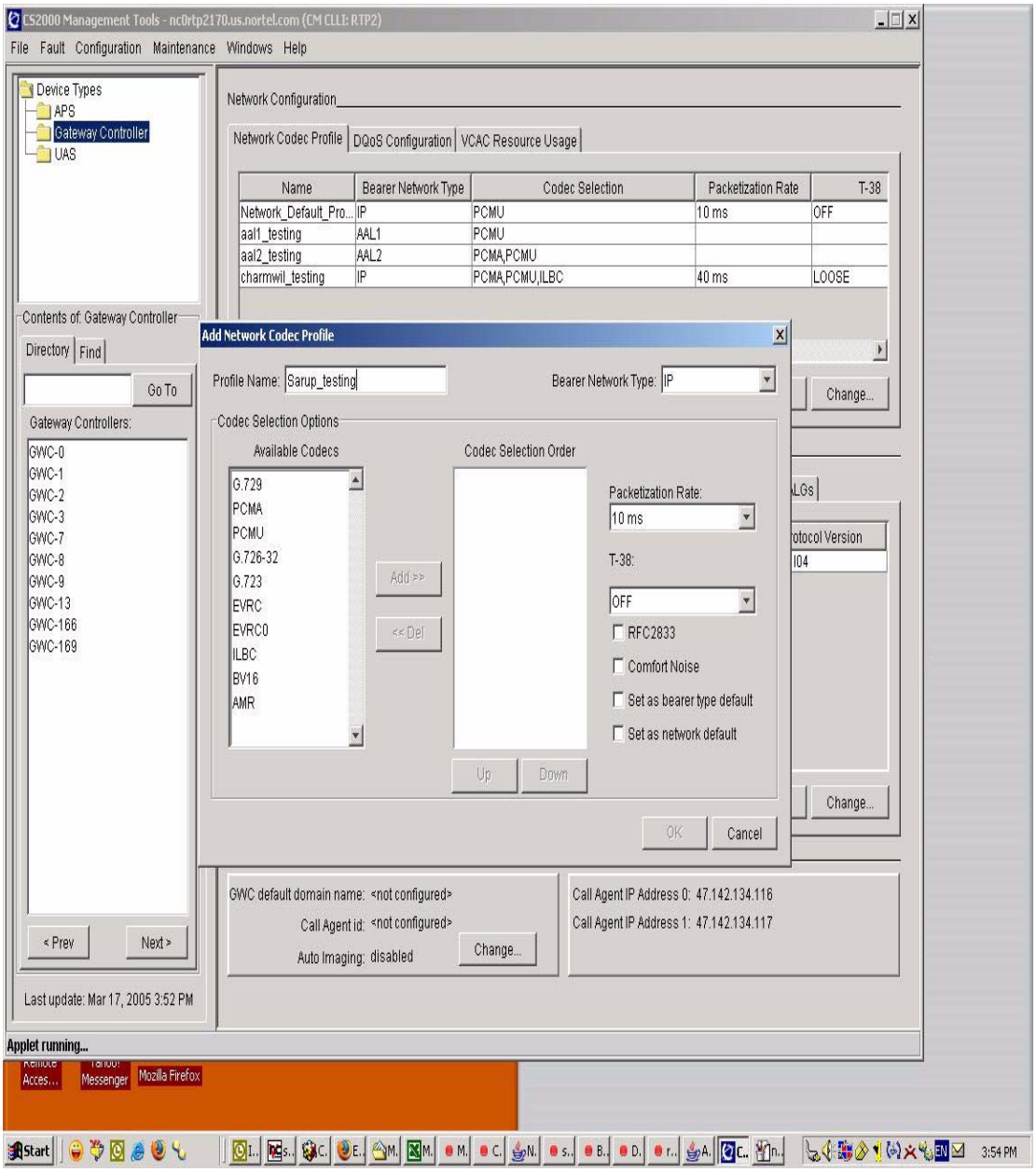
2.1 CS2M GUI Functionality Modifications

2.3.1 Add Network Profile Dialog

When adding a new network profile, the customer could choose three of the eleven codecs listed in the text area. Whatever combination of three that the customer chooses, that combination must include PCMA or PCMU.

The customer can choose from one to maximum of three codecs to provision within their network. Figure one shows the "Add Network Profile Dialog" screen that listed a subset of the codecs the CS2M support.

figure one: Add Network Profile Dialog

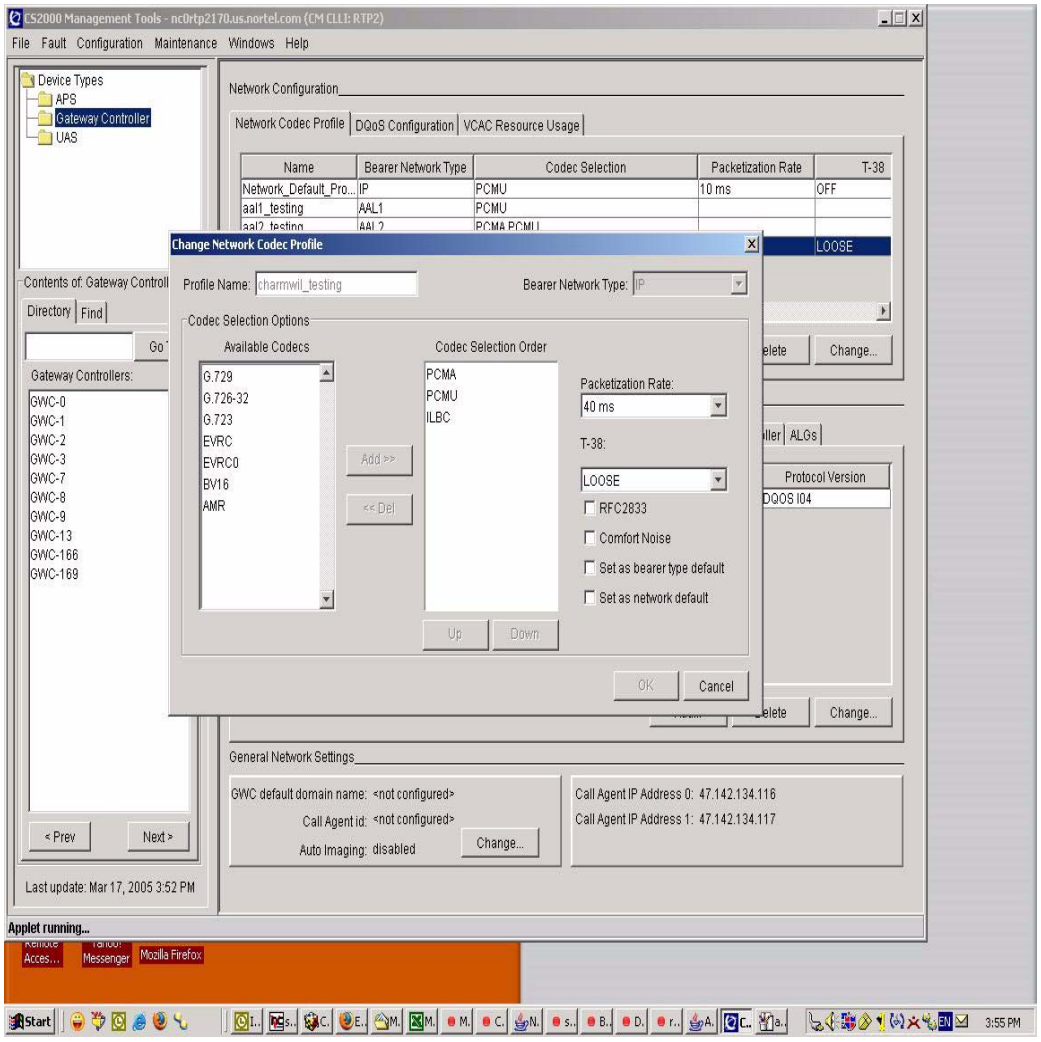


2.3.2 Change Network Profile Dialog

When changing the Network profile, the customer can now select from eleven codecs shown in the selection listing area. Figure two shows the "Change Network Profile Dialog" screen which allows the user to change their previous selection/s.

Note: The same restriction stated in "Add Network Profile Dialog" section applies here.

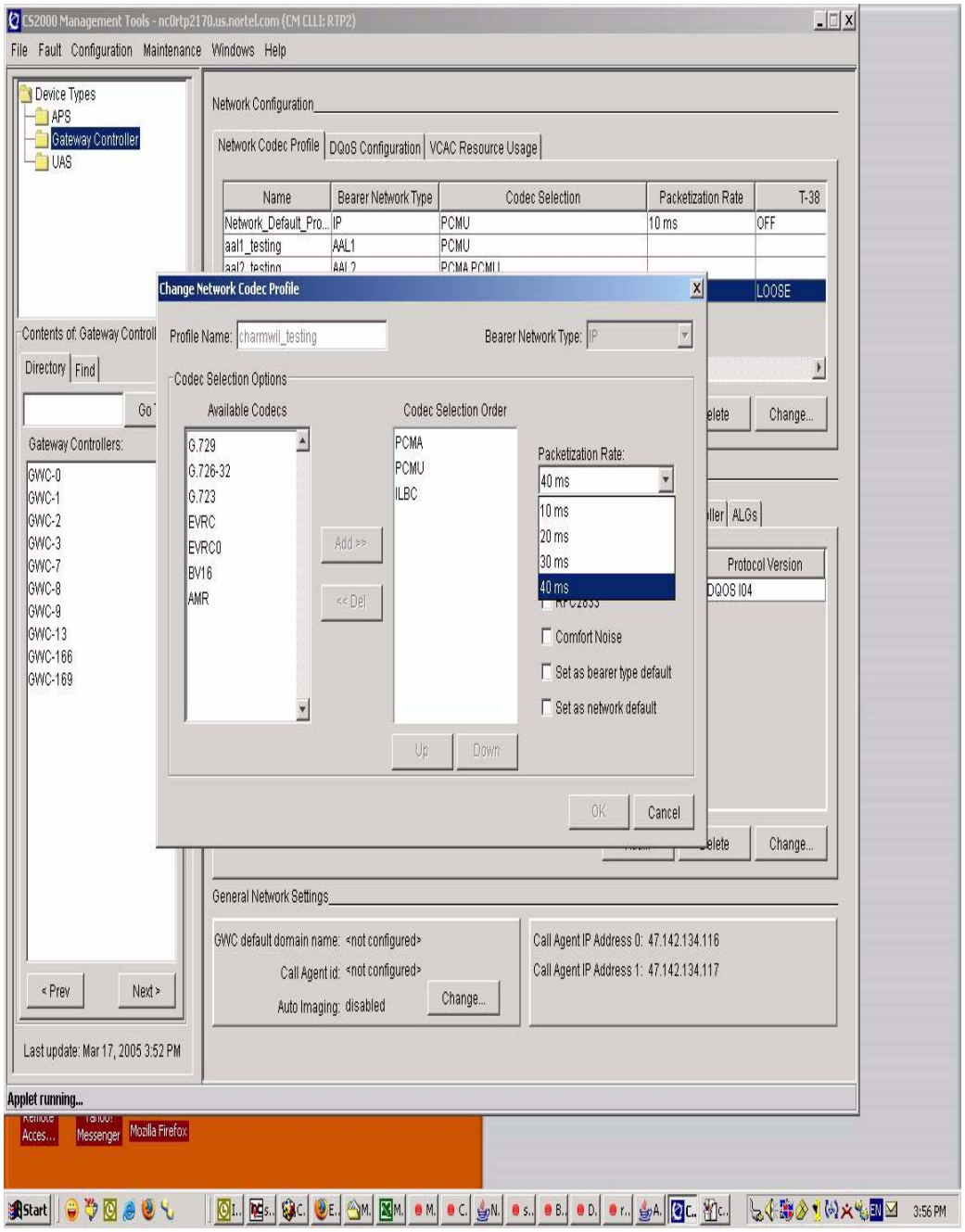
Figure 2: Change Network Profile Dialog



2.3.3 Add P-time Dialog

The customer can now select from four p-times. The p-times are p10ms, p20ms, p30ms and p40ms. Figure 3 shows the screen image of the P-time menu.

Figure 3: Add P-time Dialog Menu



2.2 Hardware Requirements or Dependencies

None.

2.3 Software Requirements or Dependencies

None.

2.4 Limitations and restrictions

- The maximum number of codecs the user is allowed to select is three.
- The user's selection/s must always include PCMA or PCMU.

2.5 Interactions

None.

2.6 Glossary

Term	Description
P-Time	Packetization rate
CS2M	CS2K Mangement Tool

Product = CS 2000

A00009353 -- GWC Unit Availability/ Health Monitoring

Functional Description

1: Applicable Solution(s)

PT-IP

1.1 Description

This feature addresses the prevention of GWC node outage caused by an improper SWACT to a GWC unit which appeared to be in good condition but was not.

This feature enhances the existing PreSwact audits and also create a new framework to monitor the health condition of the application resources like TAPI resource objects and Acceptor queues.

This feature will address the following:

1. Enhancement of the existing PreSwact audit.

2. Introduce a new alarm which will be raised whenever PreSwact audit fail.

1.1.1 Enhancement of the Existing PreSwact audit

Currently the PreSwact audit performs a set of checks to estimate the health of the inactive unit. This feature enhances the checks to consider additional fault conditions, such as

1. Datasync mismatch with the SESM
2. Invalid/Mismatch in some of GWC flash and GWC RAM data.
3. Application resource issues such as TAPI blocks (Transaction, Request and call)
4. Messaging resources (Acceptor queue on TAPI and Connection Broker).
5. Patching in progress in the inactive unit.However no alarm will be raised if the preSwact audit fails under this condition.

The PreSwact audit runs at a frequency of 40 seconds and with priority 6.

Swact force can still be used to force a manual warmswact when the preSwact audit fails and alarm raised.This existing functionality will not be changed.

1.1.2 New PreSwact alarm

This feature will introduce a new alarm which will be raised when ever PreSwact audit fails. An alarm will be raised with proper text which explains which component has led Preswact audit to fail. The PreSwact runs periodically and raises alarm for PSA fail on error conditions.The specific problem displayed at the GWC level for the alarm raised will match with the swact failure reason at the SESM GUI.

1.1.2.1 Details of alarm

The details of the new alarm are as follows:

Table 1: PreSwact Alarm details

Description	PreSwact Audit Failure
Severity or Level	Major
Category	QualityOfService
Probable Cause	resourceAtOrNearingCapacity
Component	NODEMTC
Specific Problem	Description about the component which caused the PreSwact audit failure.

1.2 Hardware Requirements or Dependencies

None.

1.3 Software Requirements or Dependencies

None.

1.4 Limitations and restrictions

This feature has been submitted in SN09 and hence requires both the Units (Active and Inactive) to have SN09 or higher versions.

1.5 Interactions

This feature will interact with another activity A00009350 to get the health status of the flash data. An interface will be provided by the above activity for the preswact audit to query the status of flash-data.

1.6 SESM ALARM Snapshots

The alarms will be displayed in the SESM under ALARM MANAGER.These are the snapshots from the SESM-ALARM MANAGER level(shown as two images for better clarity.)

- Alarm Manager - Connected to: 172.16.17.5
ork Element
Category
Alarm Time
Quality of Service
20:05:49 12-Jan-2005 IST
Communications
15:40:53 13-Jan-2005 IST
Communications
00:30:10 13-Jan-2005 IST
Communications
00:30:10 13-Jan-2005 IST
Communications
00:30:10 13-Jan-2005 IST
Quality of Service
16:58:14 13-Jan-2005 IST
Severity
Probable Cause
Major
Underlying resource unavailable
Major
Underlying resource unavailable
Major
Communications subsystem failure
Major
Communications subsystem failure
Major
Communications subsystem failure
Major
Resource at or nearing capacity

1.7 Glossary

Term	Description
EM	Element Manager
GWC	Gate Way Controller
PSA	PreSwact Audit
SWACT	Switch of Activity

Product = CS 2000

A00009364 -- CICM End-of-Call QoS Reporting

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

In Voice over IP networks, Quality of Service (QoS) can be adversely affected by the components in the network. Unlike TDM networks where the voice quality is consistent for all calls, VoIP networks can experience different voice quality on all calls.

Per-call QoS statistics can be used for the following:

- Network engineering
- Trend analysis
- Trouble-shooting network problems
- Service Level Agreement (SLA) validation

The CICM reports QoS statistics as shown in Figure 1, "CICM QoS Reporting," and can be described as follows:

- The CICM reports the QoS statistics at the end of the call. Each ephemeral associated with a call reports QoS statistics separately. When the GWC instructs the CICM to subtract the ephemeral termination, QoS statistics are sent to:
    - The gateway controller (GWC) over H.248

  - The extended QoS server (a predefined ip address and port number) over UDP in an ANSI based XML format.

- The GWC reformats the QoS statistics reported by the gateway into a binary format and sends the QoS report to the QoS Collector Application (QCA).
- The QCA manages QoS streams from multiple GWCs, reformats the data to an IPDR format, and stores the data to disk.

QoS statistics are accumulated on supported clients/terminals while a call is active. If a call is placed on hold, the QoS statistics are frozen (no more statistics are accumulated) until the call is resumed.

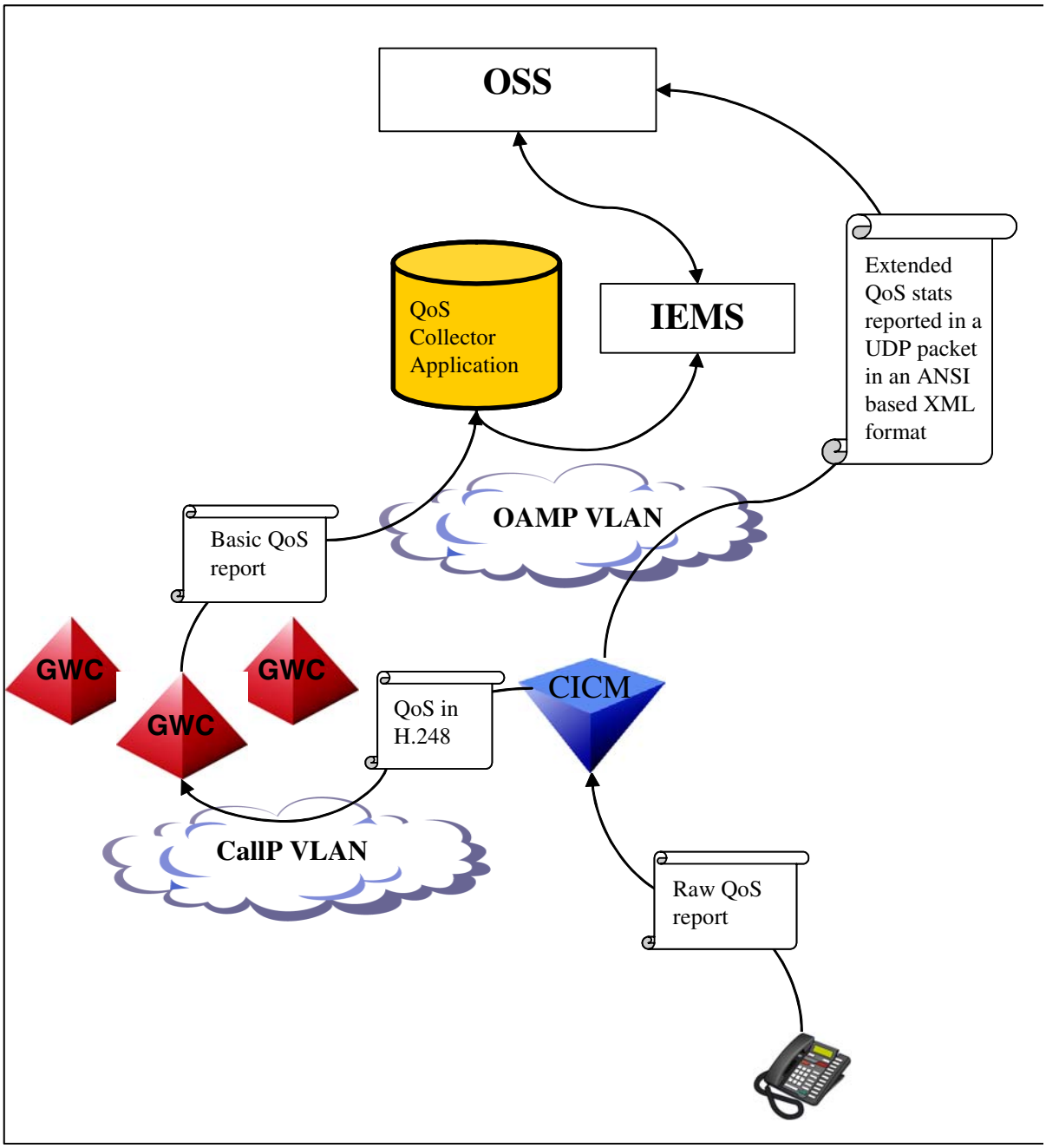


Figure 1CICM QoS reporting

See Table 1 for a list of supported QoS parameters.

NOTE 1: Phase 1 terminals support version 1 QoS reporting only. Phase 2 terminals support version 2 “extended” QoS reporting. A complete list of QoS statistics is shown in Table 1 QoS parameters reported. See section Limitations

and restrictions for further details on supported client/terminal types and firmware requirements.

NOTE 2: Statistics which cannot be obtained from a client/terminal are reported upwards (to the GWC and extended QoS server) with a value of '0'.

Table 1 QoS parameters reported

Terminal /Client QoS reporting version					**CICM QoS Report type**	
1	**2**	**Parameter Name**	**Extended report abbrev.**	**Description**	**Basic (QCA)**	**Extended (extended QoS server)**
X	**X**	**Jitter Average**	JA	Average variation in packet arrival times due to transmission (routing, queuing delay, etc…) through the network. Represented in 1/65536 of seconds, of the incoming RTP packets inter-arrival time.	X	X
X	**X**	**Jitter High Water Mark**	JHW	Max variation in packet arrival times due to transmission (routing, queuing delay, etc…) through the network. Represented in 1/65536 of seconds, of the incoming RTP packets inter-arrival time.		X
X	**X**	**Far End Originated Loss**	FEOL	Far end orginated loss	X	X
X	**X**	**Round Trip Average**	RTA	Average RTCP packets round trip time. Represented in 1/65536 of seconds, of the incoming RTP packets inter-arrival time.		X
X	**X**	**Round Trip High Water Mark**	RTHW	Max RTCP packets round trip time. Represented in 1/65536 of seconds, of the incoming RTP packets inter-arrival time.		X
	X	**Local Silence Suppression**	SS	Indicates if silence suppression was used.		X

	X	**Local Rx and Tx Codec Type**	rC/tC	Codec Type		X
	X	**Local Rx and Tx Packetization Rate**	rPR/tPR	Frame duration in milliseconds**.**		X
	X	**End System Delay**	ESDA	Most recently specified/calculated end system delay in milliseconds. This includes the sample accumulation and encoding delay, as well as the average jitter buffer delay, decoding and playout delay.		X
	X	**Average One Way Delay**	OWDA	average one-way delay in milliseconds.	X	X
	X	**Maximum One Way Delay**	OWDM	maximum one-way delay in milliseconds.		X
	X	**Average Noise Level**	NLA	ratio of the silent period background noise level to overflow signal power, expressed in decibels; 127		X
	X	**Average Signal Power**	SPA	ratio of the signal level to overflow signal level, expressed in decibels; measured only for packets containing speech energy.		X
	X	**Echo Return Loss**	ERL	sum of the measured echo return loss (ERL) and the echo return loss enhancement (ERLE) expressed in dB; the ratio of a transmitted voice signal that is reflected back to the talker.		X
	X	**Listening R factor**	LRF	direct measure of the call quality or transmission quality, and incorporate the effects of CODEC type, packet loss, discard, burstiness, delay etc.; this metric describes the segment of the call that is carried over this RTP session.		X
	X	**Conversational R factor**	CRF	segment of the call that is carried over a network segment, external to the RTP segment, for example a cellular network; relates to the outward voice path from the Voice over IP termination for which this metrics block applies.		X

	X	**Listening Quality MOS**	LM	estimated mean opinion score for listening quality. The valid scale is 10 to 50 representing MOS 1.0 to 5.0, respectively.		X
	X	**Conversational Quality MOS**	CM	estimated mean opinion score for conversational quality. The valid scale is 10 to 50 representing MOS 1.0 to 5.0, respectively.		X
	X	**Burst R factor**	BRF	R factor during a burst period; a burst is defined as a longest sequence of packets bounded by lost or discarded packets		X
	X	**Average Burst Density**	BDA	average percentage of MIU's lost or discarded during burst periods. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X
	X	**Burst count**	BC	number of bursts that have occurred on the call		X
	X	**Average Burst Length in MS**	BLA	average length of all burst periods in milliseconds that have occurred on the call		X
	X	**Gap R factor**	GRF	R factor during a gap period; a gap is defined as the period of time between two bursts.		X
	X	**Average Gap Density**	GDA	average MIU'S lost or discarded within gap periods. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X
	X	**Average Gap Length in MS**	GLA	average length in milliseconds of all gaps that have occurred on the call.		X
	X	**Average Loss Rate**	LRA	total average percentage of MIUs lost and/or discarded. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X
	X	**Average Network Loss Rate**	NLRA	total average percentage of MIUs lost in the network. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X
	X	**Average Discard Rate**	DRA	total average percentage of MIU's discarded. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X

	X	**MIU Duration**	MD	duration of each MIU, in milliseconds		X
	X	**MIU per packet**	MPP	total number of MIU's in each RTP packet		X
	X	**MIU Loss percentage**	MLP	percentage of MIUs handled by the call channel that were lost in the network. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X
	X	**MIU Discard percentage**	MDiP	percentage of MIUs handled by the call channel that were discarded by the endpoint. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X
	X	**MIU Out of order percentage**	MOOOP	percentage of MIUs handled by the call channel that is discarded by the endpoint. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X
	X	**MIU Duplicate percentage**	MDP	percentage of MIUs handled by the call channel that is discarded by the endpoint. This value is an 8:8 fixed–point value (i.e. scaled by 256).		X
	X	**Number of RTP packets rx/tx**	rP/tP	Number of RTP packets received and transmitted	X	X
	X	**Number of RTP packets out of order**	rPOOO	Number of RTP packets received out of order		X
		Octets rx/tx	rO/tO	Octets sent and received. NOTE: This parameter is not currently supported by any terminal types. This value will be set to '0' in all reports.	X	X

1.1.1 Extended QoS statistics

The complete list of QoS statistics displayed in Table 1 "QoS parameters reported" can be obtained by configuring the ip address and port number of an extended QoS server on the element manager (see section Datafill for further details on datafill). Extended QoS statistics for each call half will then be reported to the extended call server. Basic QoS statistics will still be reported to the QCA.

The extended report is sent to the configured destination by UDP (using the CICMs admin ip address, port number 34366) in an ANSI-based XML format. An example extended QoS XML report is displayed below:

NOTE: Depending on the client/terminal type hosting the call. Please see section Limitations and restrictions for further information.

```
<?xml version="1.0" ?>
<qos>
<ST>2005-18-03T16:19:06Z</ST>
<ET>2005-18-03T16:19:08Z</ET>
<host>CICM-180-B</host>
<LEN>CICM 180 0 00 01</LEN>
<Ip>47.123.124.125</Ip>
<JA>4294967295</JA>
<JHW>4294967295</JHW>
<FEOL>256</FEOL>
<RTA>4294967295</RTA>
<RTHW>4294967295</RTHW>
<SS>1</SS>
<rC>256</rC>
<tC>256</tC>
<rPR>65535</rPR>
<tPR>65535</tPR>
<PE>256</PE>
<ESDA>65535</ESDA>
<OWDA>65535</OWDA>
<OWDM>65535</OWDM>
<NLA>65535</NLA>
<SPA>65535</SPA>
<ERL>65535</ERL>
<LRF>256</LRF>
<CRF>256</CRF>
<LM>65535</LM>
<CM>65535</CM>
<BRF>256</BRF>
<BDA>65535</BDA>
<BC>65535</BC>
<BLA>4294967295</BLA>
<GRF>256</GRF>
<GDA>65535</GDA>
<GLA>4294967295</GLA>
<LRA>65535</LRA>
```

```
<NLRA>65535</NLRA>
<DRA>65535</DRA>
<MD>65535</MD>
<MPP>65535</MPP>
<MLP>65535</MLP>
<MDiP>65535</MDiP>
<MOOOP>65535</MOOOP>
<MDP>65535</MDP>
<rP>4294967295</rP>
<tP>4294967295</tP>
<rPOOO>4294967295</rPOOO>
<rO>4294967295</rO>
<tO>4294967295</tO>
</qos>
```

The header information for the extended QoS XML report is described in the following table.

Table 2 Extended QoS report header information

Extended QoS XML header tag	Description	Format	Example
ST	Start time (Universal time – UTC)	yyyy-dd-mm**T**hh:mm:ss**Z**	**2005-18-03T16:19:06Z**
ET	End time (Universal time – UTC)		
Host	Machine host name	CICM-xxx-x	CICM-180-A
LEN	LEN	CICM xxx x xx xx	CICM 180 0 00 01
Ip	Ip address of the client	xxx.xxx.xxx.xxx	47.121.122.123

1.1.2 Datafill

QoS reporting is enabled/disabled from the GWC element manager (see the following figure).

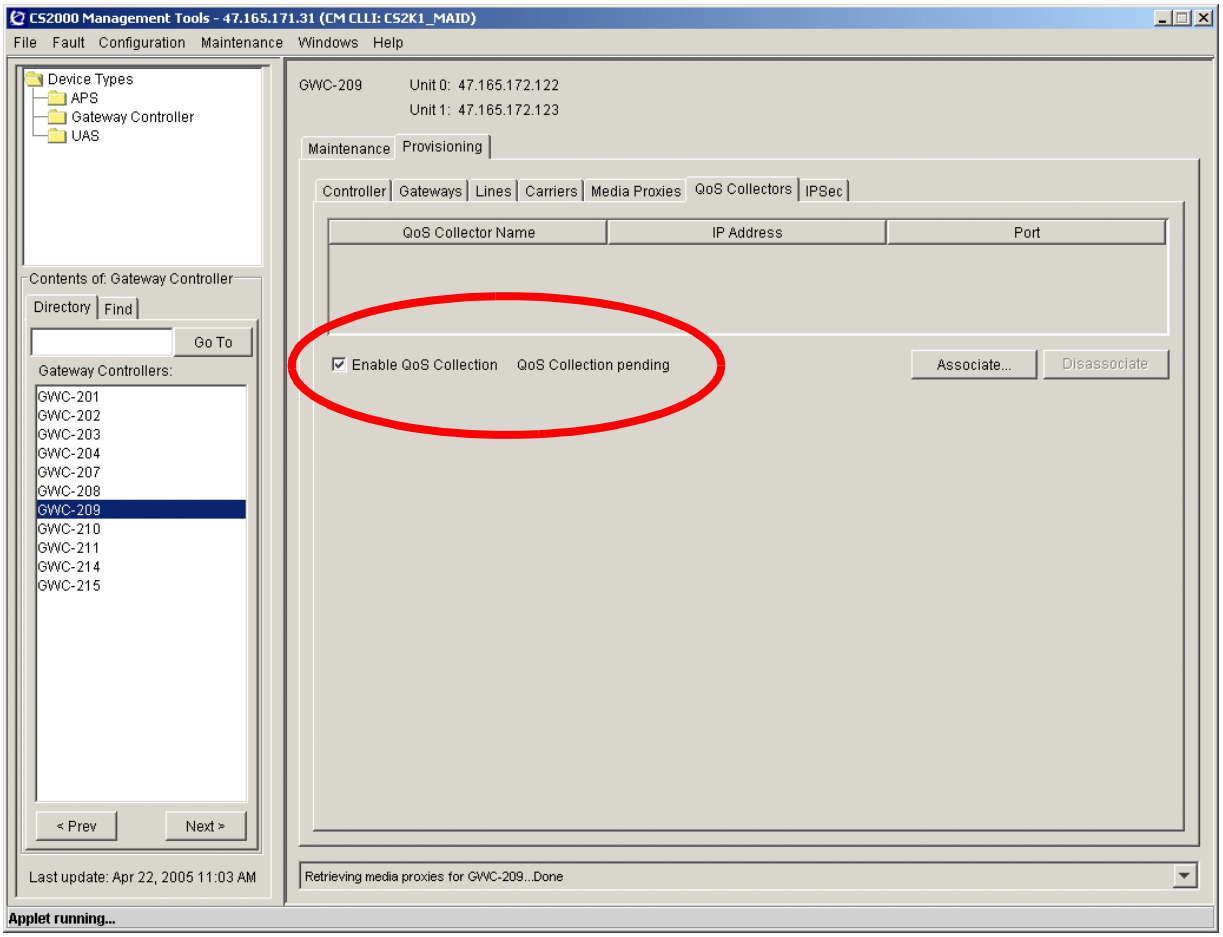


Figure 2 GWC element manager – Enabling/Disabling QoS

Extended QoS reporting is enabled/disabled from the CICM element manager (see the following figure). Extended QoS statistics will only be sent if a destination ip address and port-number have been datafilled on the CICM element manager global settings page.

Modifications to the extended QoS ip address and port number are picked up dynamically (within 2 minutes) and do not require a reboot.

To disable extended QoS reporting, both the extended ip address and port number must be deleted.

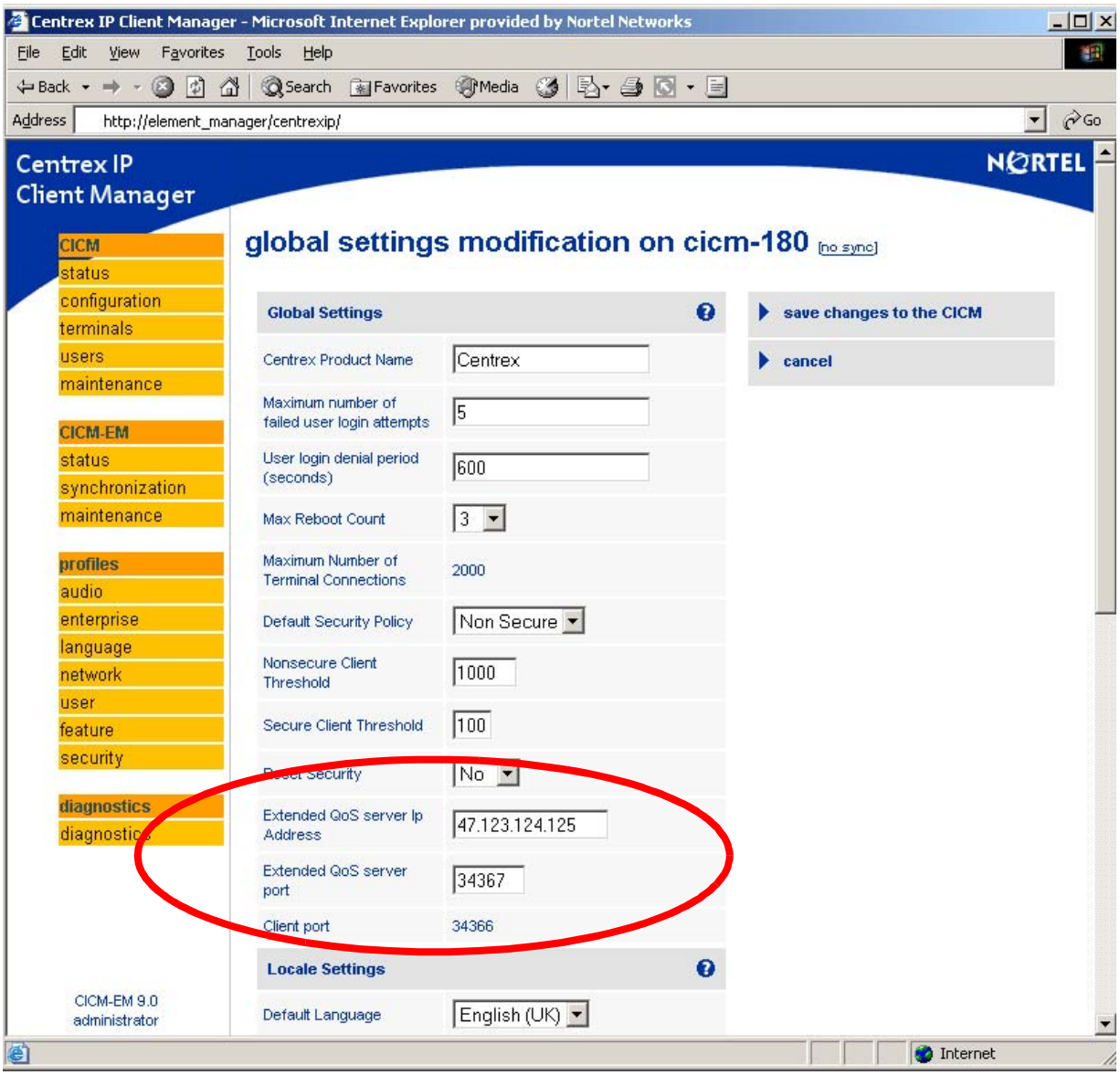


Figure 3 CICM element manager - Enabling/Disabling extended QoS reporting

1.2 Hardware Requirements or Dependencies

QoS Collector Application QCA

1.3 Software Requirements or Dependencies

Not Applicable

1.4 Limitations and restrictions

Terminal type	Version 1 QoS report supported		Version 2 “Extended” QoS report supported (Phase 2 terminals only)	
	Y/N	Minimum firmware version	Y/N	Minimum firmware version
i2001	Y	3.90	Y	3.90
i2002	Y	1.74	Y	3.90
i2004	Y	1.74	Y	3.90
i2007	N	N/A	N	N/A
i2033	N	N/A	N	N/A
I1001	N	N/A	N	N/A
I1002	N	N/A	N	N/A
I1006	N	N/A	N	N/A
I1007	N	N/A	N	N/A
I2210	N	N/A	N	N/A
I2211	N	N/A	N	N/A
I2212	N	N/A	N	N/A

Table 3 Supported terminal types and firmware requirements

Client type	Version 1 QoS report supported		Version 2 “Extended” QoS report supported	
	Y/N	Minimum version	Y/N	Minimum version
M6350	N	N/A	N	N/A
I2050	N	N/A	N	N/A

Table 4 Supported softclient types and version requirements

- Version 2 “Extended” QoS reports are only supported on Phase 2 terminals. Phase 1 terminals support Version 1 QoS reporting only. Please see Table 1 "QoS parameters reported" for a complete list of available statistics.

- Statistics which cannot be obtained from a client/terminal are reported upwards (to the GWC and extended QoS server) with a value of ‘0’.
- If the codec is renegotiated, QoS statistics will only be reported from the point that the new codec starts.

1.5 Interactions

Not Applicable.

1.6 Logs

Alarm	SubtractConnectionAckFailed
Component Id	CICM
Category	Communications
Description	Subtract ConnectionAck Failed
Specific Problem	SubtractConnectionAck::can't determine destination for message
Severity	NONE
Log Type	CustomerLog
Report Number	363
Event Type	INFO

Product = CS 2000

A00009375 & 9376 -- CICM Third-party Corrective Content Patching & CICM Selective Binary Component Patching

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

1.1.1 Overview

In pre-SN09 loads, all corrective content is delivered via the Maintenance Release (MR) process. In SN09, the MR process will be complimented with new functionality to allow the application of patches containing application, operating system or third party corrective content to the CICM or CICM-EM.

Patches will be built and released by Nortel CICM GNPS, and will be applied onto the CICM or CICM-EM, via the maintenance pages on the CICM-EM.

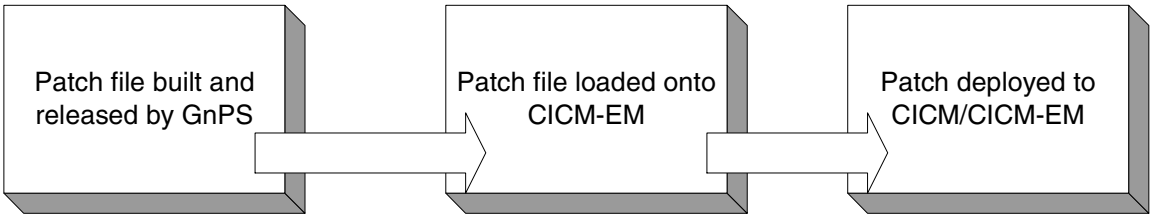


Figure 1 Patch Delivery Overview

1.1.2 Detail

The patching process will compliment the existing MR process by delivering corrective content quickly and efficiently in between the normal MR deliveries. From an end-user perspective the main differences will be as follows.

Maintenance Releases

- Will be delivered at regular intervals
- May contain a large number of corrective content fixes
- May contain a combination of application, operating system or third party corrective content.
- Will replace ALL application binaries (CICM/CICMEM software) on the system to which it is applied.
- The installation of an MR always requires at least one system restart.

Patches

- Will be delivered on an ‘as needed’ basis
- Will contain a single fix for a specific issue
- May contain application, operating system or third party corrective content. But typically not a combination.
- Will only replace application binaries / make other system image changes needed to deliver the corrective content.
- The installation of a patch will not always require a system restart.

1.1.3 Patch Delivery and Application

Nortel GNPS will deploy a patch to a customer in the form of a single patch file and a 128-bit MD5 checksum. The patch file and the checksum will be distributed separately in order to ensure the integrity of the patch file. The checksum of a file will be displayed upon the CICM EM web page once a

patch has been selected, the craftsperson may wish to confirm that the number shown is the same as that expected.

This md5 checksum system described in the last paragraph will also be in place for Maintenance Releases.

1.1.3.1 Patch Delivery

The patch file will be delivered to the customer either via electronic transfer or on physical media. The MD5 checksum will be delivered to the customer via e-mail or through publication on an externally accessible Nortel website.

Nortel has corporate wide guidelines on the categorisation and description of Corrective Content (CC). Regional Patch Solutions (RPS) is our interface to the criteria and practice.

RPS offers the PatchFeed tool for submission of CC and this will be used by GnPS to deliver patches to the Nortel website, customer drop-boxes etc. once the patch has been built.

The patch that PatchFeed takes is encapsulated in metadata before being sent on. This metadata is in addition to the metadata added to the CAB files themselves and serves to identify the patch; it's category, status and applicability conditions to RPS systems.

RPS defined categories for CC are:

- GEN--General content (mass deployment)
- EMG--Emergency content (accelerated mass deployment)
- ACT--Feature rich content (mass or specific Customer deployment)
- LTD--Limited content (specific Customer deployment)
- DBG--Debug content (specific Customer deployment)
- OBS--Obsolete content
- OBE--Obsolete Emergency content

Patches will fall under the GEN, EMG, LTD or DBG category, dependent upon the function of the patch in question.

The RPS statuses are:

- V--VO content (limited deployment)
- R--Released (mass deployment – depending on category)

Patches may be released with either of these statuses.

1.1.3.2 Patch Application

Upon receiving the patch file, the customer will transfer the file into the patching directory on the Master Element Manager (D:\CentrexIP\support\patches) via secure file transfer. Once there the patch can be applied to any suitable node that is under the management of the EM.

All patch management and installation will be carried out under the Element Manager Maintenance pages.

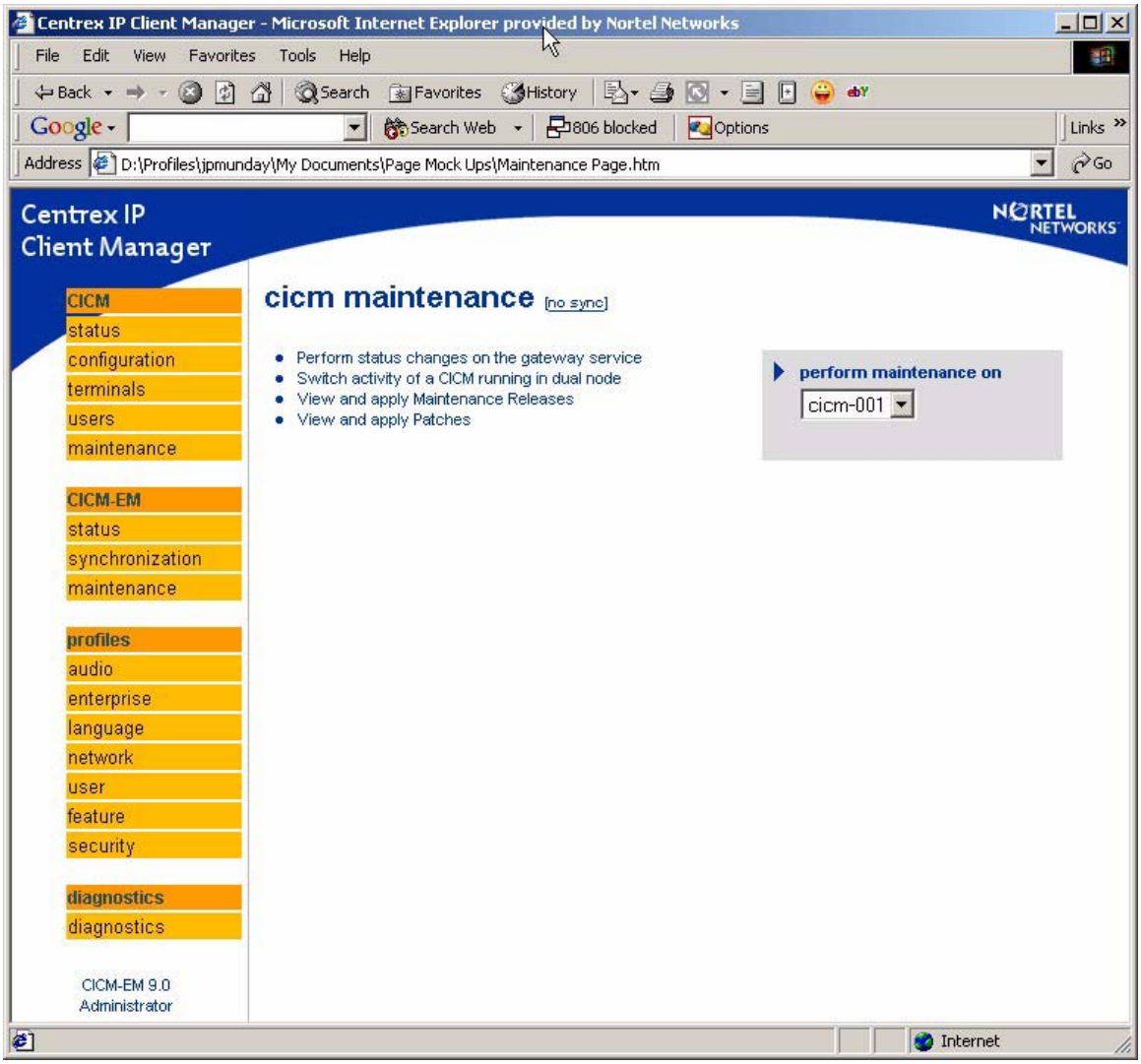


Figure 2 EM Maintenance Page

The diagram below shows the new web page layouts before and after the implementation of the SN09 patching features.

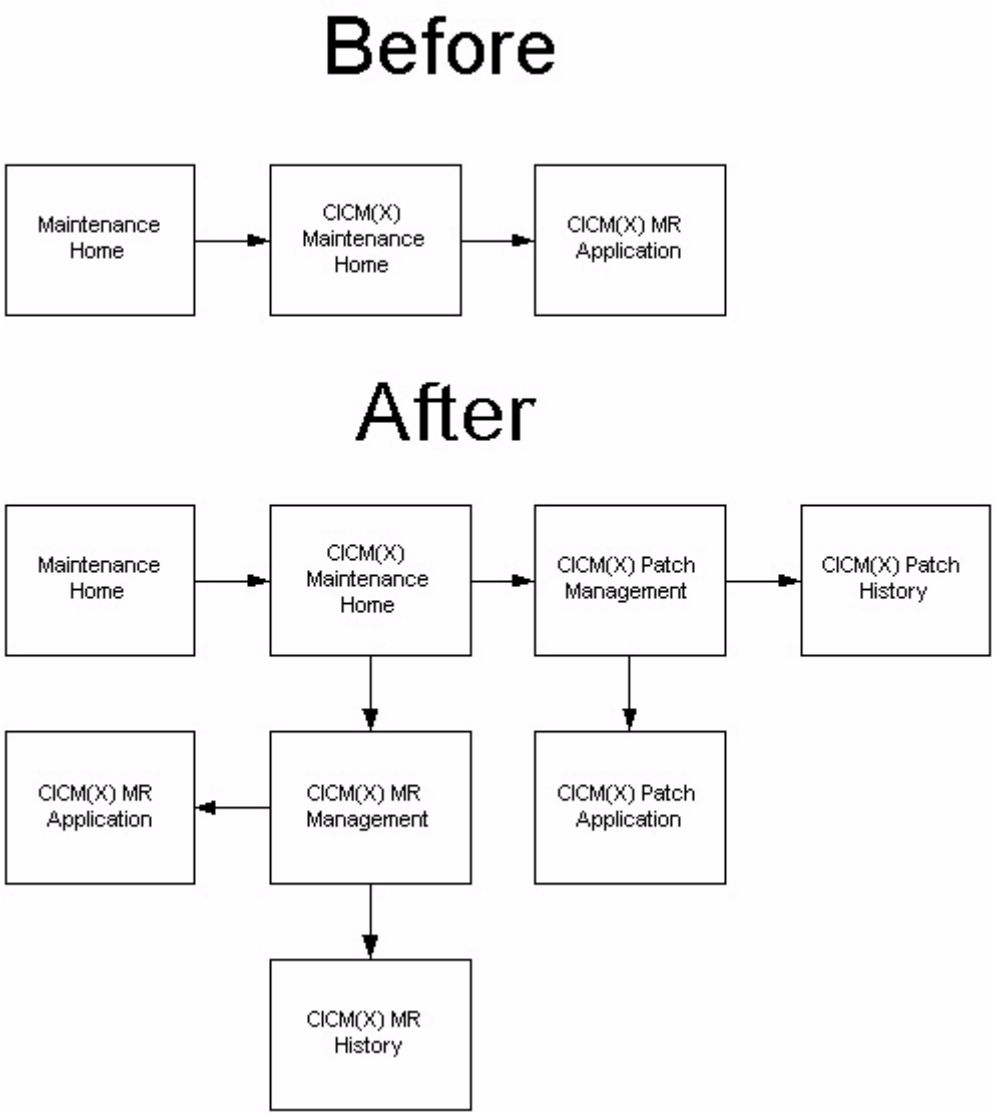


Figure 3 New Webpage access diagram

Once a user has selected the CICM node that they wish to carry out maintenance on they will be taken to the corresponding maintenance status page. The examples that follow show the maintenance and patching pages for a CICM, however the procedure and pages for applying a patch to a CICM-EM will be similar.

As with previous releases, the Maintenance Status page will display maintenance information for this CICM. In addition a new link will be available to allow access the patch management pages for a particular node on this CICM.

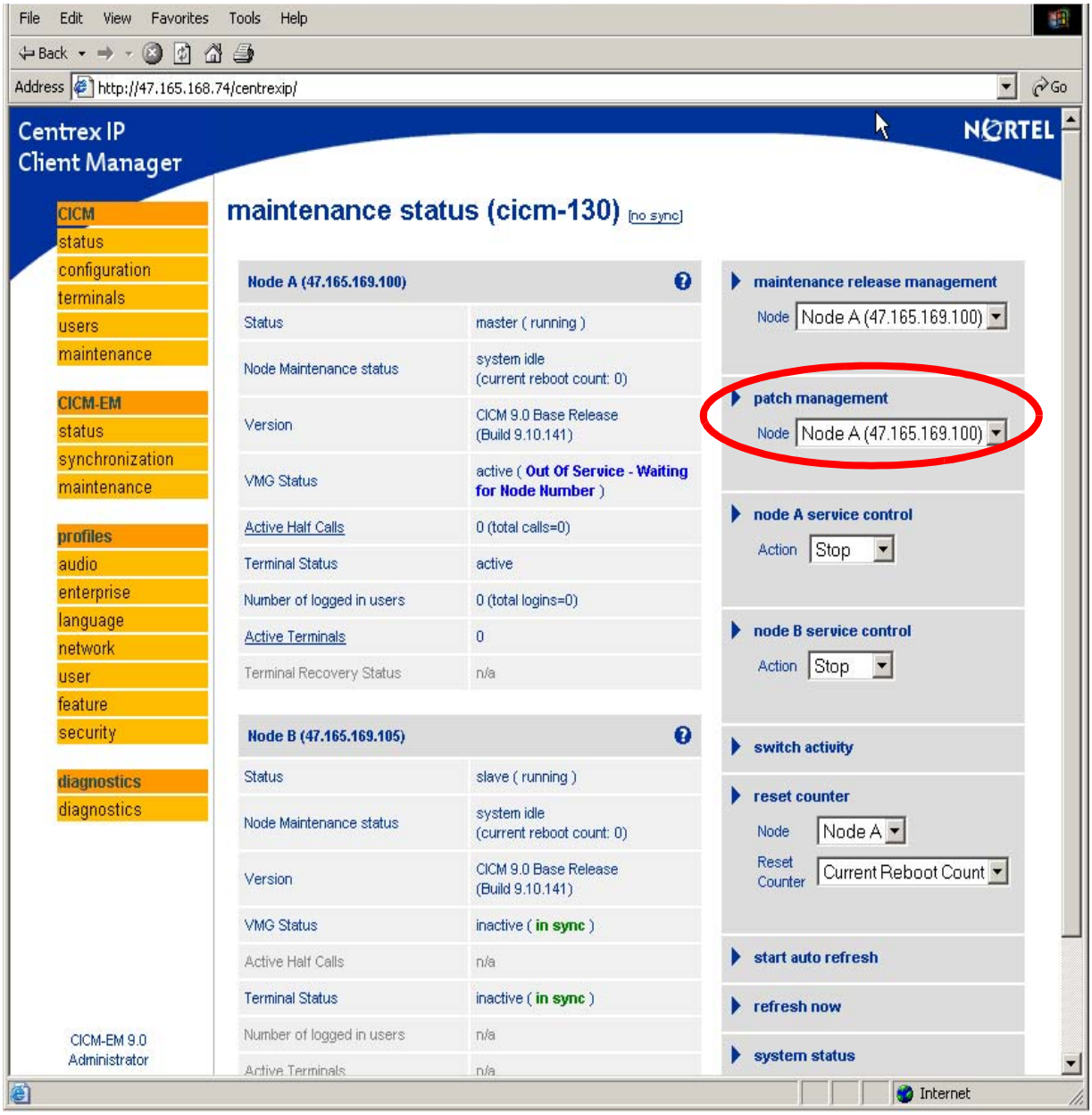


Figure 4 Maintenance Status Page

Selecting this link will take the user to the Patch Management page shown below…

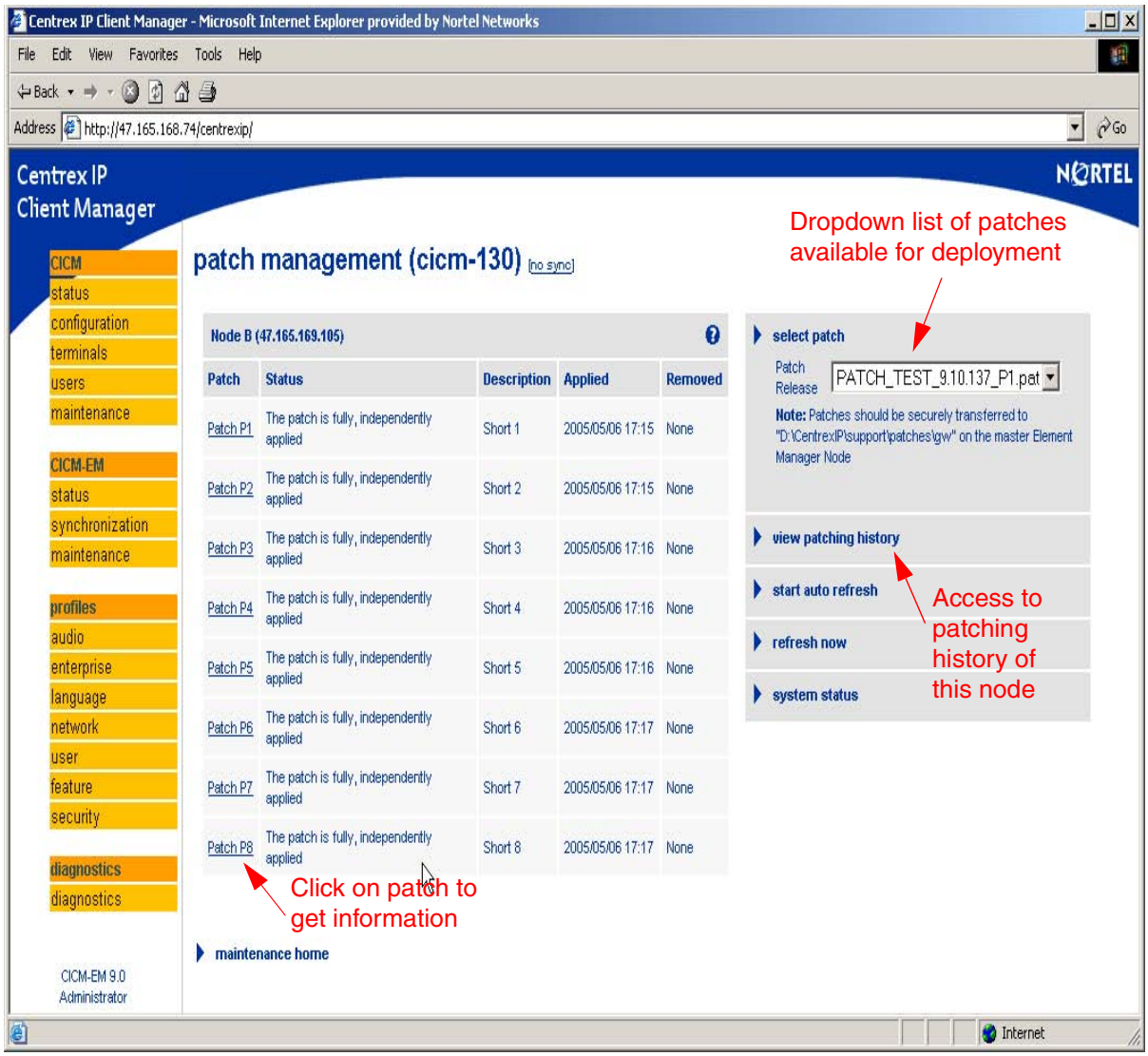


Figure 5 Patch Management Page

The patch management page shows a table of all patches that have been applied to this node **since the last Maintenance Release,** along with their application date and time, removal date and time (if applicable), a brief description and their status. This list is alphabetically ordered by Patch ID. Note that this Microsoft Windows convention of ordering will mean that patches 1, 2 and 10 will be ordered 1, 10 and 2. This ordering is independent of the order in which the patches were applied. To determine the application order the reader is referred to the paragraphs further down concerning the patch history page.

All patches will have a status of either ‘Applied’ – indicating that the corrective content of this patch is currently present on the system, ‘Removed’ – indicating that the corrective content of this patch has been removed by another patch or ‘Subsumed’ – indicating that the corrective content of the patch has been wholly subsumed by a later applied patch.

All patches copied into the patching directory on the Master Element Manager (D:\CentrexIP\support\patches) will be present in the ‘Select Patch’ dropdown menu.

When the user selects the patch to be applied from the dropdown list, they are taken to the patch application page shown below.

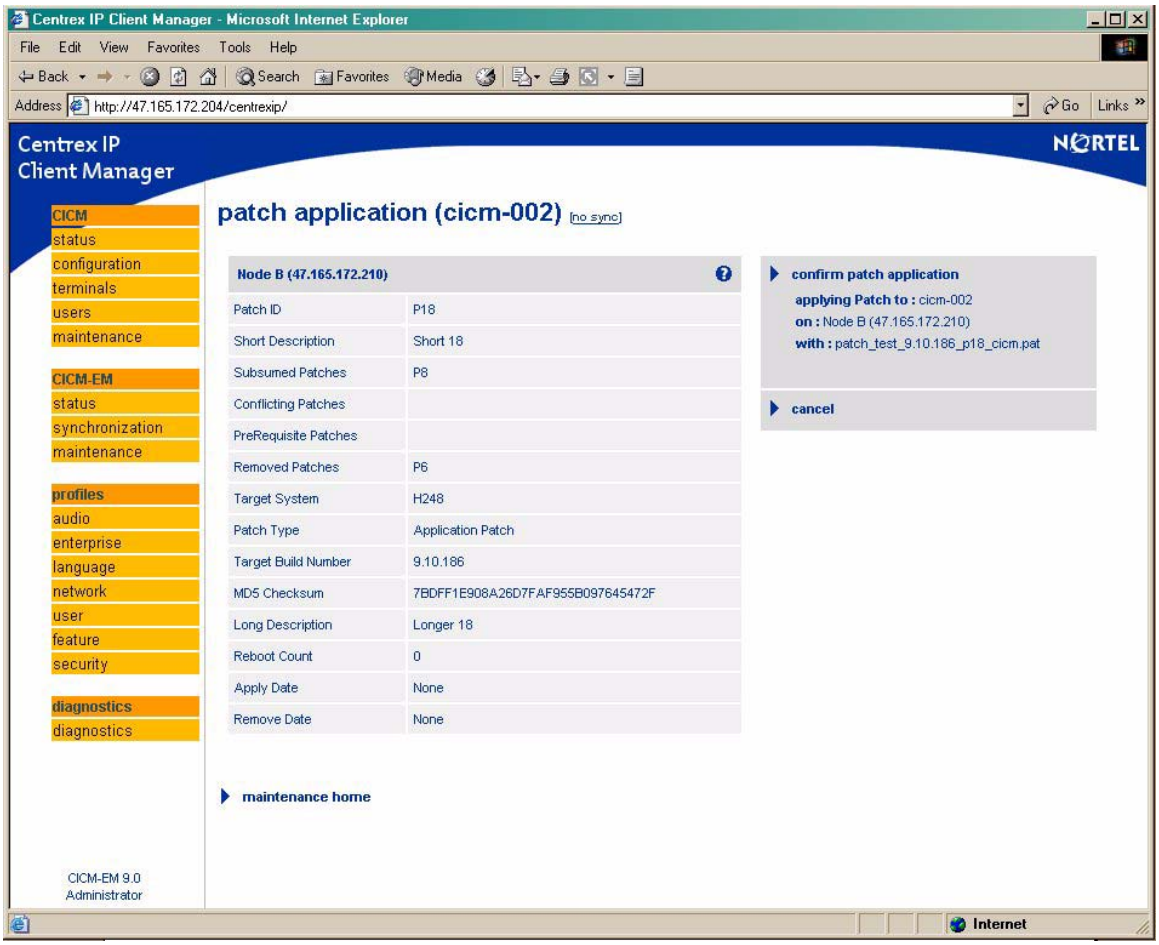


Figure 6 Patch Application Page

The Patch Application page will display all the details of the selected patch. Any conditions that would prevent this patch from being installed will be displayed in the right hand tab where the ‘confirm patch application’ link would normally appear.

If all Conflicts and Dependencies have been satisfied then the ‘Confirm Patch Application’ link will be enabled in order to allow patch application. Otherwise the link will be disabled along with details of why the patch cannot be applied, as shown.

The patch application page will display the following information.

Patch ID	The unique identifier for this patch
Target System	Indicates which type of node this patch can be applied to. This can be ‘H248 CICM’ or ‘CICM EM’. If this patch is not valid for this node type the ‘confirm patch application’ link will be disabled and replaced with a message indicating the conflict.
Target Build Number	Indicates the target release that this patch can be applied to. If this patch is not valid for this node type the ‘confirm patch application’ link will be disabled and replaced with a message indicating the conflict.
MD5 Checksum	The MD5 checksum of this patch file. The user should check that this checksum matches the checksum provided by Nortel for the patch file before applying the patch.
Description	A brief description of this patch
Conflicts	A list of patches with which this patch will conflict. Conflicts preventing installation will be shown in the right hand frame. *For more information see the section on Patch Version Control later.*
Dependencies	A list of patches upon which this patch is dependent. Dependencies preventing installation will be shown in the right hand frame. *For more information see the section on Patch Version Control later.*
Subsumes	A list of patches which are subsumed by this patch. Contained elements preventing installation will be shown in the right hand frame. *For more information see the section on Patch Version Control later.*
Removes	A list of patches which will be removed by this patch. Removed elements preventing installation will be shown in the right hand frame. *For more information see the section on Patch Version Control later.*
Reboot Count	The number of times the target system will reboot during the course of the patch application. See section “Selective Service Start-up and Shutdown” on page 1313.
Short Description	The ‘patch title’ giving basic information on what this patch does.
Longer Description	More detailed information released by GNPS providing technical information on the patch.

Once the target system and all conflict and dependency checking as been satisfied, it is the responsibility of the user to ensure that the checksum

displayed for the patch file is identical to the checksum provided by Nortel before applying the patch.

Once this is done, the patch can be applied by clicking on the ‘Confirm Patch Application’ link. The user will then be taken to the Maintenance Status page where the status on the patch installation will be displayed. Patches can only be applied to the Slave node of a CICM or CICM-EM pair. However, application to the Master is permitted if the Slave is unavailable. The user will be shown a warning message in this scenario.

Assuming that the patch application is successful, the patch will appear on the Patch Maintenance page with a status of ‘Applied’. The user can now run sanity on the system or test the functionality of the patch.

If the patch installation fails for some reason, the patch will remain unapplied and will not be added to the list of applied patches on the Patch Management page. An entry will not be added into the patching history page. If the patch application failed during consistency checking the system service will not have been nor will be affected. If the application failed whilst the patch was actually being applied maintenance action may then be required to return the node to full service. In the event of a patch application installation failure in this latter case, customers are strongly recommended to contact the next level of support.

If the user wishes to view more detailed information on a previously applied patch, they can click on the Patch ID on the Patch Maintenance page. This will display the patch information page shown below.

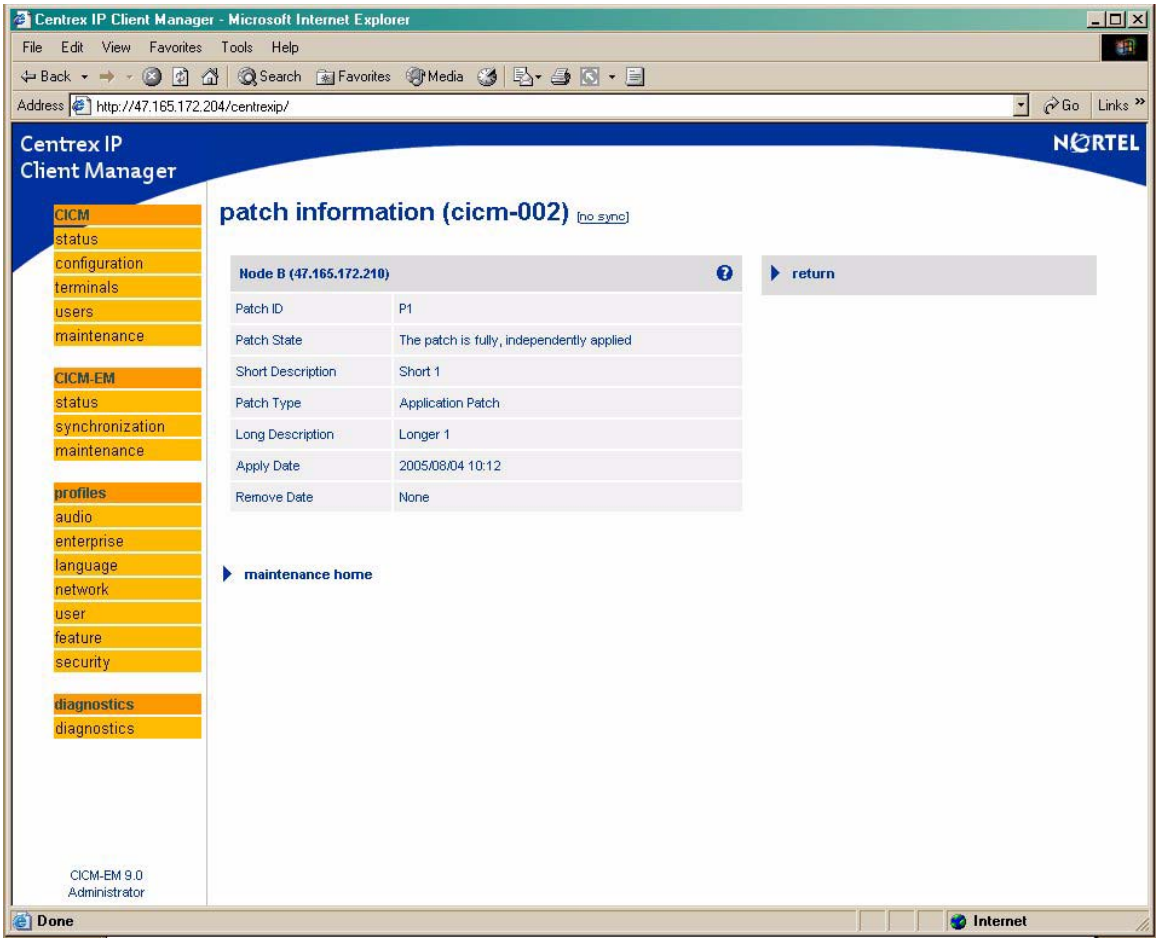


Figure 7 Patch Information Page

In addition, if a user wishes to view the patching history of a particular node, they can access the Patching History page via the ‘View Patching History’ link on the Patch Maintenance Page.

The Patching History page contains a list of all successful patching activity since the last Maintenance Release was applied. Details of patch applications, subsumations and removals will form this list.

A sample Patching History page is shown below.

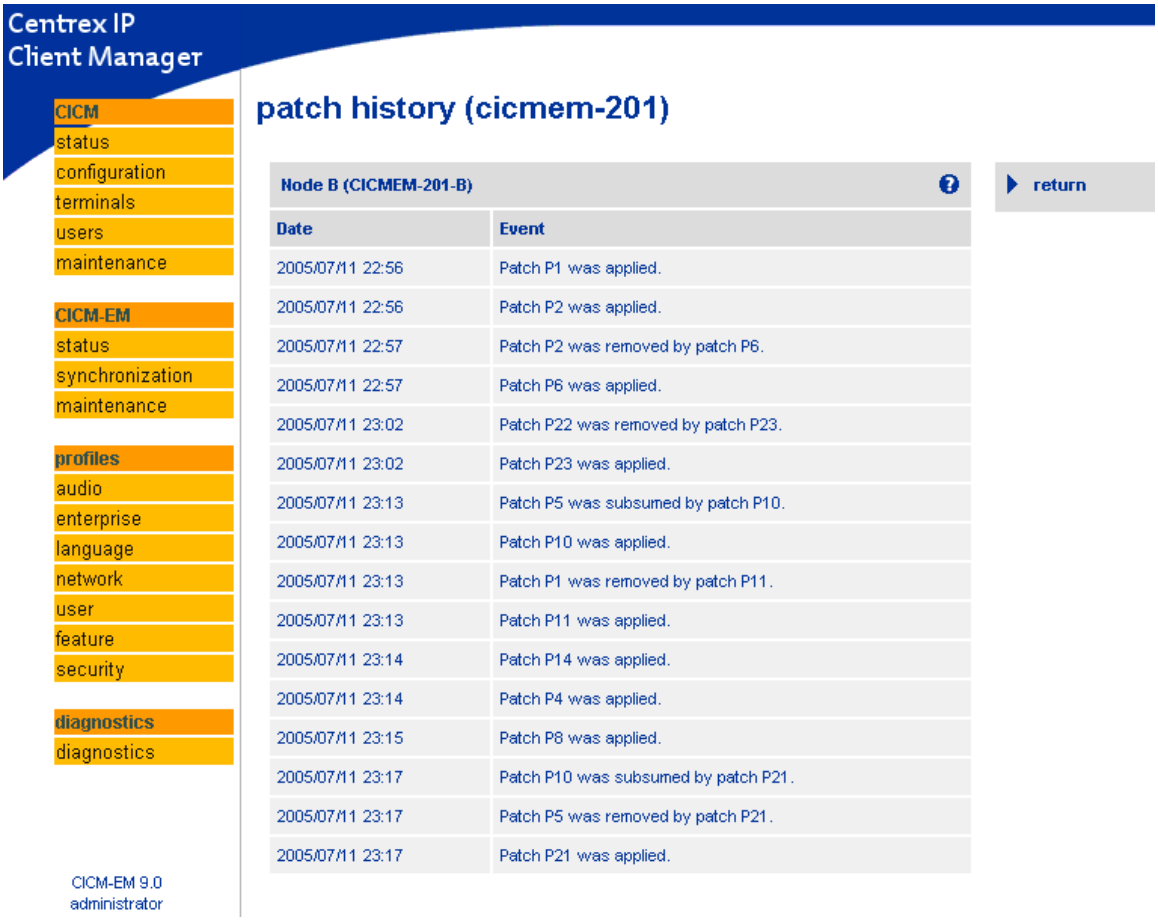


Figure 8 Patching History Page

When a Patch is not applied to the CICM or CICM-EM but it is in the removal list of a patch that was applied then the Patch History Page will still show the patch as removed (even though it may have never actually been applied). In this case the applied date field for the patch that was never applied will be “None”.

The possible states of patches are…

- The patch has been removed by another patch. A patch can not be re-applied to the system once it has been set to removed.
- The patch is fully, independently applied. The patch is independently applied and not subsumed by another. The ‘independence’ of a patch refers solely to subsumation i.e. whether it is contained in another patch or not. It does not have any bearing on the dependencies of the patch.
- The patch has been applied as a subsumation. This patch has been subsumed by another.

1.1.4 Maintenance Release Delivery and Application

Although the function of Maintenance Releases remains largely unchanged with the introduction of this feature, the addition of the Patching functionality will lead to changes in the deployment and application methods for installing an MR.

From SN09 Nortel GNPS will deploy Maintenance Releases to a customer in the form of a single MR file and a 128-bit MD5 checksum. The MR file and the checksum will be distributed separately in order to ensure the integrity of the Maintenance Release file.

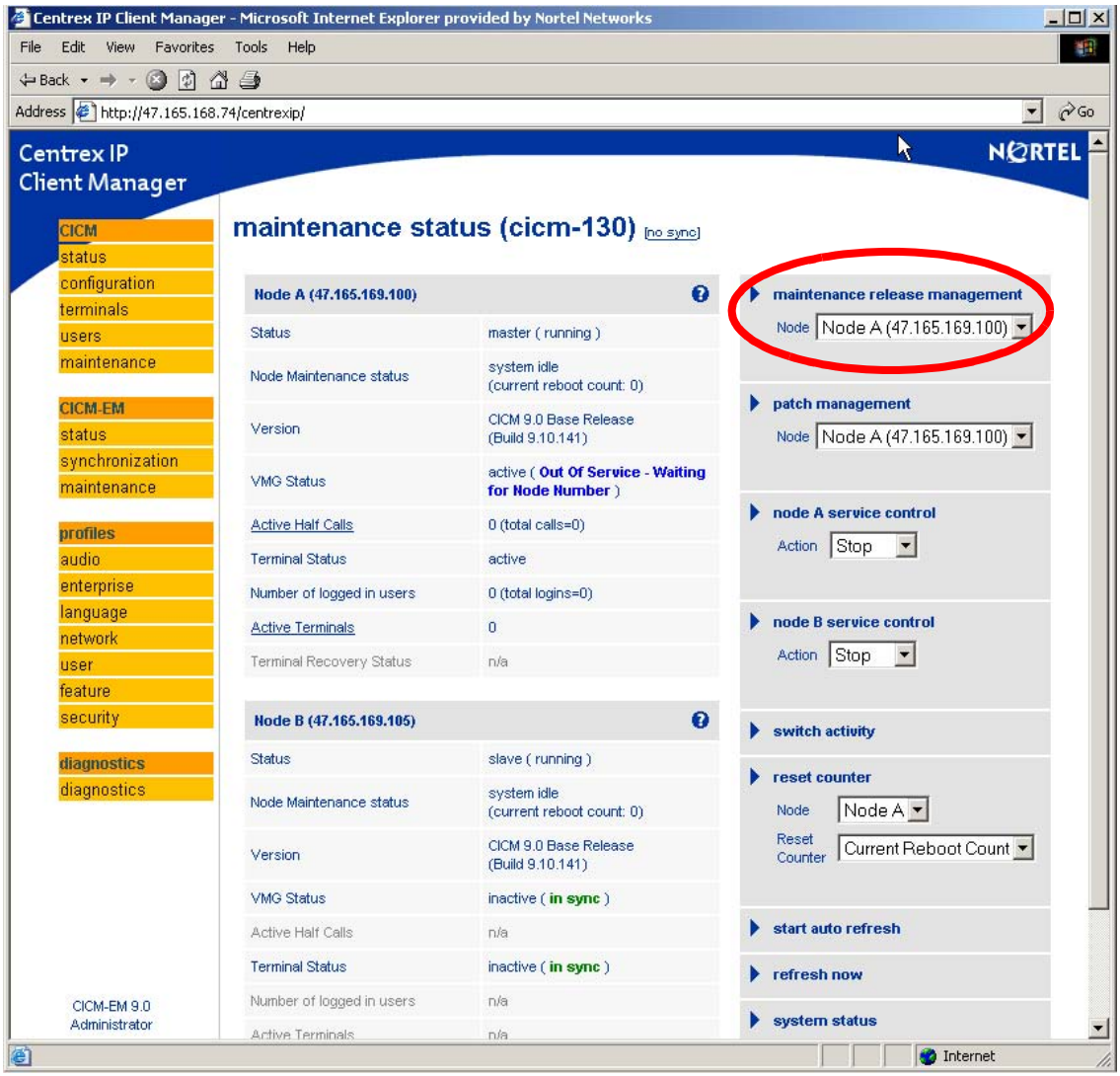


Figure 9 Maintenance Status Page

As with patches, the MR file will be delivered to the customer either via electronic transfer or on optical media. The MD5 checksum will be delivered to the customer either via e-mail or through it's publication on an externally accessible Nortel website.

Upon receiving the patch file, the customer will transfer the MR file into the Maintenance Release directory on the Master Element Manager (D:\CentrexIP\support\upgrades) via secure file transfer. Once there, the patch can be applied to any suitable node that is under the management of the CICM-EM.

From SN09, users will no longer be able to directly apply an MR from the main Maintenance Status page. Instead users will need to navigate to a new sub-Maintenance Release Management page from the main Maintenance Status page (see Figure 3).

The Maintenance Release Management page will display a table of all MRs that have been applied to this node along with their application time, date and status as shown below.

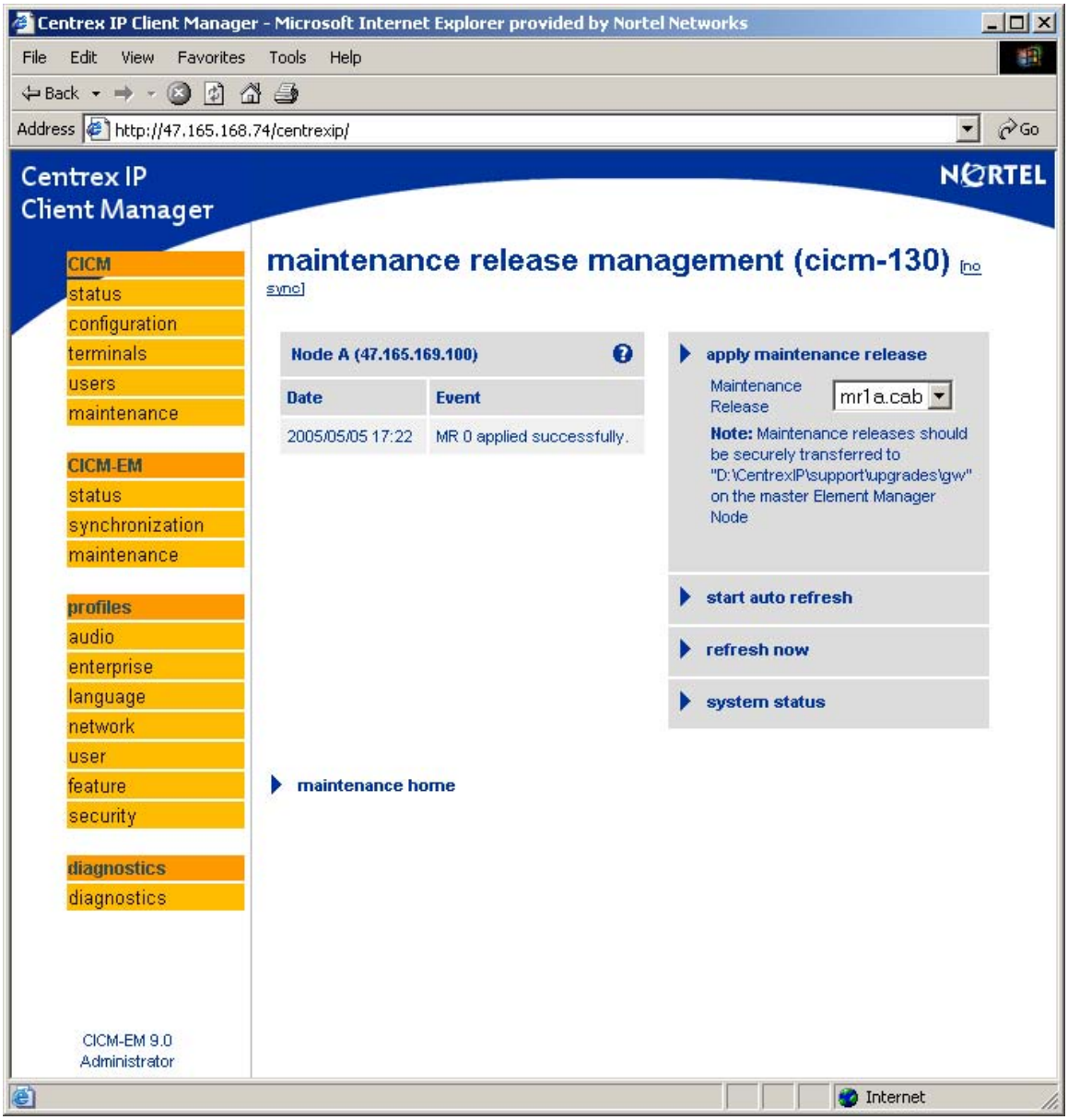


Figure 10 Maintenance Release Management Page

All MRs will have a status of ‘Applied’, since there is no way to remove an MR.

In addition, if a user wishes to view the patching history of a particular node, they can access the Patching History page via the ‘View Patching History’ link.

All Maintenance Releases copied into the MR directory on the Master Element Manager (D:\CentrexIP\support\upgrades) will be present in the ‘Select Patch’

dropdown menu. Once a user has selected the Maintenance Release to be applied from the dropdown list, they will be taken to the Maintenance Release Application page shown below.

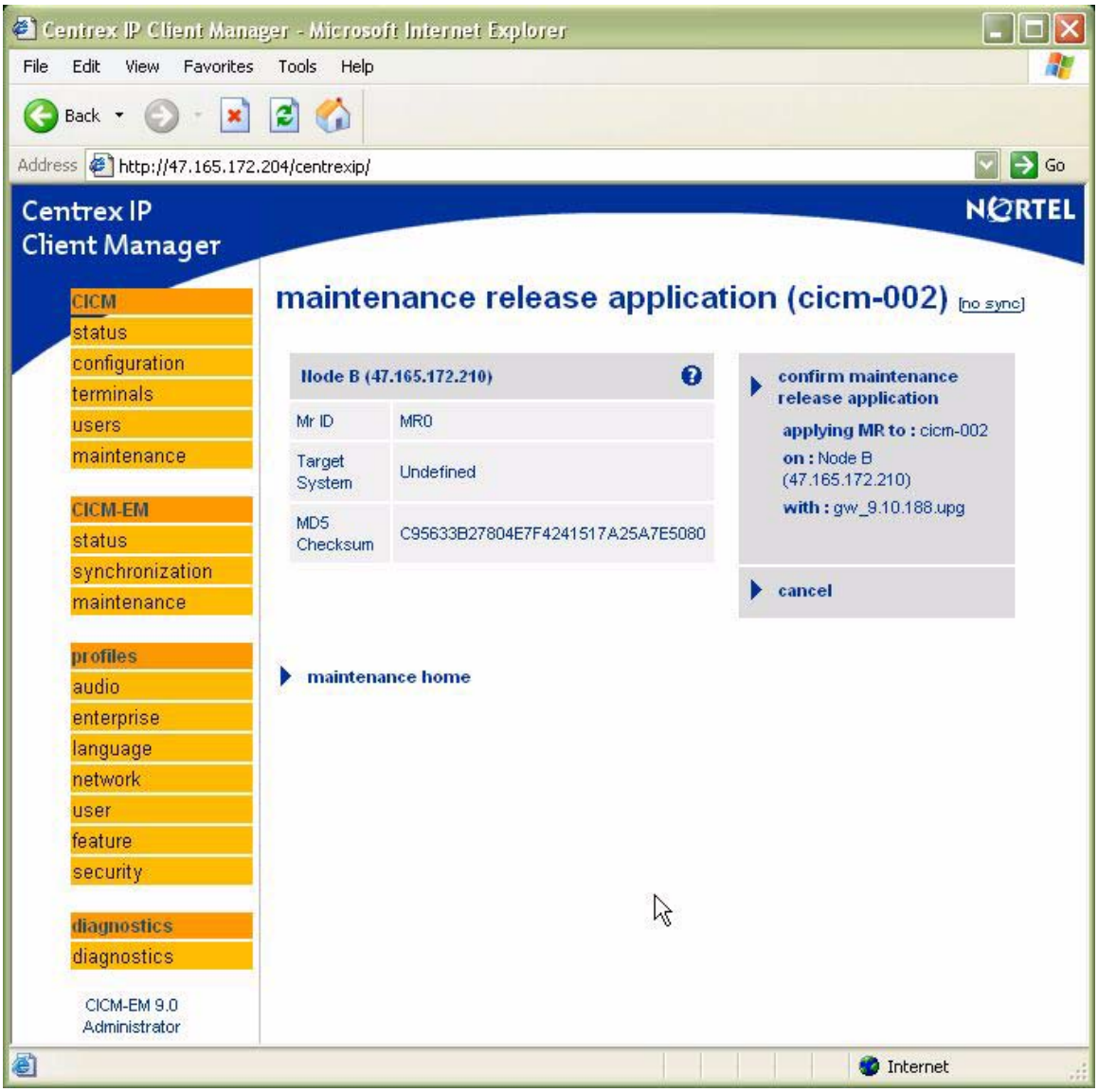


Figure 11 Maintenance Release Application Page

The Maintenance Release Application page will display all the details of the selected MR. If the selected node is of the correct system type and the MR has not already been installed, then the 'Confirm MR Application' link will be enabled in order to allow the application of the Maintenance Release. Otherwise the link will be disabled along with details of why the MR cannot be applied.

The Maintenance Release Application page will display the following information…

MR ID	The unique identifier for this MR
Checksum	The MD5 checksum of this patch file. The user should check that this checksum matches the checksum provided by Nortel for the Maintenance Release before applying the MR.
Target System	Indicates which type of node this patch can be applied to. This can be 'H248 CICM' or 'CICM EM'. If this patch is not valid for this node type it will be highlighted in Red.

It is the responsibility of the user to ensure that the checksum displayed for the patch file is identical to the checksum released for the patch by Nortel before applying the patch.

Once this is done, the Maintenance Release can be applied by clicking on the 'Confirm Patch Application' link. The user will then be taken to the Maintenance Status page where the status of the MR installation will be displayed. Assuming that the MR application is successful, it will appear on the Maintenance Release Management page with a status of 'Applied'.

If the MR installation fails for some reason, the MR will remain unapplied and will not be added to the list of applied MRs displayed on the Maintenance Release Maintenance page. As for patches, details concerning the failure will be generated in the debug log files.

In the event of a Maintenance Release installation failure, customers should contact the next level of Support.

1.1.5 Patch Version Control

The CICM and CICM-EM will follow an *independent* patching strategy. This means that as long each patch's rules for version control are satisfied…

- Customers can apply patches in any order they desire.
- Customers are not compelled to install *every* patch released by Nortel[1]

In order to allow this flexible independent patching strategy, whilst maintaining the overall sanity of the load content on the CICM and CICM-EM at all times, a patching version control system has been implemented.

This effectively defines what can and can not be applied to any particular CICM or CICM-EM. Overall load integrity and sanity is maintained by simply preventing incompatible content from being installed.

[1] Although customers should always follow the recommendation of Nortel CICM GNPS with regards to whether individual patches should be applied to in-service systems.

Patching Version Control is carried out by comparing records of what is currently installed on the system with information contained within each patch detailing its content and incompatibilities. If it is determined that the application of a particular patch would break one or more version control rules, then the 'Confirm Patch Application' link on the Patch Application page will be disabled, preventing the patch from being installed. In this instance, an the reason preventing the patch application will be given to the user so that corrective action can be taken.

Each patch will contain four lists defining its content, dependencies and conflicts as shown below.

Dependency List	This defines a list of patches that must be present on this node for this patch to be applied. If any of the patches contained within this list are not currently applied, then this patch cannot be applied.
Conflict List	This defines a list of patches which are incompatible with this patch. If any of the patches contained within this list are present on this node, then this patch cannot be applied. In addition, once applied, no patch contained within the conflict list of this patch can be applied without the removal of this patch first.
Subsumation list	This defines a list of all patches that are wholly subsumed (or contained) within in this patch. A patch can only subsume previously released patches. A patch which subsumes another patch contains fully the functionality of the previously released patch. Applying this patch will therefore also apply all the other patches contained within this list (if they are not already applied).
Removal list	This defines patches that will be removed by the application of this patch. Once applied, no patch contained within the removal list of this patch can be re-applied. Even if the patch has not been applied, the target system will not allow its application in the future.

When a patch is selected for application, the following simplified checks are carried out…

- The patch being installed must be of the correct type (CICM / CICM-EM) for the node it is about to be applied to.
- The build number of the target system must be that the patch is intended for.
- Each patch listed in the patch dependency list of the patch being installed must be presently installed on the system.
- None of the patches listed in the conflict list of the patch being installed may be presently installed on the system.
- None of the patches listed in the removal list of the patch being installed are present in the dependency lists of any of the currently applied patches.

- None of the patches listed in the content list of the patch being installed are present in the conflict or removal lists of any of the currently applied patches.

Only if ALL of the criteria above are met is the ‘Confirm Patch Application’ link enabled and the patch can be installed.

Once patch installation has been started ALL patches present in the Content list of the patch will be installed. Note that it is not possible to selectively install only some of the content of a patch.

Once a patch has been installed, the following changes are made to the patch content table on the node which the patch was applied to.

- All patches listed in the Content list of the patch applied are added to the list of applied patches with a status of 'Applied'.
- Any patches listed in the Removal list of the patch applied, that are present in the Applied Patch Table, will be changed to a status of 'Removed by <Patch ID>'.

In additional, the Dependency, Conflict, Content and Removal lists of the installed patch are stored on the node on which the patch was installed to assist with the version control checking of future patches.

1.1.6 Selective Service Start-up and Shutdown

An advantage the new patching functionality provides over the Maintenance Release functionality is that the application of a patch will not necessarily require a restart of the node that it is applied to, and may even be able to maintain service during its application.

Depending on the corrective content being delivered, the patch application software has the ability to apply a patch with either…

- A Full Node Outage (and loss of redundancy)
- A Partial Node Outage
- No Node Outage

The level of Service Outage required will always be defined by the patch. Patches that require a Full Service Outage will have the ‘Reboot Count’ field set to a non-zero number to indicate that as part of the patch installation the node will be rebooted and therefore be unavailable for a period.

Patches that have the ‘Reboot Count’ field set to nought will either require a Partial Service Outage or No Service Outage.

In the case of a patch that will need a partial service outage during installation, the exact level of the service outage that will be encountered, along with

exactly what service impact the customer can expect will be defined in the release notes of the patch by Nortel GNPS.

It is the responsibility of the craftsperson applying the patch to read and fully understand what impact the installation of a specific patch will have on an in-service system. And it is recommended that the supported patch installation procedure is always used when applying patched to in-service sites (see section 2.1.8 on Patching Procedure)

1.1.7 Patching Procedure

The following is the basic procedure for applying a patch to a pair of CICM nodes.

1 Take a system backup of the nodes being patched using the EM backup tool

2 SWACT call processing to Node A

3 Apply the patch to node B – should the patch installation fail, please stop and contact the next level of Support.

4 SWACT call processing to Node B

5 If possible verify the patch functionality and system sanity. If a problem is found, stop and contact the next level of Support.

6 Apply the patch to Node A – should the patch installation fail, please stop and contact the next level of Support.

7 SWACT call processing to Node A

8 If possible verify the patch functionality and system sanity. If a problem is found, stop and contact the next level of Support.

9 Patch installation is complete.

The following is the basic procedure for apply a patch to a pair of CICM-EM nodes.

1 Take a system backup of the nodes being patched using the EM backup tool

2 SWACT the CICM-EM if necessary so that Node A is the Master

3 Apply the patch to node B – should the patch installation fail, please stop and contact the next level of Support.

4 SWACT the CICM-EM so that Node A is the Master

5 If possible verify the patch functionality and system sanity. If a problem is found, stop and contact the next level of Support.

6 Apply the patch to Node A – should the patch installation fail, please stop and contact the next level of Support.

7 SWACT the CICM-EM so that Node A is the Master

8 If possible verify the patch functionality and system sanity. If a problem is found, stop and contact the next level of Support.

9 Patch installation is complete.

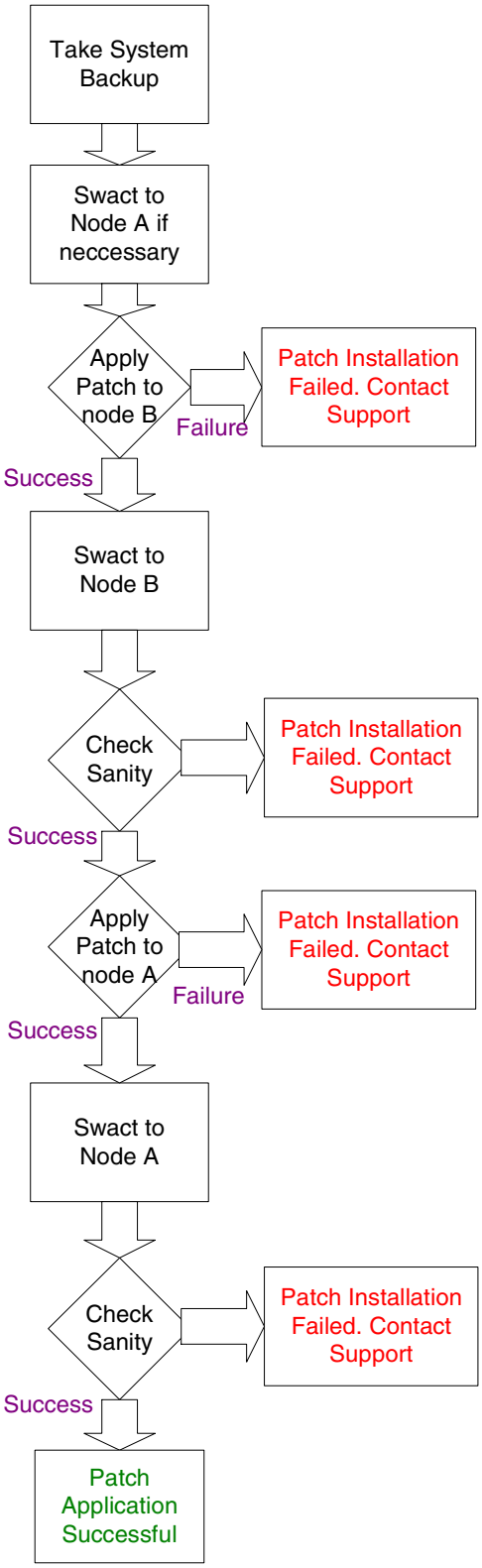


Figure 12 Patch Procedure

1.1.8 Maintenance Release Interaction with Patching

The web interface for Maintenance Release applications has been modified slightly. However from a functional point of view Maintenance Releases will be released and applied in exactly the same manner to the way they were before this feature was implemented.

The only minor exception is that from SN09 Maintenance Releases will be released with a checksum that should be checked to ensure integrity before application.

Maintenance Releases replace all application binaries on a system and apply all OS and Third Party Content up to a recognized and supported level (which is defined by the MR version).

An MR has no dependencies on the patch state of the target system before it is applied, since it is about to overwrite all content. Therefore an MR has no dependency or conflict lists and carries out no version checking against the current patch state before application. However, verification of the target type (CICM/CICM-EM) and upgrade path between build numbers is carried out.

Since a Maintenance Release overwrites all previous software versions, the record of all previous patches applied to this system will become irrelevant. For this reason, one impact of the application of a Maintenance Release is that it will erase the list of all currently applied patches. The content of this system is now defined by the MR version.

Normally the functionality of all the currently released patches will have been incorporated into a Maintenance Release. So although the record of applied patches has disappeared, the content of those patches will still be present on the system after the MR has been installed. A complete record of the content of a Maintenance Release, including all patches that it subsumes will be listed in its Release Notes of the Maintenance Release.

The current patch level of any system should be considered to be the MR version *plus* the patches listed in the applied patch list.

1.2 Hardware requirements

The SN09 Patching features introduce no new hardware dependencies or requirements.

The SN09 load is supported on:

- Motorola 5370 CPU cards
- Motorola 5385 CPU cards

1.3 Software Requirements or Dependencies

The Third Party Corrective Content Patching and Selective Binary Component Patching features are introduced in the SN09 CICM release. This load level must therefore be installed on any CICM-EM being used to apply a patch and on any CICM / CICM-EM that is being patched.

1.4 Limitations and restrictions

These features will only deploy Patches and Maintenance Releases built and released by Nortel CICM GNPS. Deployment of no other Patch or Maintenance Release files will be supported.

1.5 Interactions

This feature will modify the delivery of Maintenance Releases both by the inclusion of a Checksum for integrity checking and by the implementation of changes to the MR application web pages on the EM.

2: Configuration for A00009375 & 9376

2.1 Data schema (DS)/ MIBs

This feature will utilise two areas of the Windows Registry for the storage of information relating to status of installed patches and maintenance releases on this node.

Table 2: MIB entries

MIB name (registry key etc)	Description (including backwards compatibility)
hklm\system\currentcontrolset\services\cxipboot\data\patches	Storage area for patch information
hklm\system\currentcontrolset\services\cxipboot\data\upgrade	Storage area for maintenance release information

2.2 Operating system parameters (OP)

No Operating System Parameters will be changed by this feature, unless of course by the deployment of an OS patch. In which case details of the Operating System Parameters changed will be in the Release Notes of the patch concerned.

2.3 Alarms (AL)

No new alarms will be raised as part of this feature.

2.4 New/modified filesystem directories (FS)

Several new directories will be required for this feature.

Table 5: directories

Directory name	Location	Function
D:\CentrexIP\support\patches	CICM-EM	Location for patch files to be written ready for installation
D:\CentrexIP\support\upgrades	CICM-EM	Location for Maintenance Release files to be written ready for installation
C:\cxipinstall\???????	Node being Patched	Temporary area for unpacking patch and maintenance release data ready for installation

2.5 Command interface (CI)

A Command Line Interface will be provided for use by GNPS to assist in the removal of partially applied patches. However this interface will not be available for use by customers and as such the details of its functionality are beyond the scope of this document.

2.6 Software optionality control (SOC)

This feature is available on all CICM and CICM-EM platforms running SN09 or later.

2.7 Licensing

This feature will utilise MD5 checksums, which require no licensing. No other Third Party licensed software was used in the development of this feature.

2.8 References

A00005987 CxipRestore Tool

Product = CS 2000

A00009443 -- T.38 Annex D for NGSS

Functional Description

1: Applicable Solution(s)

PT-IP, CHS

1.1 Description

1.1.1 Overview

The main part of this activity provides support for H.248 T.38 Annex D interworking with SIP. This functionality is only available if both the remote MTA and SIP server support T.38 Annex D. A new provisioning flag **T.38 Annex D Supported** is added to the remote server option list to indicate that the remote server supports T.38 Annex D.

The call scenarios covered by this feature are described by ITU-T T.38 Annex D, specifically section D.2.2.4 - Voice and facsimile connection.

This activity intends to provide T.38 Annex D interworking support for SIP with H.248 PVG on the local side. For this feature to work, the Gateway controller must have T.38 enabled in the network codec profile provisioning, the H.248 GW PVG must support T.38, and the **T.38 Annex D Supported** flag must be enabled in the NGSS provisioning remote server option page. If so, then upon fax detection, a switch over is performed from G.729 (or G.711) to T.38 codec.

The switch-over is performed using an existing mechanism based on sending a re-Invite message with the new codec in the SDP. If the offer is accepted, the call switches to T.38 mode once the re-Invite sequence completes.

In case that a switch attempt is rejected by either end, an attempt will be made to preserve the call by switching to G.711 codec.

This feature is done in parallel with SN09 activity A00009294 which is responsible for the connection broker changes in the GWC.

The second part of this feature provides ability to prevent automatic upspeed from G729 to G711 by 248 PVG on fax detection as is the default PVG behavior. A new field **Re-Invite for Voice Band Data** is added to enable this functionality. If this field is enabled, the PVG will not auto upspeed to G711 but send a Re-Invite upon fax detection, to switch either to G711 codec or to T.38 if **T.38 Annex D Supported** is provisioned. Note that if the original media for the call was set up using G711 codec, the new field has no effect, and the call behavior is dependent only on whether the **T.38 Annex D Supported** is enabled or not, as described above.

1.1.2 Scenarios covered by this activity:

There are 2 basic T.38 scenarios covered by this feature, as illustrated in the following figures. Figure 1 shows a scenario in which PVG detects the T.38 tones and initiates the switch. Figure 2 shows a scenario in which T.38 tones are detected by the Cisco/MCS which initiates the switch to T.38.

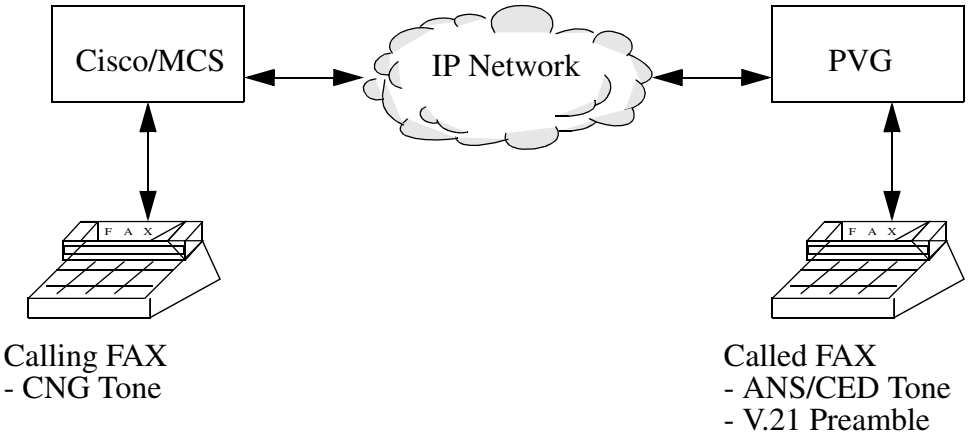
Note that for the T.38 call scenarios covered by this feature it does not matter which side originated the original voice call, but which gateway sends the T.38

tones (emitting gateway) and which gateway (receiving gateway) detects the tones and initiates the switch. For this feature, it is always the receiving gateway that initiates the switch.

The call scenarios that use the field **Re-Invite for Voice Band Data** are very similar to the T.38 call scenarios discussed here. If the **Re-Invite for Voice Band Data** is provisioned, but **T.38 Annex D Supported** is not, then the call switches to G.711 codec upon fax detection exactly in the same fashion as described below for T.38. If both fields are provisioned, PVG end will attempt to switch first to T.38, and if the attempt is rejected by the far end which does not support T.38, PVG will send another Re-Invite to switch to G.711.

1.1.2.1 T.38 fax calls originating from SIP/NGSS and terminating at PVG.

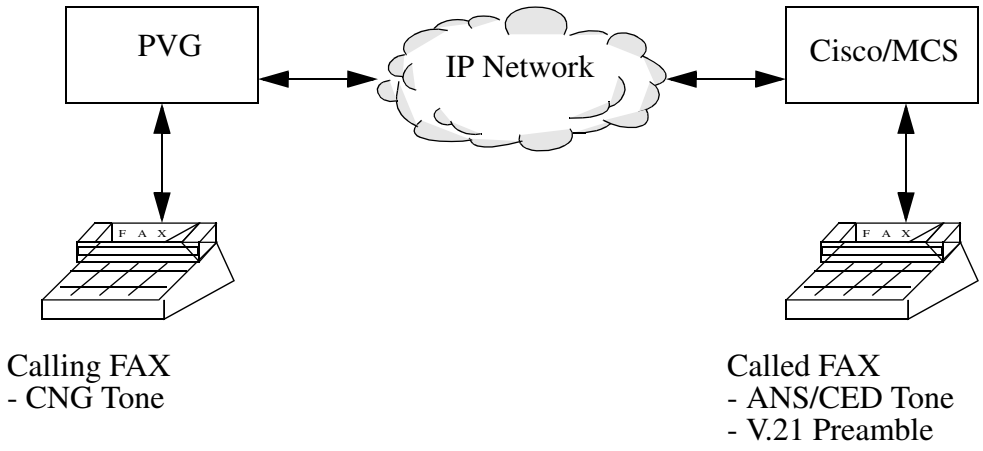
Figure 1



- A SIP Invite is sent to the CS2K by the CISCO/MCS requesting a voice connection.
- A voice connection is then established.
- Upon detection of fax tone the receiving gateway, PVG, it sends a V.21 notification to CS2K.
- CS2K then sends a SIP Re-Invite request to the emitting gateway (with the same Call-ID as the already existing voice connection) for a T.38 facsimile connection.
- Upon completion of the facsimile call establishment, the T.38 fax call proceeds with a T.38 V.21 flags indicator packet.

1.1.2.2 T.38 fax calls originating from PVG and terminating at SIP/NGSS.

Figure 2



- For calls originating from the PVG end, a SIP Invite is sent to the CISCO/MCS requesting for a voice connection.
- A voice connection is established.
- A V.21 notification is received by the CISCO/MCS.
- It sends a re-invite to the originating side PVG, and the switch-over to T.38 occurs.

1.1.3 New functionality provided by this feature

1.1.3.1 Provisioning

Two new provisioning fields are added by this feature.

A new boolean provisioning flag **T.38 Annex D Supported** is added to the NGSS option list on the remote server provisioning web page to indicate that the remote server supports T.38 Annex D. This flag has to be set to 'Y' to enable this functionality. It should be set to 'Y' only if the remote SIP server supports T.38 Annex D.

A new boolean provisioning flag **Re-Invite for Voice Band Data** is added to the NGSS option list on the remote server provisioning web page to prevent automatic upspeed from G729 to G711 by 248 PVG on fax detection as is the default PVG behavior. This flag has to be set to 'Y' to enable this functionality. It has no effect on non-PVG gateways.

1.1.3.2 Proprietary header for the SIP INFO message

A SIP info message is used to tandem the T.38 scan request to the other CS2K. It contains a new proprietary Nortel SIP header to indicate to the other CS2K that it should scan for T.38 tones.

The new header is defined as follows:

x-nt-action-req = "action" HCOLON action-value *(";" action-value)
action-value = "38annexd" / “vbdannexd”

The following is an example of the SIP INFO message using this header:

INFO sip:9192461814@MGCA;user=phone SIP/2.0
Via:SIP/2.0/UDP MGCA;maddr=47.174.75.160
To:<sip:9192461814@MGCA;user=phone>
From:<sip:2461817@MGCA;user=phone>
Call-ID:0111.5119-22-19-49-11.68@MGCA
CSeq:1 INFO
X-nt-action-req: t38annexd
Content-Length:0

If a SIP info message containing the above header with action value of ‘38annexd’ is received by an NGSS in any CS2K, it should have the same meaning as if the **T.38 Annex D Supported** was provisioned on the NGSS. The CS2K should start scanning for T.38 fax tones and initiate the switch to the T.38 codec if detected. In a similar fashion, a SIP info message containing the above header with action value of ‘vbdannexd’ received by an NGSS in any CS2K should have the same meaning as if the **Re-Invite for Voice Band Data** was provisioned on the NGSS.

1.1.3.3 Call preservation in case of codec switch rejection.

In case that the remote SIP server rejects a re-Invite message initiating the switch to T.38 by sending a 488 Not Acceptable Here response, the CS2K will attempt to preserve the call by sending another re-Invite with G.711 codec offer. If this offer is accepted, the call will be preserved.

In case that the PVG rejects the attempt to switch to T.38 codec initiated by the remote server re-Invite, the CS2K will respond with 488 Not Acceptable Here message. It is up to the remote SIP server to initiate a switch back by sending another offer in the re-Invite.

1.1.4 Supported Call Flows

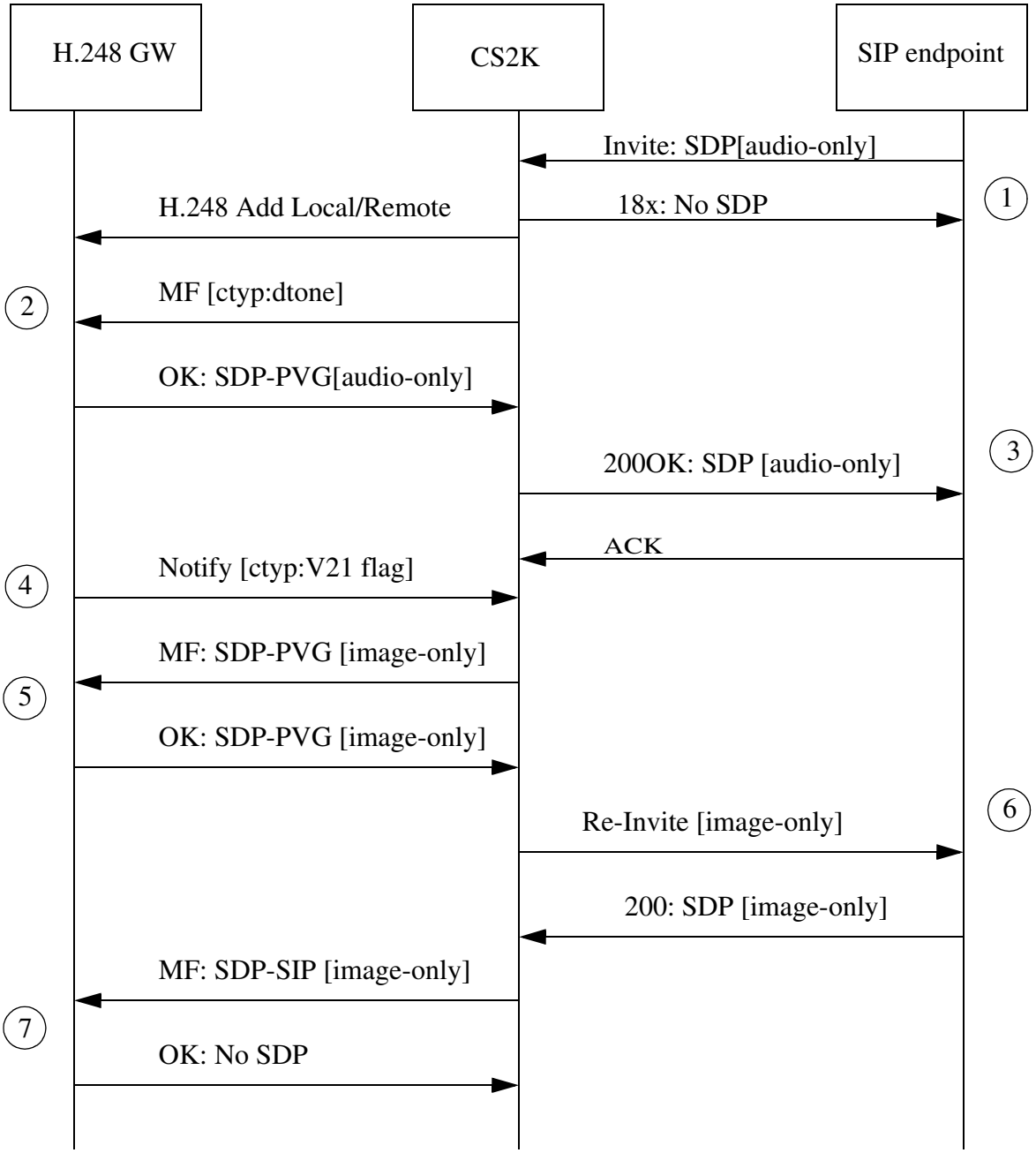
Description of T.38 Annex D functionality is provided via call flows provided in the following figures. The description of the first call flow is given in detail and may be applied to other subsequent call flows.

1.1.4.1 Basic Call Scenario: SIP to PVG interworking.

When the call is originated from the CISCO/MTS SIP endpoint:

In this scenario, the voice call is call originates from CISCO/MTS in the form of SIP INVITE sent to CS2K. Since the **T.38 Annex D Supported** is enabled in the NGSS for the remote server, during the voice call setup the PVG is asked to scan for fax tones. A voice call is established successfully, and then PVG detects a V.21 flag. V.21 Fax notify is sent from PVG which triggers an attempt to change the codec from G.711 or G.729 to T.38 communicated to the remote end via a re-Invite sequence.

Figure 3 T.38 Calls originating from CISCO/MTS and terminating at PVG on CS2K



Note 1: After receiving an INVITE from the SIP endpoint, a voice call is established. If in the Gateway controller configuration, T.38 is enabled in the network codec profile provisioning the ephemeral is added, and the PVG is asked to choose from m = audio $$$ m = image $ udptl t38.

Note 2: If the **T.38 Annex D Supported** flag is enabled on the remote server, the H248 GWC requests the PVG to scan for all events on the ctyp/dtone package.

Note 3: The PVG replies with the intersection of the PVG capability and the offer from SIP Invite, which is sent to the remote SIP end point. At this point voice call is established.

Note 4: The PVG then reports any detected ctyp/dtone event to the GWC.

Note 5: Upon detection of a CNG or a V.21 flag the GWC will send a modify to the PVG with the local descriptor m=image $ udptl t38.

Note 6: CS2K sends this image only SDP to the remote SIP end point in Re-INVITE message.

Note 7: Upon receipt of SDP(T.38) from remote SIP end point, CS2K sends a modify indicating the offer has been accepted. At this point T.38 fax call is established.

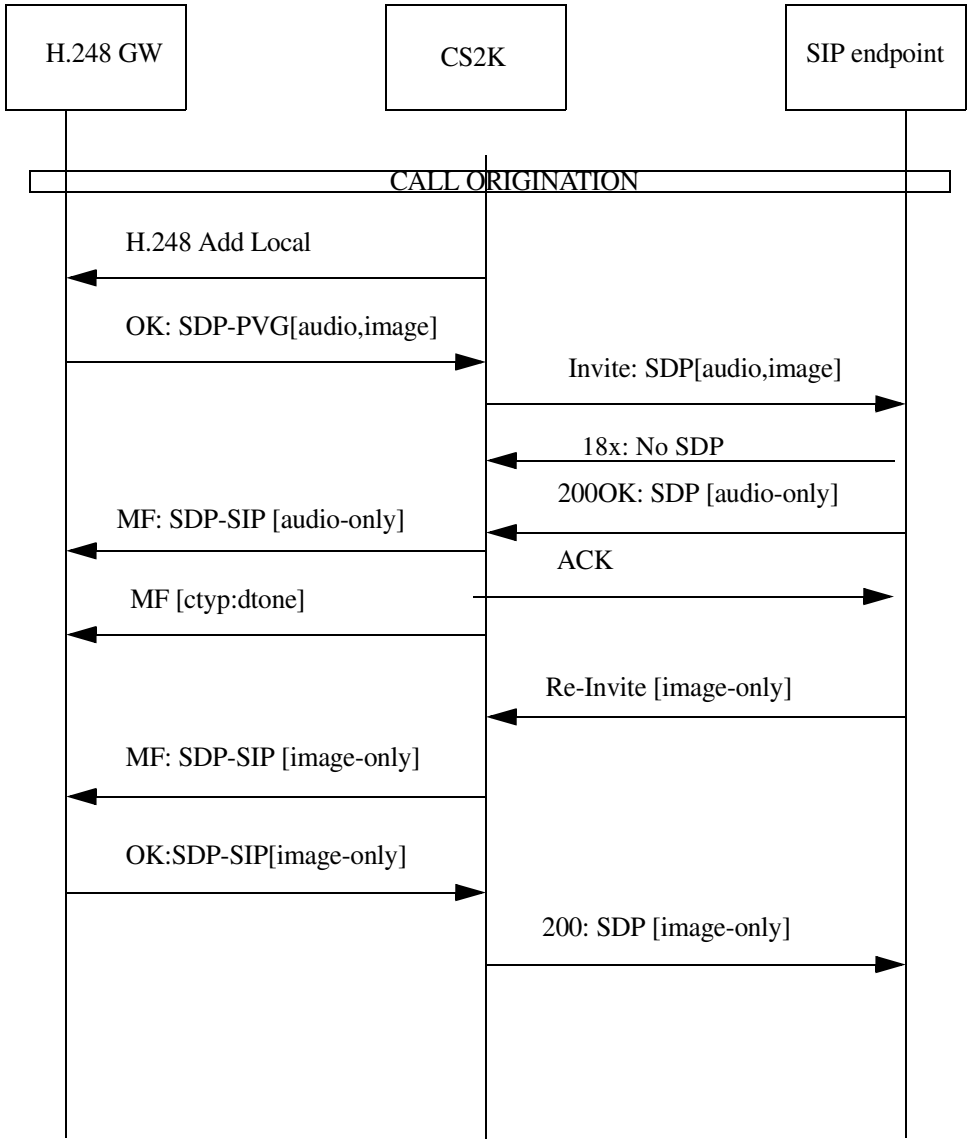
Note 8: The content of SDP uses following abbreviation:

- SDP (audio) for processing of audio media stream.
- SDP (t38) for processing of t38 media stream.
- SDP (audio, t38) for simultaneous processing of audio and t38 media streams.
- SDP (audio, t38-cap) for processing of audio media stream and for t38 capability indication.

1.1.4.2 Basic Call Scenario: PVG to SIP interworking.

When a call originates from PVG, a SIP INVITE is sent from CS2K to the SIP Endpoint which replies with its SDP. Since the **T.38 Annex D Supported** is enabled in the NGSS for the remote server, during the voice call setup the PVG is asked to scan for fax tones. After the voice call is established successfully the remote receiving gateway detects V.21 flag and starts the re-Invite sequence leading to change from G.711 or G.729 codec to T.38. Once the sequence completes, the T.38 fax call is established.

Figure 4 T.38 Calls originating from PVG on CS2K and terminating at CISCO/MTS

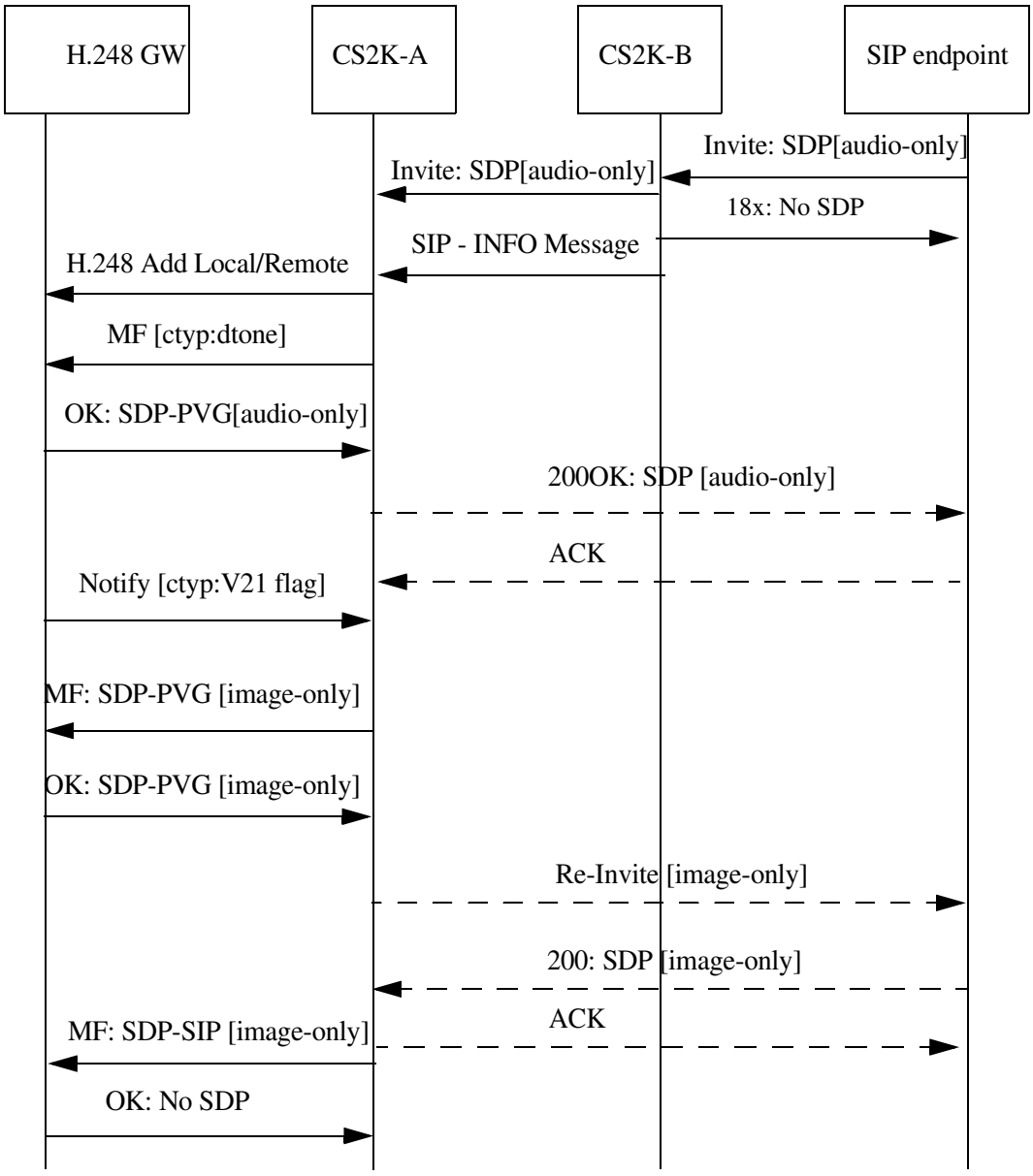


1.1.4.3 Tandeming Support

In this scenario **T.38 Annex D Supported** is enabled in the CS2K-B NGSS, but the call is tandemed to CS2K-A which is not aware that the remote SIP server supports T.38. A SIP INFO message with a proprietary header is used to inform CS2K-A that T.38 support is required causing the CS2K-A to instruct the H.248 PVG to scan for fax tones during the voice call establishment. A voice call is established successfully, and then PVG detects a V.21 flag. V.21 Fax notify is sent from PVG which triggers an attempt to

change the codec from G.711 or G.729 to T.38 communicated to the remote end via a re-Invite sequence.

Figure 5 T.38 Fax calls spanning over more than one CS2K

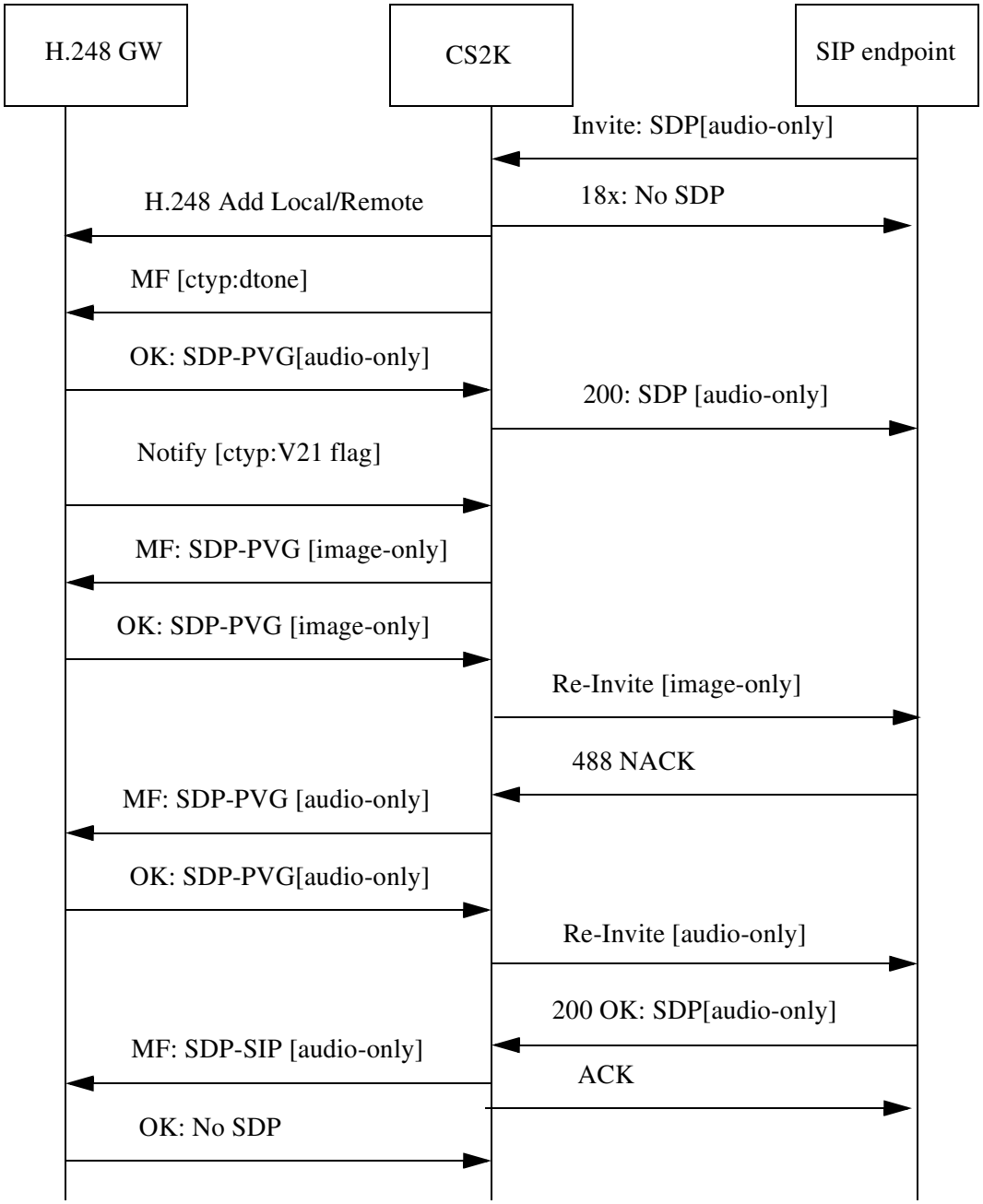


1.1.4.4 Unsuccessful switch attempt, far end rejection.

This scenario describes an unsuccessful T.38 Fax call attempt, where the SIP Re-INVITE for the switch-over from voice to T.38 mode is rejected by a SIP 488 Not Acceptable Here response. In this case an attempt is made to preserve the call by switching back the codec to voice. This is done via another SIP

Re-INVITE sequence with voice only codec to switch the call back to voice, as shown in Figure 6.

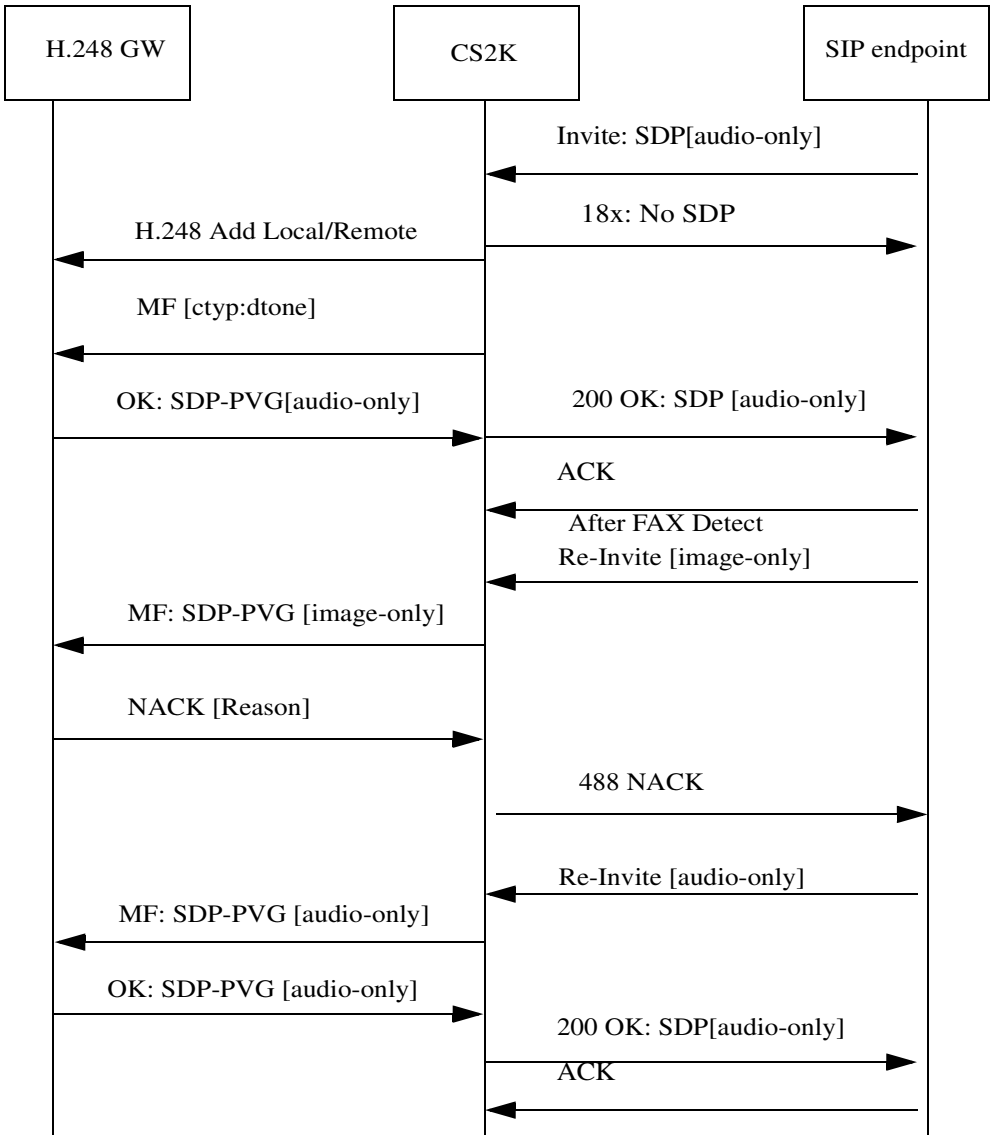
Figure 6 SIP endpoint rejects the Offer



1.1.4.5 Unsuccessful switch attempt, local rejection

When the SIP Re-INVITE Fax offer for a switch to T.38 comes from the remote SIP side and the PVG NACKS it, the PVG sends the reason for the rejection to the SIP side which in turn sends a SIP Re-INVITE to change the SDPs to audio-only mode.

Figure 7 PVG Rejects Offer



1.2 Hardware Requirements or Dependencies

No new hardware is required.

1.3 Software Requirements or Dependencies

CM/GWC/NGSS: SN09 load

H.248 GW: supporting H.248.1, H.248.2 ctyp package, T.38 mode.

T.38 should be provisioned on the H.248 GWC

T.38 Annex D Supported option should be provisioned on the NGSS Remote SIP Server provisioning page.

1.4 Limitations and restrictions

- This feature verifies T.38 Annex D interworking for H.248 PVG GW on one call leg and 3rd party SIP User Agent Server supporting T.38 Annex D functionality on the other call leg. It should not be enabled for remote SIP servers that don't support T.38 Annex D.
- **Re-Invite for Voice Band Data** field should be only used to prevent auto upspeed on fax detection from G.729 to G.711 by an H.248 PVG that is provisioned to support G.729.

1.5 Interactions

Not Identified.

1.6 Glossary

Term	Description
New term	Definition
CED	Called terminal identification answer tone of Fax device (2100 +/- 15 Hz, continuous tone, duration 2.6-4.0 sec.) see T.30 chapter 4.1
CM	Call Manager, Computing Modules
CNG	Calling tone of Fax device (1100 +/- 38 Hz, 0.5 sec. on, 3.0 sec. off, duration 60-120 sec.) see T.30 chapter 4.2.
CS2K	Call Server 2000

Term	Description
G3FE	Group 3 Facsimile Equipment G3FE refers to any entity which presents a communication interface conforming to ITU- T Recommendation T. 30, T. 4, and optionally T. 6. A G3FE may be a traditional G3 facsimile machine, an application with a T. 30 protocol engine or any other possibility mention in the network model for IP Facsimile mentioned in Recommendation T. 38.
GW	Gateway (Signalling Gateway and Media Gateway)
GWC	Gateway Controller
MCS	Multimedia Communication Server
PSTN	Public Switched Telephone Network.
PVG	Passport Packet Voice Gateway
RFC	Request For Comments (IETF)
RTP	Real-time Transport Protocol (IETF 1889, 3550)
SDP	Session Description Protocol (IETF RFC 3266)
SIP	Session Initiation Protocol (IETF RFC 3261)
UDP	User Datagram Protocol (IETF RFC 768)
UDPTL	Facsimile UDP Transport Layer protocol (ITU T.38)
V.21 Preamble	Series of flag sequences 01111110 for 1 sec +/- 15%.

Product = CS 2000

A00009463 -- CBM to Support Centralized User Authentication, Authorization, and Admin with IEMS

Functional Description

1: Applicable Solution(s)

PT-AAL1, PT-IP, DMS, PT-AAL2

1.1 Description

This feature provides the CBM capability to support Centralized Authentication, Authorization, Administration (AAA) with the Integrated Element Management System (IEMS). This feature activates PAM, RADIUS, PAM-MKHOMEDIR, NSS-SAML and SAML modules to enable integration

of CBM with the IEMS and SAML, in order to allow the use of Centralized AAA.

This feature is the equivalent of the SN08 A00007489 which provided similar capability on the SDM product, with the exception of the following points:

- There is neither the support nor the introduction of any new user group on the CBM as part of this feature (not included in SN09 features).
- There is no new security or audit log generated by this feature.
- In addition to the SSH, there are other applications (e.g. login, su, etc.) that are supported on the CBM. The ProFTP and SFT (for CM->CBM Secure FTP) are however not supported.

Note: The details of the above-mentioned equivalent SDM feature is found in PLS fmdoc library under A00007489.aa14 design documents.

With respect to AAA functionality, there are two possible configurations supported by the CBM, which are described in this document, and captured in the following figures:

Figure 1 CBM with central security server configuration & components

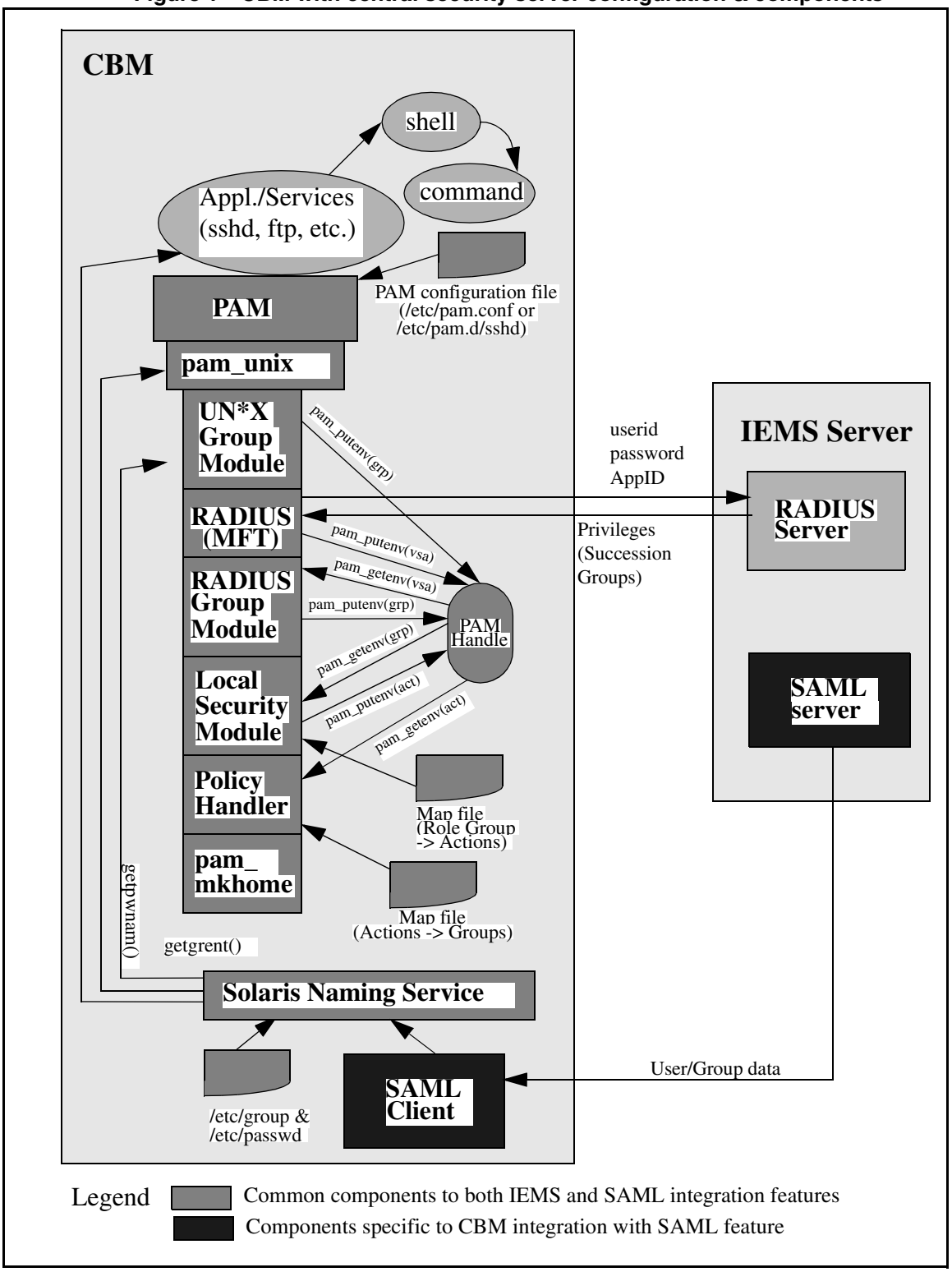
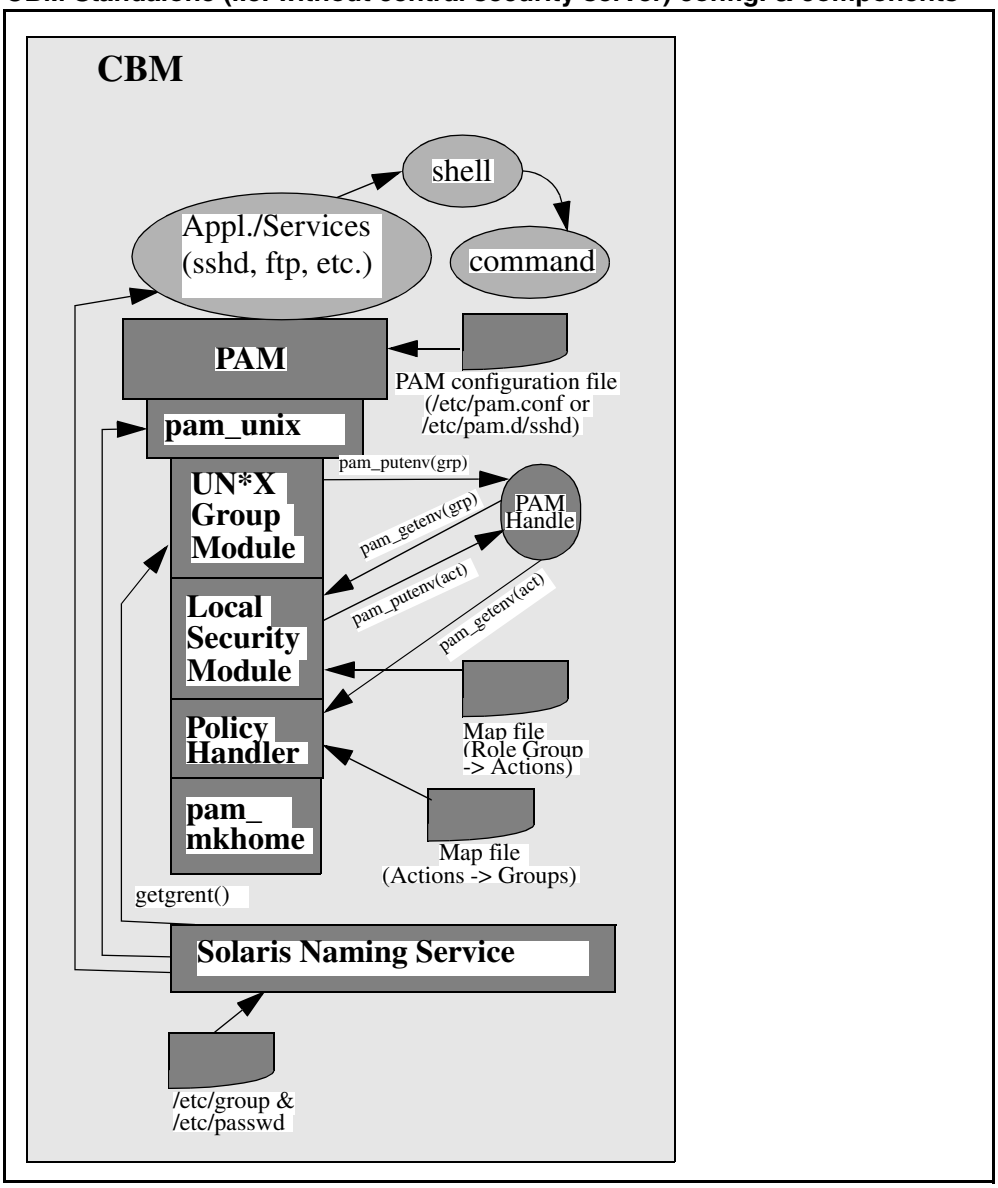
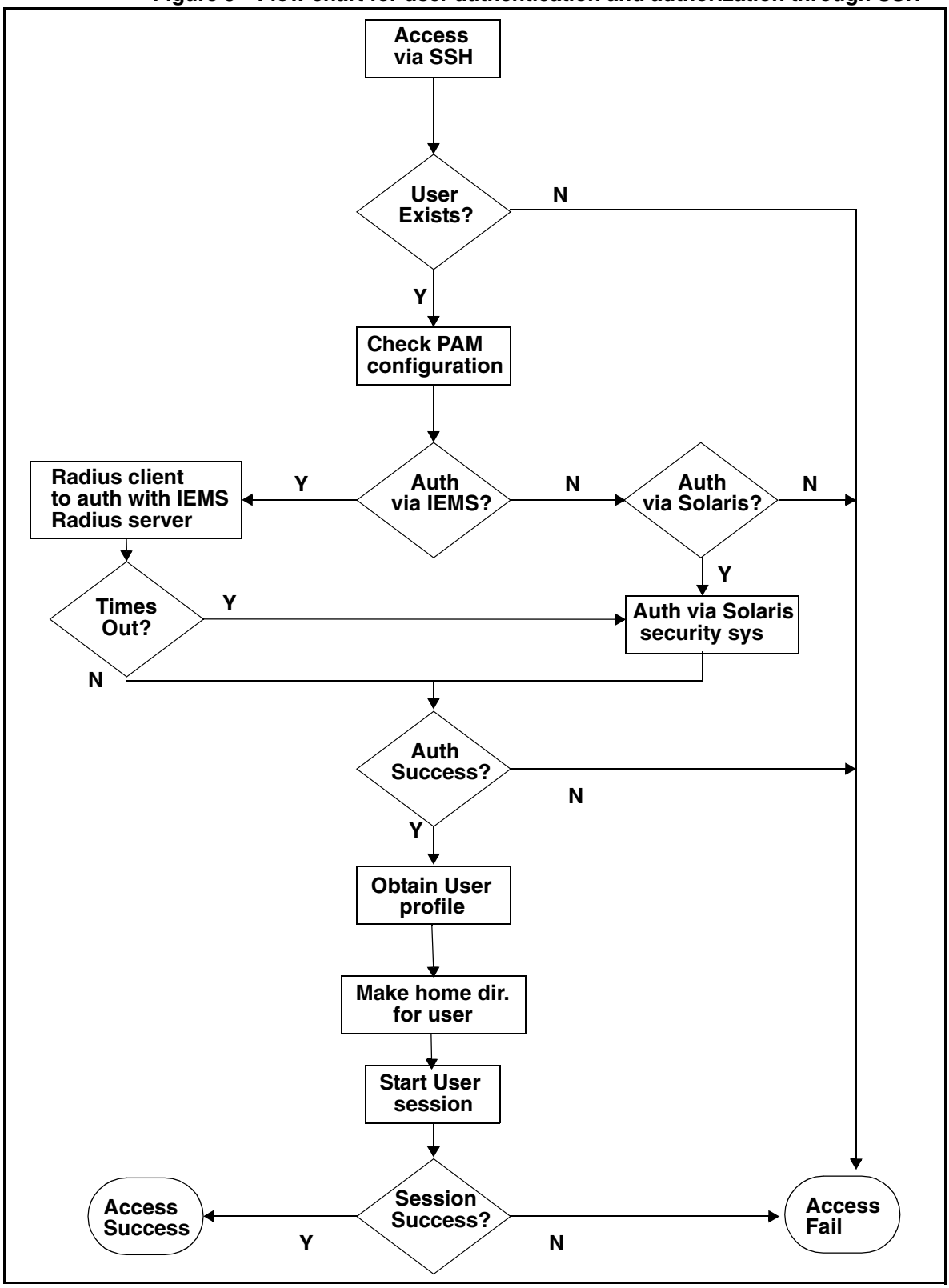


Figure 2 CBM Standalone (i.e. without central security server) config. & components



The following is a flow chart for user authentication and authorization through SSH.

Figure 3 Flow chart for user authentication and authorization through SSH



1.2 Hardware Requirements or Dependencies

No new hardware dependency is introduced in this feature for the Standalone CBM deployment (i.e. without centralized security server). For the CBM deployment with IEMS centralized security server, the IEMS and its hardware dependencies are required by this feature.

1.3 Software Requirements or Dependencies

The PAM, RADIUS and SAML software are required on the CBM. Also, for the CBM deployment with IEMS centralized security server, IEMS and its software dependencies are needed by this feature.

1.4 Limitations and restrictions

TBD

1.5 Interactions

1.5.1 Changes to Network Connectivity Applications

The following table shows the impact of this feature to network connectivity applications.

Table 1 Network Connectivity Applications

Application	Current Release	SN09	Configurable - i.e. Turn On/Off (Y/N)	Support IEMS central security server (Y/N)
SSH (with password)	Enable	Enable	N	Y
SFTP (with password)	Enable	Enable	N	Y
SSH (with key)	Enable	Enable	N	N
SFTP (with key)	Enable	Enable	N	N
Telnet	Enable	Enable	N	Y
FTP	Enable	Enable	N	Y
Console access	Enable	Enable	N	Y
su	Enable	Enable	N	Y
ProFTP	Disable	Disable	N	N
SFT (FTP Proxy)	Enable	Enable	N	N

Note: It is recommended that Telnet and FTP applications should not be used since SSH and SFTP are more secure tools.

When an application/service is not integrated to work with a central security server, the service can only permit access to users who have accounts locally on the CBM.

1.6 Glossary

Term	Description
AAA	Authentication, Authorization, Accounting
CBM	Core and Billing Manager
CUA	Centralized User Administration
IEMS	Integrated Element Manager System
PAM	Pluggable Authentication Module
SAML	Security Assertion Markup Language
SDM	SuperNode Data Manager
VSA	Vendor Specific Attributes

Product = CS 2000

A00009470 -- SDM to Support Security Assertion Markup Language NNSSwitch client

Functional Description

1: Applicable Solution(s)

UA-IP, PT-AAL2

1.1 Description

SuperNode Data Manager (SDM) to support Security Assertion Markup Language (SAML) NSSwitch client feature.

This feature will add SAML NSSwitch client function on SDM to integrate with centralized IEMS's (SS 1.1) SAML server.

This SN09 feature is to enhance the existing SDM security functionality which was developed in SN08. It will improve SDM centralized AAA function through IEMS by removing the need to update user accounts on SDMs whenever an SDM user is added/deleted/modified on IEMS.

Note: Please refer to SN08 IEMS Integration feature document in PLS FMDOC (a00007489) for detailed information on SN08 functionality.

In SN08, SDM only provided access to the user attributes (identification) information in local /etc files. It did not support other naming/identification information sources for the user attributes. As a result, when an SDM user account was created on IEMS, the user account also needed to be added on each SDM via an SDM script (enableIEMSUser). Likewise, when an SDM user account was deleted on IEMS, the user account also needed to be removed on each SDM via an SDM script (disableIEMSUser).

This SN09 feature will address this limitation by providing SAML (Security Assertion Markup Language) client on SDM for user information retrieval. This will allow IEMS centralized security server to be one of the naming/identification information sources for the user attributes. There will be no need to maintain the local /etc files with enableIEMSUser and disableIEMSUser scripts whenever an SDM user is /added/modified/deleted on an IEMS server.

1.2 Hardware Requirements or Dependencies

No new hardware dependency is introduced in this feature for Standalone SDM deployment without centralized security server.

For SDM deployment with IEMS centralized security server, IEMS and its hardware dependencies are needed by this feature.

1.3 Software Requirements or Dependencies

For SDM deployment with IEMS centralized security server, IEMS and its software dependencies are needed by this feature.

This feature has included the following dependency software for SAML client:

- curl
- log4cpp
- Xerces-c
- xml_security_c
- OpenSAML

Please refer to 1.11 “License” in DID section for detail on third party software and their copyright notices.

1.4 Limitations and restrictions

- Authentication: This feature doesn’t change the existing authentication method for IEMS users. The users on the IEMS server will remain being

authenticated by SDM through PAM, which in turn uses RADIUS protocol to authenticate IEMS users.

- SDMMTC User level can only be used to change user/group attributes when an SDM is configured to use local security server. When IEMS central security server is configured for the SDM, IEMS Security Administration GUI must be used to update the user/group information.
- Password update: This feature doesn't provide IEMS users to change password from an SDM. The IEMS Security Administration GUI is still the tool for this purpose.
- Account and password status: An IEMS user will not get expiration warning when she/he logs into SDM. However, since the authentication is done through RADIUS, an IEMS user with an expired account and/or password will not be allowed to log into SDM because the RADIUS server will fail the login attempt.

1.5 Interactions

No new interaction is introduced by this feature.

1.6 Glossary

Term	Description
AAA	Authentication, Authorization, Accounting
CBM	Core and Billing Manager
IEMS	Integrated Element Manager System
LAM	Loadable Authentication Module
LDAP	Light-weight Directory Access Protocol
MFT	Management Framework Technology
NE	Network Element
OSS	Operations Support System
PAM	Pluggable Authentication Module
SAML	Security Assertion Markup Language
SDM	SuperNode Data Manager
SSL	Secure Sockets Layer
SSO	Single Sign-On
VSA	Vendor Specific Attributes

2: Configuration for A00009470

2.1 Hardware and Software Requirements

SDM standard hardware and software are required.

No new hardware is needed for this feature. However, the software for this feature needs to be installed on an SDM before feature configuration can take place.

For SDM deployment with IEMS centralized security server, IEMS and its hardware and software dependencies need to be available and configured.

2.2 Initial Configuration

- No hardware initial configuration for this feature.
- The initial software configuration for this feature is using local security server (i.e. native AIX security system) for authentication and authorization. No user input is needed for initialization.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable to this feature.

2.4 Upgrade Considerations

2.4.1 Dump and Restore (CM)

Not applicable to this feature.

2.4.2 Element Management Upgrade

No impact to Element Management Upgrade when an SDM is deployed without external security server.

IEMS central server must be upgraded to the same release as SDM before an SDM can be configured to use IEMS as the centralized security server.

Local user migration from SDM to IEMS should not take place during upgrade. It should take place after SDM and IEMS are upgraded to the same software release.

2.4.3 Downgrade impact

No impact to downgrade if the SDM feature installation is aborted.

2.5 Data schema (DS) (CM, MIBS, RDB)

Not applicable to this feature.

2.6 Service Orders (SO) (CM & SESM)

Not applicable to this feature.

2.7 Software optionality control (SOC)

Not applicable to this feature.

2.8 Element Management

2.8.1 CLUI Interface

2.8.1.1 sdmmtc SecuConf

In order to configure SAML client on SDM, SecuConf menu under sdmmtc will be enhanced for SAML client configuration.

The following is the proposed SecuConf screens for selecting SAML for naming service.

```
   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                M                             Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16
17 Help
18 Refresh
 jjsecu1
Time  15:30  >
```

```
   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                M                             Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16
17 Help
```

```
18 Refresh
 jjsecu1
Time  15:31  >change 1


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                 M                            Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15          Change Authentication Naming Service
16          Please choose one of the following available option(s) on the
17 Help      system. More option(s) will be available if the corresponding
18 Refresh   fileset(s) is(are) applied. (1) SAML (2) LOCAL :
 jjsecu1
Time  15:38  >1


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                 M                            Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16          Change Authentication Naming Service - SAML
17 Help
18 Refresh   Enter the IP Address of the SAML Server:
 jjsecu1
Time  15:40  >47.1.2.3


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                 M                            Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
```

```
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16          Change Authentication Naming Service - SAML
17 Help
18 Refresh   Enter the Fully Qualified Domain Name of the SAML Server:
 jjsecu1
Time  15:43  >iems-server1.nortel.com


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                M                             Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: LOCAL
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16          Change Authentication Naming Service - SAML
17 Help
18 Refresh   Enter the system account password of the SAML Server:
 jjsecu1
Time  15:45  >****[2]


    SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                M                             Fault Tolerant
SecuConf
 0 Quit
 2
 3
 4
 5
 6
 7
 8
 9
10
11          Change Authentication Naming Service - SAML
12
13          The SAML Server to be configured:
14             IP address: 47.1.2.3
15             Fully Qualified Domain name: iems-server1.nortel.com
16
17 Help      Do you wish to proceed?
18 Refresh   Please confirm ("YES", "Y", "NO", or "N")
```

[2] Stars may not be shown in future releases.

```
 jjsecu1
Time  15:47  >y


   SDM       CON     NET     APPL    SYS      HW    CLLI: NONE
   ISTb       .      SysB     .      ISTb     .     Host: wcary2p7
    M                 M                           Fault Tolerant
SecuConf
 0 Quit
 2          1 Authentication Naming Service: SAML
 3
 4          2 Authentication PAM Stack: LOCAL
 5
 6          3 Remote Security Log Destination: -
 7
 8          4 Remote Audit Log Destination: -
 9
10
11
12
13
14
15
16
17 Help
18 Refresh   Change 2 - Command complete.
 jjsecu1
Time  15:48  >
```

The same configuration steps should be used when any of the SAML client configuration values (IP Address, Fully Qualified Domain Name or System account password) need to be changed later.

NOTE: For network amAdmin system account password change, please refer to MFT's Security Services 1.1 Interface Definition Appendix G (IEMS amAdmin password change procedure).

http://knowledgeonline.ca.nortel.com/sws/livelink.exe/3747266/Security_Services_1.1_ID?func=doc.Fetch&nodeid=3747266

When SAML is selected for Authentication Naming Service, IEMS should be used for Authentication PAM Stack. This is the correct combination for using IEMS as the central security server on an SDM.

2.8.2 New command: deleteIEMSLocalEntry

A new command, deleteIEMSLocalEntry, is added so the administrator can clean up the /etc/passwd file after a SN08 SDM with IEMS as the central server is upgraded to SN09 SDM software. This command is not needed when an SDM with IEMS configuration is upgraded from SN09 or newer releases.

The synopsis of the command is:

```
deleteIEMSLocalEntry { "ALL" | user}
```

Where:

ALL will cause all IEMS user entries in /etc/passwd will be deleted

<user> is the UID of the IEMS user that will be deleted

2.8.2.1 Example

The following is the example command line for cleaning up /etc/passwd after an SDM with IEMS configuration is upgraded from SN08 to SN09:

```
deleteIEMSLocalEntry ALL
```

2.8.3 Deleted command: enableIEMSUser

SN08 SDM command, enableIEMSUser for allowing an IEMS user to logon to an SDM will be deleted.

2.8.4 Deleted command: disableIEMSUser

SN08 SDM command, disableIEMSUser to disallow an IEMS user to logon to an SDM will be deleted.

2.9 User interface changes

Not applicable to this feature.

2.10 OSSGate Interface Changes

Not applicable to this feature.

2.11 Security

The feature will enhance user authentication and authorization for SDM.

2.11.1 Network configuration

n/a

2.11.2 Key management

n/a

2.11.3 Protocol

n/a

2.11.4 Authentication

When a SDM is deployed without an external security server, user authentication and authorization will be performed locally on the SDM.

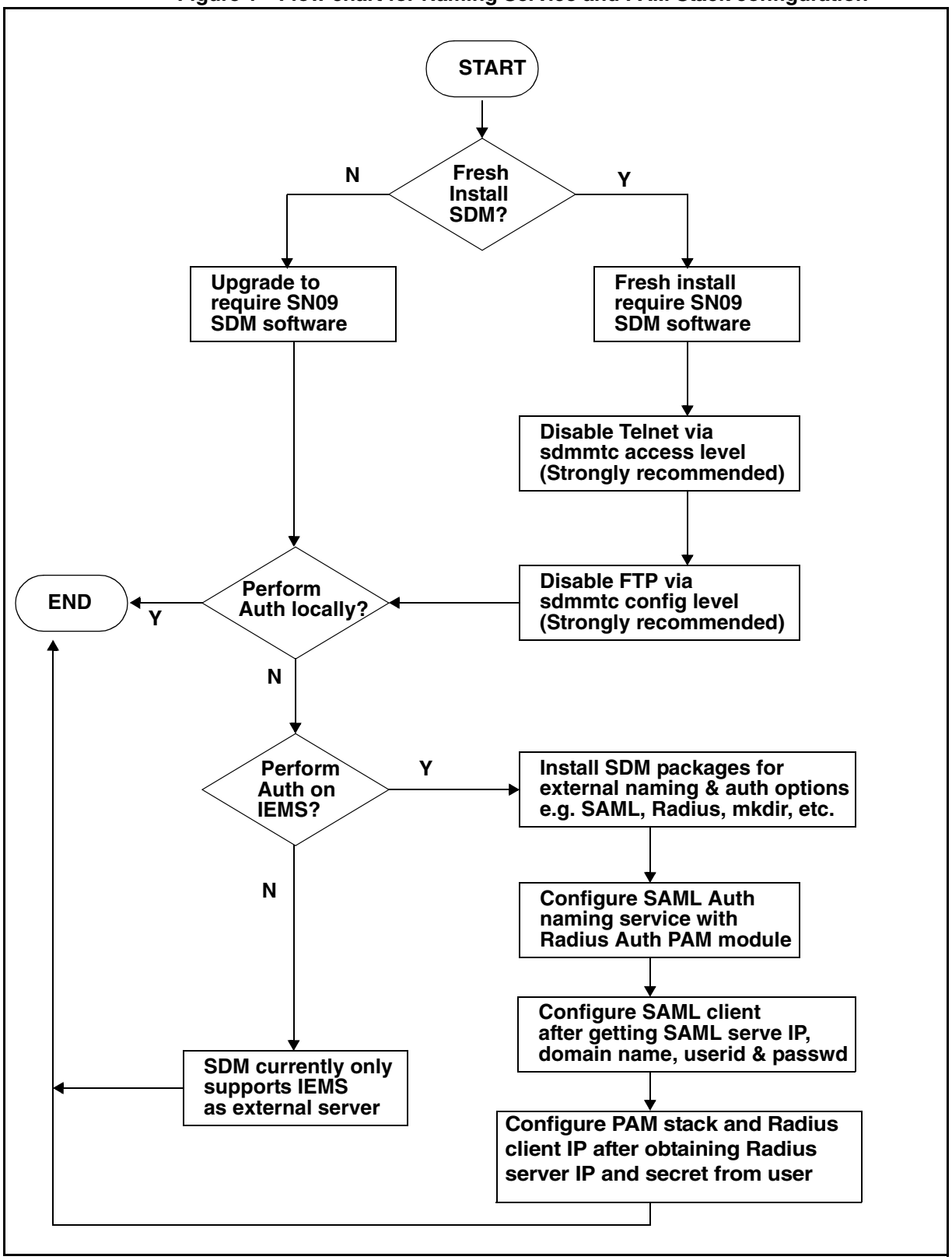
When a SDM is deployed with an external security server like IEMS, user authentication and authorization will be performed through IEMS via Radius protocol.

2.12 Configuration Walkthrough

2.12.1 Security services configuration

The following figure shows the configuration steps for this feature.

Figure 1 Flow chart for Naming Service and PAM Stack configuration



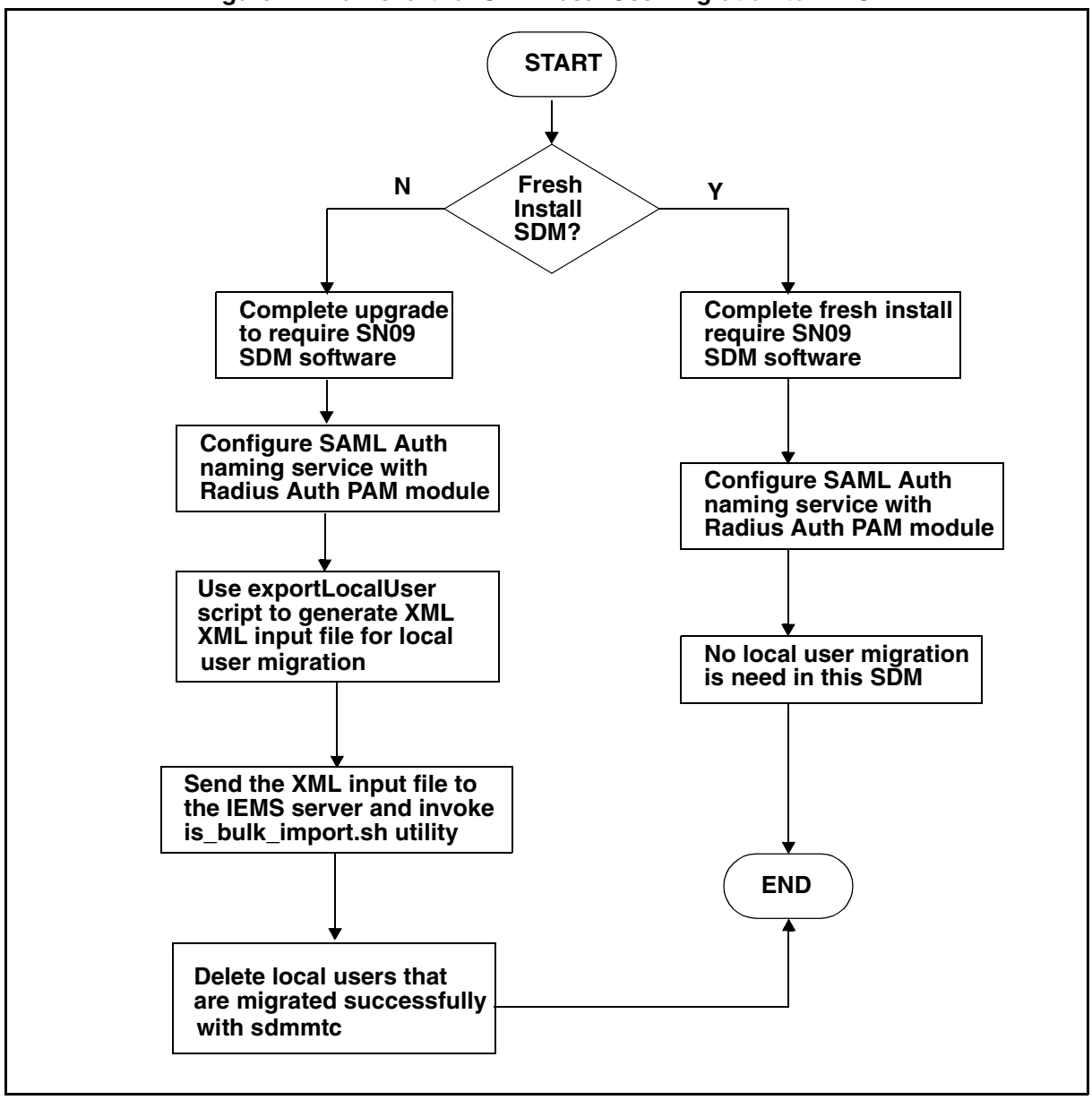
2.12.2 SDM Local User Migration to IEMS

SDM user migration to IEMS needs to take place when an SDM is changed from local security configuration to IEMS central security server configuration.

A new SDM exportLocalUser script is introduced by this feature to generate the XML input file needed by IEMS's is_bulk_import.sh utility for SDM local user migration.

The following figure shows the steps for SDM local user migration to IEMS.

Figure 2 Flow chart for SDM Local User Migration to IEMS



Product = CS 2000

A00009508 -- AMA SIP Line Identification

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

Automatic Message Accounting Session Initiation Protocol (SIP) Line Identification feature introduces the new AMA billing Module 260 which captures originating and terminating agent component and protocol information for packet network agents. Module 260 contains two fields. Table 620 captures the connection side and component type. Table 622 captures the protocol type used. Module 620 is outlined below with current table values:

Module Code 260 - IP/Packet Party Identification (Vendor Specific)

Module Code	88	2	0
Component Type	620	4	1
IP Service Protocol	622	4	3
		Total	5

Table 620, Component Role (NDGR)
Chars Meaning
1: Connection Side (default = 0)
1 = Originating
2 = Terminating
2-3: Component Type
01 = Customer Premise Equipment
02 = Network Edge Component
03 = Gateway System
99 = Unspecified
4: SIGN (hex-C)

Table 622 - IP Service Protocol (Vendor Specific)
Chars Meaning
1: Reserved (default = 0)
2-3: Protocol Type
00 = unspecified
01 = SIP
02 = SIP-T
03 = SIP-I
04 = H.323 v1
05 = H323.v2
06 = H.248/MEGACO
07 = MGCP
4: SIGN (hex-C)

Feature A00009508 provides the framework to capture all variants; however, only the capturing of SIP lines client information is provided by this feature. This feature complements the OAM&P core development done under A00008556 by providing identification of SIP lines for billable calls. The following are sample records illustrating SIP line party information capture:

```
*HEX ID:AA  STRUCTURE CODE:40625C  CALL CODE:110C  SENSOR TYPE:036C
SENSOR ID:0619351C  REC OFFICE TYPE:036C  REC OFFICE ID:0619351C
DATE:50314C  TIMING IND:00000C  STUDY IND:0200000C  CLD PTY OFF-HK:1C
SERVICE OBSERVED:0C  OPER ACTION:0C  SERVICE FEATURE:000C  ORIG NPA:613C
ORIG NUMBER:6215671C  OVERSEAS IND:0C  TERM NPA:00519C
TERM NUMBER:8885672C  CONNECT TIME:1103004C  ELAPSED TIME:000000000C
IC/INC PREFIX:02221C  CC DATE:50314C  CC TIME:1102217C
ELAPSED CC:000000387C  IC/INC EVENT STATUS:007C  TRUNK GROUP NUMBER:30638C
ROUTING INDICATOR:0C  DIALING INDICATOR:1C  ANI INDICATOR:1C
MODULE CODE:306C  OLIP:031C  MODULE CODE:260C  COMPONENT ROLE:101C
IP SERVICE PROTOCOL:001C  MODULE CODE:000C

*HEX ID:AA  STRUCTURE CODE:40625C  CALL CODE:119C  SENSOR TYPE:036C
SENSOR ID:0619351C  REC OFFICE TYPE:036C  REC OFFICE ID:0619351C
DATE:50314C  TIMING IND:00000C  STUDY IND:0200000C  CLD PTY OFF-HK:1C
SERVICE OBSERVED:0C  OPER ACTION:0C  SERVICE FEATURE:000C  ORIG NPA:613C
ORIG NUMBER:6215671C  OVERSEAS IND:0C  TERM NPA:00519C
TERM NUMBER:8885672C  CONNECT TIME:1103009C  ELAPSED TIME:000000000C
IC/INC PREFIX:02221C  CC DATE:50314C  CC TIME:1102218C
ELAPSED CC:000000390C  IC/INC EVENT STATUS:001C  TRUNK GROUP NUMBER:30638C
ROUTING INDICATOR:0C  DIALING INDICATOR:FF  ANI INDICATOR:1C
MODULE CODE:306C  OLIP:031C  MODULE CODE:260C  COMPONENT ROLE:201C
IP SERVICE PROTOCOL:001C  MODULE CODE:260C  COMPONENT ROLE:201C
IP SERVICE PROTOCOL:001C  MODULE CODE:000C
```

For the above examples, the Call Code 110 originating Equal Access AMA record contains a Module 260 which shows that a SIP client at the customer's premise originated the call. Component Role value of 101 can be broken into (1) originating and (01) customer premise equipment. IP Service Protocol shows SIP (01) being used. The Call Code 119 terminating Equal Access AMA record contains a Module 260 that shows the call terminated to a SIP client. Component Role value 201 can be broken into (2) terminating and (01) customer premise equipment.

Feature A00009508 uses a new tuple in table AMAOPTS to activate and deactivate Module 260 inclusion. The new OPTION is called RECORD_MC260, and the SCHEDULE will be either ON or OFF. The default setting is OFF. The new option activates recording of packet client involvement for both originating and terminating agents. This option does not force billing; it collects the additional information for existing billable scenarios.

The following CI session shows how feature functionality is activated. Deactivation is achieved by setting schedule back to OFF.

```
>table amaopts
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: AMAOPTS
```

```
>pos RECORD_MC260
        RECORD_MC260                    OFF
>lis
           OPTION                   SCHEDULE
-------------------------------------------------------
        RECORD_MC260                    OFF
>cha
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: OFF
>on
TUPLE TO BE CHANGED:
        RECORD_MC260                     ON
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
TUPLE CHANGED
JOURNAL FILE INACTIVE
```

1.1.1 On the SDM/CBM Side:

This feature A00009508 introduces the new AMA Module Code 260 with two new fields COMPONENT ROLE and IP SERVICE PROTOCOL to the BAF database on SDM/CBM.

The new Module 260 with the two new fileds and its definitions are added to baf.db file (BAF database) to be supported by AMADUMP tool on SDM/CBM.

Definition of the two new fields added in baf.db are:

COMPONENT_ROLE 16 4 bcd 0 COMPONENT_ROLE
COMPONENT ROLE

IP_SERVICE_PROTOCOL 16 4 bcd 1 IP_SERVICE_PROTOCOL
IP SERVICE PROTOCOL

And the following is the complete module code defined in baf.db:

[Subrecord]
260
MODULE_CODE_ID
COMPONENT_ROLE
IP_SERVICE_PROTOCOL
[^]

This functionality could be verified using AMADUMP tool by executing the following steps:

Login to SDM or CBM as root user or maint user

Execute the listfile command for AMA stream to get the filename(s)

billmtc; filesys; listfile ama

Execute amadump command to display the billing file with module code 260

billmtc; tools; amadump ama

AMADUMP>> dump details sum fname <file- name>

Where <file-name> is from the output of listfile command.

The following is the AMADUMP output of a billing file with Module Code 260 on SDM/CBM:

Record data:

RDW 00610000
HEX_ID aa
STRUCTURE_CODE 40625C
CALL_CODE 110C
SENSOR_TYPE 036C
SENSOR_ID 0000000C
RECORD_OFFICE_TYPE 036C
RECORD_OFFICE_ID 0000000C
DATE 50418C
TIMING_INDICATOR 00000C
STUDY_INDICATOR 0001000C
ANSWER 0C
SERVICE_OBSERVED 0C
OPERATOR_ACTION 0C
SERVICE_FEATURE 000C
ORIGINATING_NPA 919C
ORIGINATING_NUMBER 8472452C
OVERSEAS_INDICATOR 0C
TERMINATING_NPA 00800C
TERMINATING_NUMBER 9917782C
CONNECT_TIME 0902091C
ELAPSED_TIME 000098182C
IC_INC_PREFIX 00001C
CARRIER_CONNECT_DATE 50418C
CARRIER_CONNECT_TIME 0902091C
ELAPSED_FROM_CC 000000000C
IC_INC_EVENT_STATUS 010C
TRUNK_GROUP_NUMBER 00584C
ROUTING_INDICATOR 0C
DIALING_INDICATOR 8C
ANI_INDICATOR 1C

Subrecord data:

MODULE_CODE_ID 042C
CALL_RECORD_SEQUENCE_NUMBER 0003851C

Subrecord data:

MODULE_CODE_ID 260C
COMPONENT_ROLE 199C
IP_SERVICE_PROTOCOL 000C
Subrecord data:

MODULE_CODE_ID 000C

1.2 Hardware Requirements or Dependencies

There are no hardware dependencies for this feature.

1.3 Software Requirements or Dependencies

Since feature A00009508 changes AMA, display and downstream utilities need to be adjusted to handle the new information now present. This feature addresses all core required changes and SDM required changes to support this new module code; however, all downstream processing programs need to be updated as well.

1.4 Limitations and restrictions

There are no restrictions.

1.5 Interactions

Feature A00008556 introduces the DPL LGRP type and DPL line option. DPL is used to denote SIP lines' components in the core. This designation is also used by this feature in determining if an agent is a SIP line.

1.6 Glossary

Term	Description
AMA	Automatic Message Accounting
DPL	Dynamic Packet Line
EA	Equal Access
LGRP	Logical Group: Used to group Succession agents
SDM	Supernode Data Manager
SIP	Session Initiation Protocol

Term	Description
RECORD_MC260	New AMAOPTs OPTION which controls A00009508 functionality.
AMADUMP	AMADUMP is a tool, which displays the billing records from AMADNS or DIRP billing files stored on SDM.

Product = CS 2000

A00009514 -- CS2K-MCS Interop for SN09

Functional Description

1: Applicable Solution(s)

PT-IP, IAC, CHS

1.1 Description

SIP on Succession Communication Server was first introduced in SN03 to enable Communication Server - Communication Server and Communication Server -MCS5200 communication. At the time of implementation, the IETF SIP/SIP-T standards were still at pre-RFC stage. Nortel being the pioneer has moved forward with its implementation and has gained vast experience in SIP-T interop in the past few years. In the meantime the IETF specifications have evolved and matured. Communication Server initial implementation was based on the GWC/VRDN architecture which has imposed few limitations on the overall application. In SN07, with the introduction of the Session Server, the SIP-T/SIP implementation on the Succession Communication Server has been revamped and evolved to an IETF compliant open interface. The Session Server is a high capacity carrier grade new platform consisting of hardware based on SAM-XTS and software consisting of base and share layers. The application introduced on this platform in SN07 was the SIP Gateway allowing interop between the Communication Server and 3rd party Call Servers and Application Servers. The Session Server enhances the capability of the Succession Communication Server which is critical in Nortel's strategic market positioning in VoIP solutions.

This feature provides support for SN09 NGSS interworking with MCS release 09 (a.k.a. MCS 4.1) and will also provide support for the backward compatibilty with MCS 3.0. SN09 NGSS interworking with MCS 4.0 will not be supported.

This feature will address upgrade scenarios, new content integration, and regression testing. One of the new pieces of functionality is the support for private/public name delivery for Converged Desktop users, which includes the support for SIP phone-context tag fields.

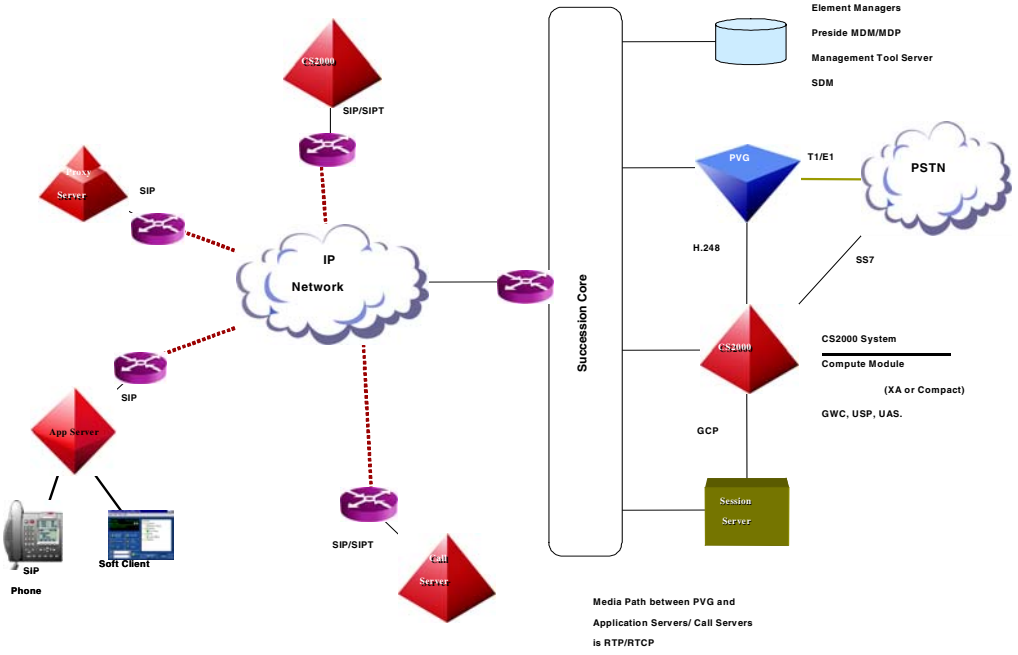


Figure-1 CS2K Network Configuration

1.1.1 Upgrade

The following table shows support for the interworking configuration of the CS2K and MCS releases.

Table 1: CS2K and MCS Releases Support

MCS	MCS 3.0	MCS 4.0	MCS 4.1
(I)SN07	Supported	Not Supported	Not Supported
(I)SN08	Supported	Supported	Supported
(I)SN09	**Supported ***	**Not Supported**	**Supported**

* Still under consideration

After any upgrade either on the CS2K side or on the MCS side the upgraded configuration must comply to the supported configuration. The following shows the CS2K configuration with the MCS.

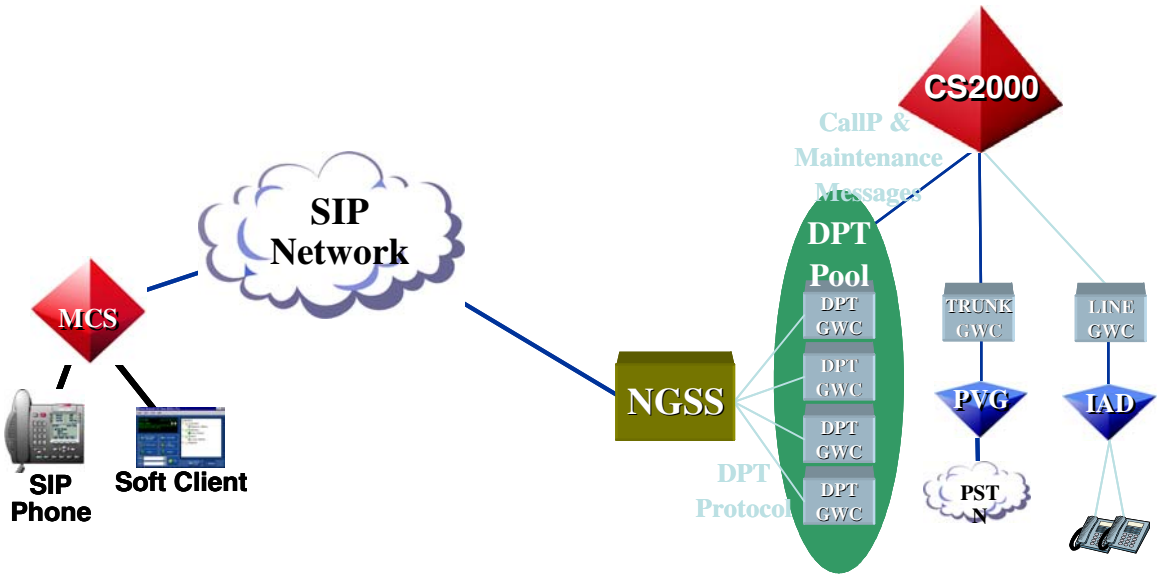


Figure-1 NGSS - MCS Interworking Configuration

The following walks through the different configuration scenarios and procedure which should be followed to upgrade the NGSS to the SN09 release.

1.1.1.1 SN07 or SN08 CS2K with VRDN Interworking with MCS 3.0

In this configuration the VRDN must be first migrated to the NGSS architecture prior to the CS2K upgrade. After the VRDN to NGSS migration CS2K components including NGSS should then upgraded to the SN09 software release. Depending on the customer requirement the MCS can either be left at MCS 3.0 or could be upgraded to MCS 4.1. MCS should not be, however, upgraded to MCS 4.0.

1.1.1.2 SN07 or SN08 CS2K with NGSS Interworking with MCS 3.0

In this configuration the CS2K components including NGSS could be directly upgraded to SN09 software release. Depending on the customer requirement the MCS can either be left at MCS 3.0 or could be upgraded to MCS 4.1. MCS should not be, however, upgraded to MCS 4.0.

1.1.1.3 SN07 CS2K with either VRDN or NGSS Interworking with MCS 4.0 or MCS 4.1 - This configuration is not supported

1.1.1.4 SN08 CS2K with VRDN Interworking with MCS 4.0

In this configuration the MCS must be first upgraded from MCS 4.0 to MCS 4.1 and the VRDN must be migrated to the NGSS architecture prior to the CS2K upgrade. When the MCS upgrade and the migration from the VRDN to NGSS has been completed then the CS2K components including NGSS could be upgraded to SN09 software release.

1.1.1.5 SN08 CS2K with NGSS Interworking with MCS 4.0

In this configuration the MCS must be first upgraded from MCS 4.0 to MCS 4.1 prior to the CS2K upgrade. When the MCS upgrade has been completed then the CS2K components including NGSS could be upgraded to SN09 software release.

1.1.1.6 SN08 CS2K with VRDN Interworking with MCS 4.1

In this configuration the VRDN must be first migrated to the NGSS architecture prior to the CS2K upgrade. When the migration from the VRDN to NGSS has been completed then the CS2K components including NGSS could be upgraded to SN09 software release.

1.1.1.7 SN08 CS2K with NGSS Interworking with MCS 4.1

In this configuration the CS2K components including NGSS could be directly upgraded to SN09 software release.

1.1.1.8 SN09 CS2K with VRDN - This configuartion is not supported because VRDN is not supported on SN09

1.1.1.9 SN09 CS2K with NGSS Interworking with MCS 3.0

Depending on the customer requirement the MCS can either be left at MCS 3.0 or could be upgraded to MCS 4.1. MCS should not be, however, upgraded to MCS 4.0.

1.1.2 GUI Support

This section describes how to access and data fill the Nature of Address/Numbering Plan Indicator to Phone Context (NOA/NPI/PC) and Out of Band DTMF Payload portions of the Succession Communication Server 2000 Session Server Manager Graphic User Interface (GUI).

1.1.2.1 NOA/NPI/PC section access

Once logged in and having accessed the Succession Communication Server 2000 Session Server Manager link, select Provisioning -> Application -> SIP Gateway to display the NOA/NPI/PC section menu option.

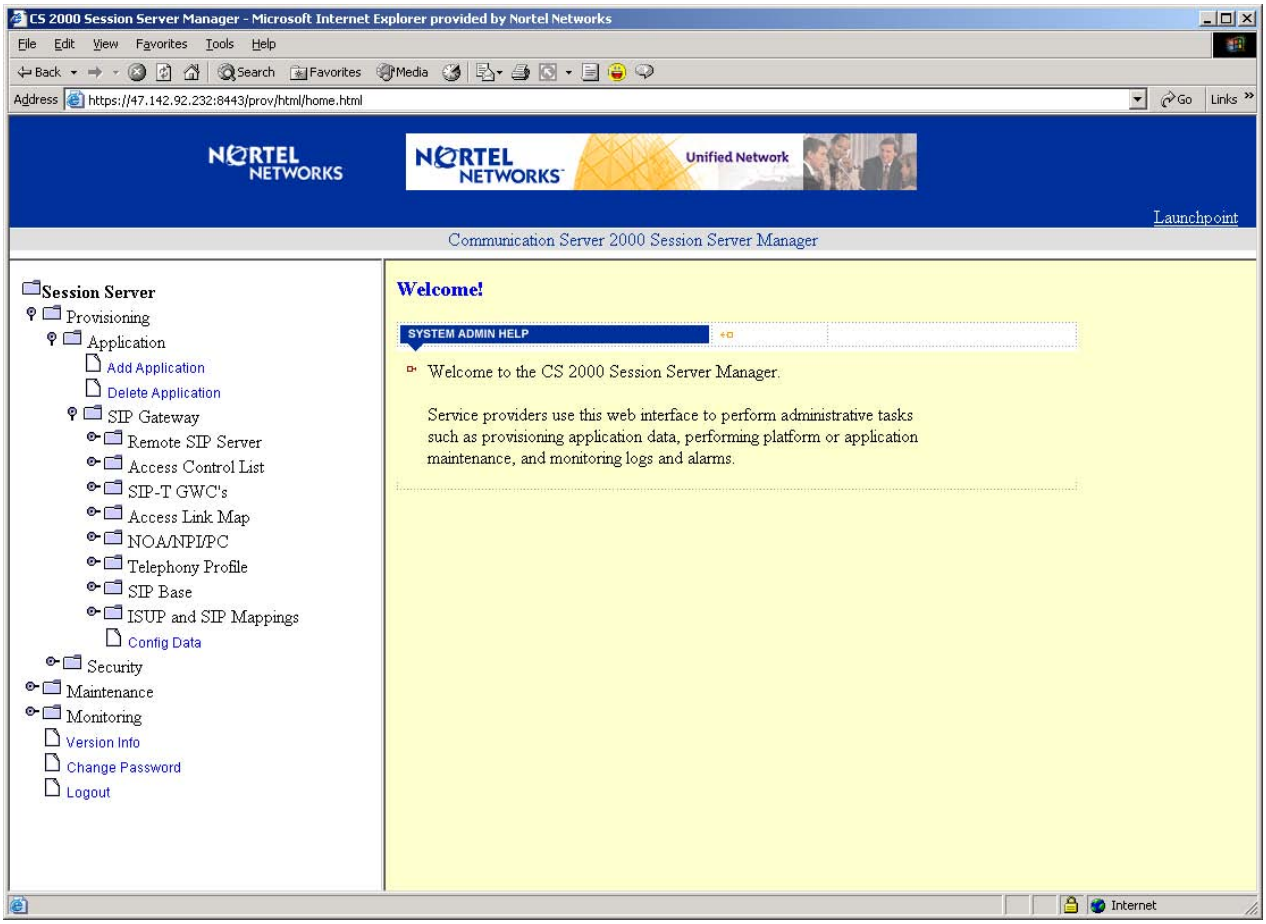


Figure 1 NOA/NPI/PC section access

1.1.2.2 Add/Listing NOA's

Select NOA/NPI/PC menu option to display the Add NOA, List NOA and NOA/NPI/PC Mapping menu options. Select List NOA menu option to view the default list of NOA's.

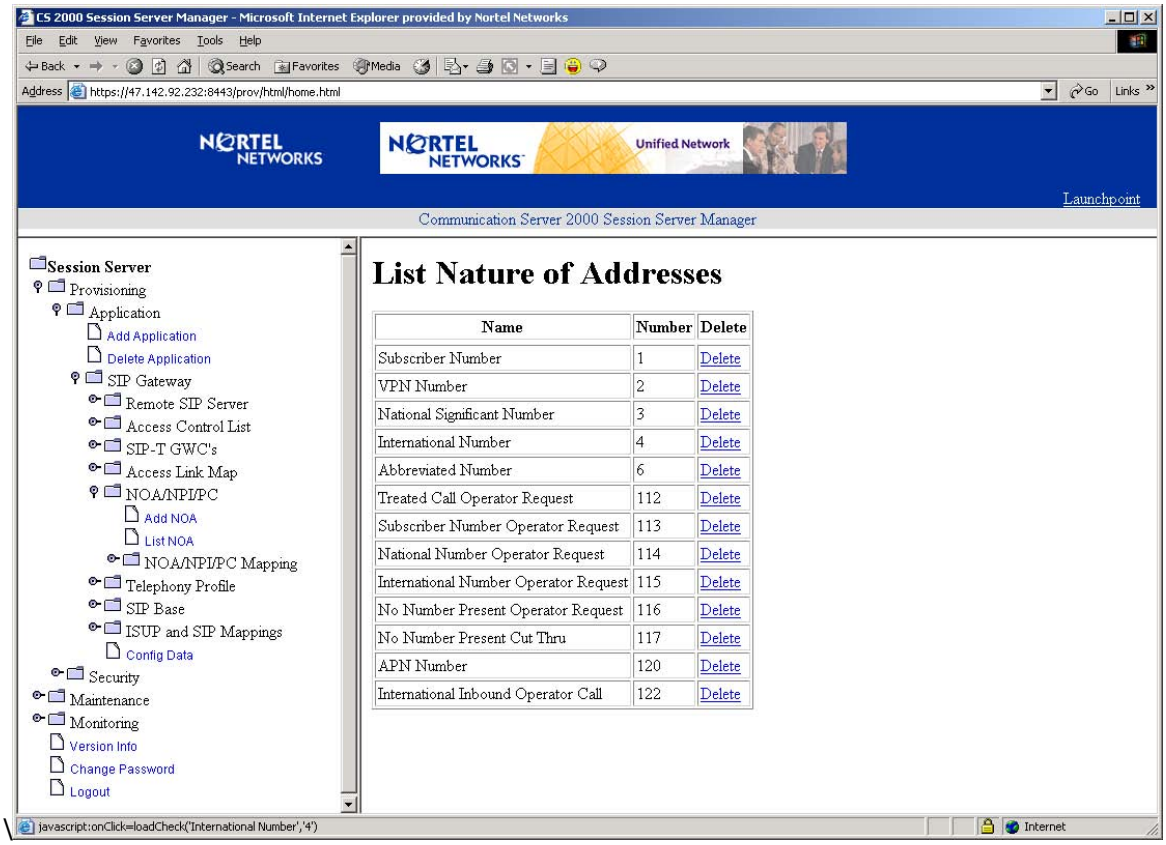


Figure 2 List Nature of Addresses

Select Add NOA menu option to add new NOA. Type in a NOA Name and NOA Number in the designated input areas and then click the Add button to complete the adding of the new NOA. If the addition of the NOA is successful, the new NOA entry will be displayed in the list of NOA's.

NOTE: Valid NOA numbers range from 1 to 150 inclusive.

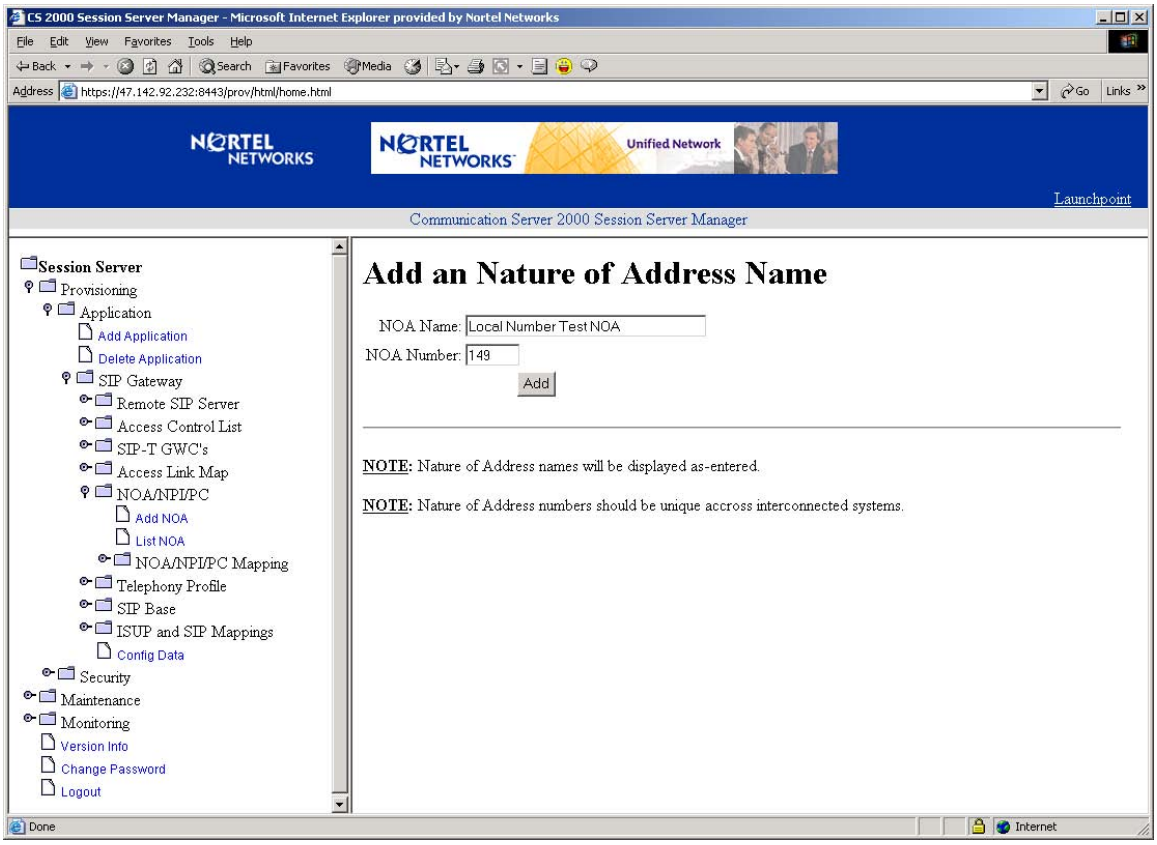


Figure 3 Add a Nature of Address Name

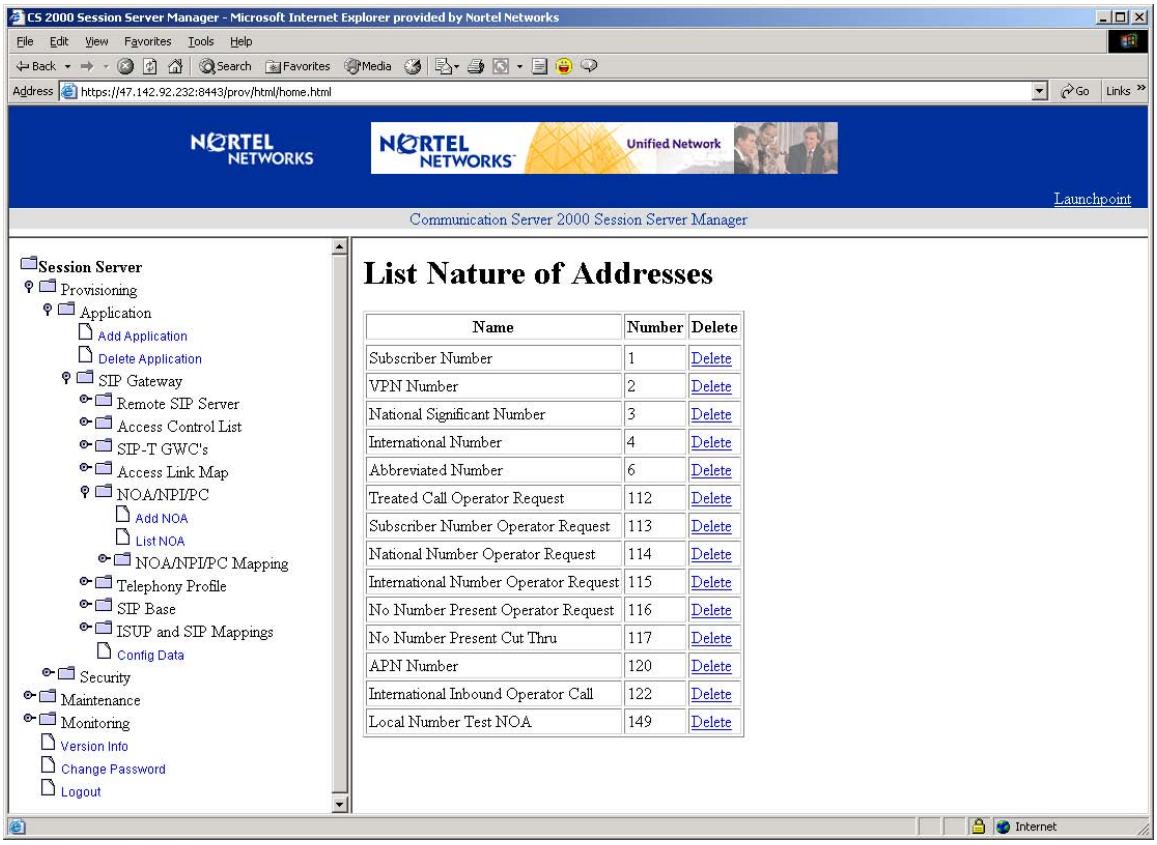


Figure 4 View of List NOA with New Entry

To delete a NOA entry, click Delete for the NOA entry to be removed and select OK in the validation pop-up window.

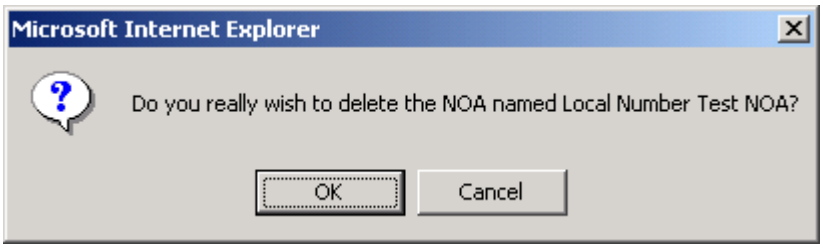


Figure 5 Delete NOA Validation Pop-up Window

The selected NOA entry is removed from the list of NOA's.

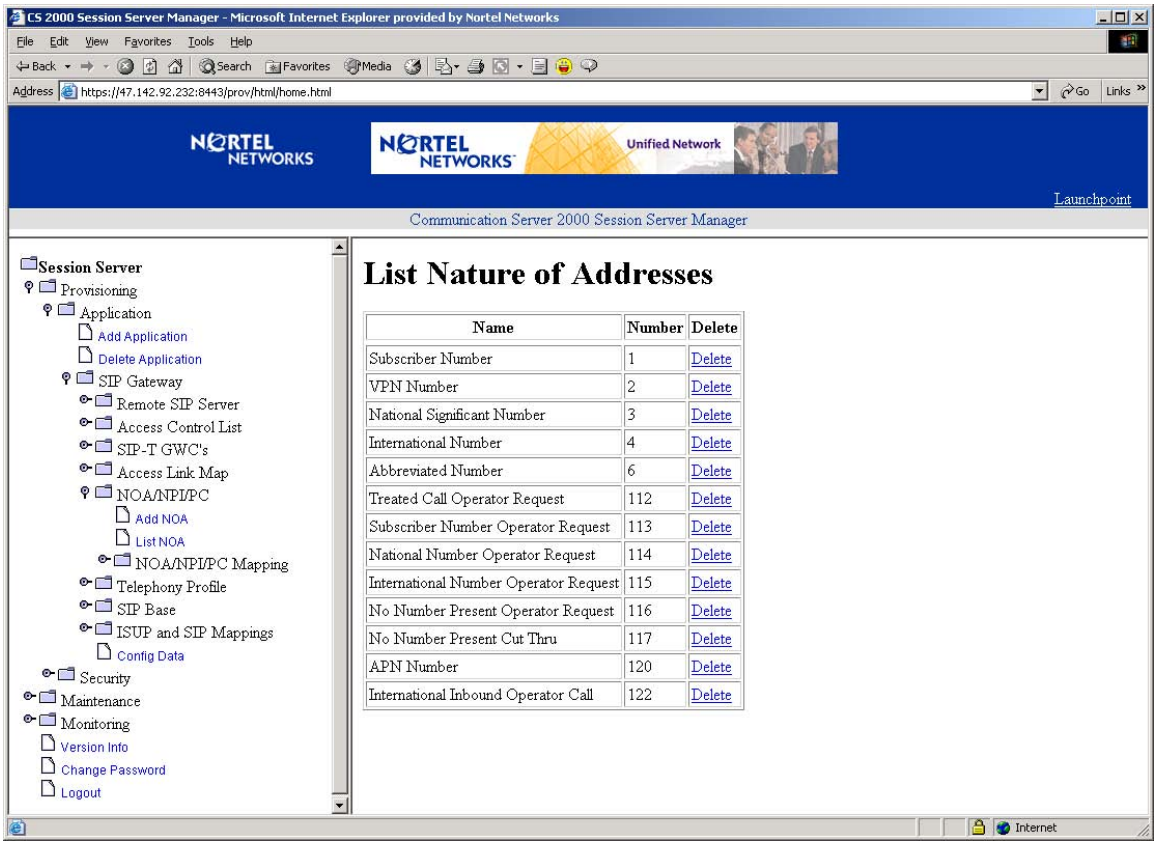


Figure 6 View of List NOA after Deletion of Entry

1.1.2.3 Addition, Deletion and Listing of Phone Context Mappings

Select the NOA/NPI/PC Mapping menu option to display Add Mapping, Delete Mapping and List Mappings menu options.

Select Add Mapping menu option to add a new NOA/NPI to Phone-Context mapping. Type in the New Mapping Name and select a Base Mapping Name from the pull down menu from the designed input areas and then click the Add button to complete the adding of the new mapping.

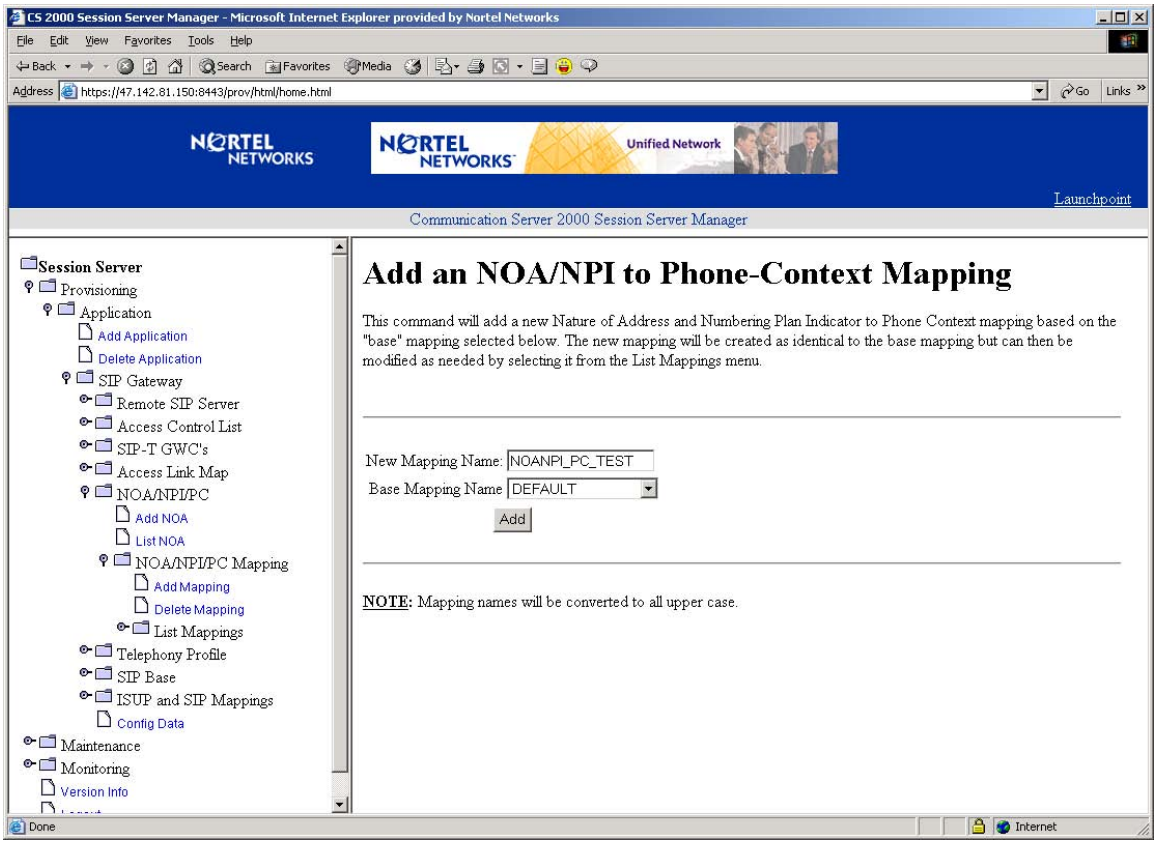


Figure 7 Add a NOA/NPI to Phone-Context Mapping

Click the Add button to add tuples to this new mapping.

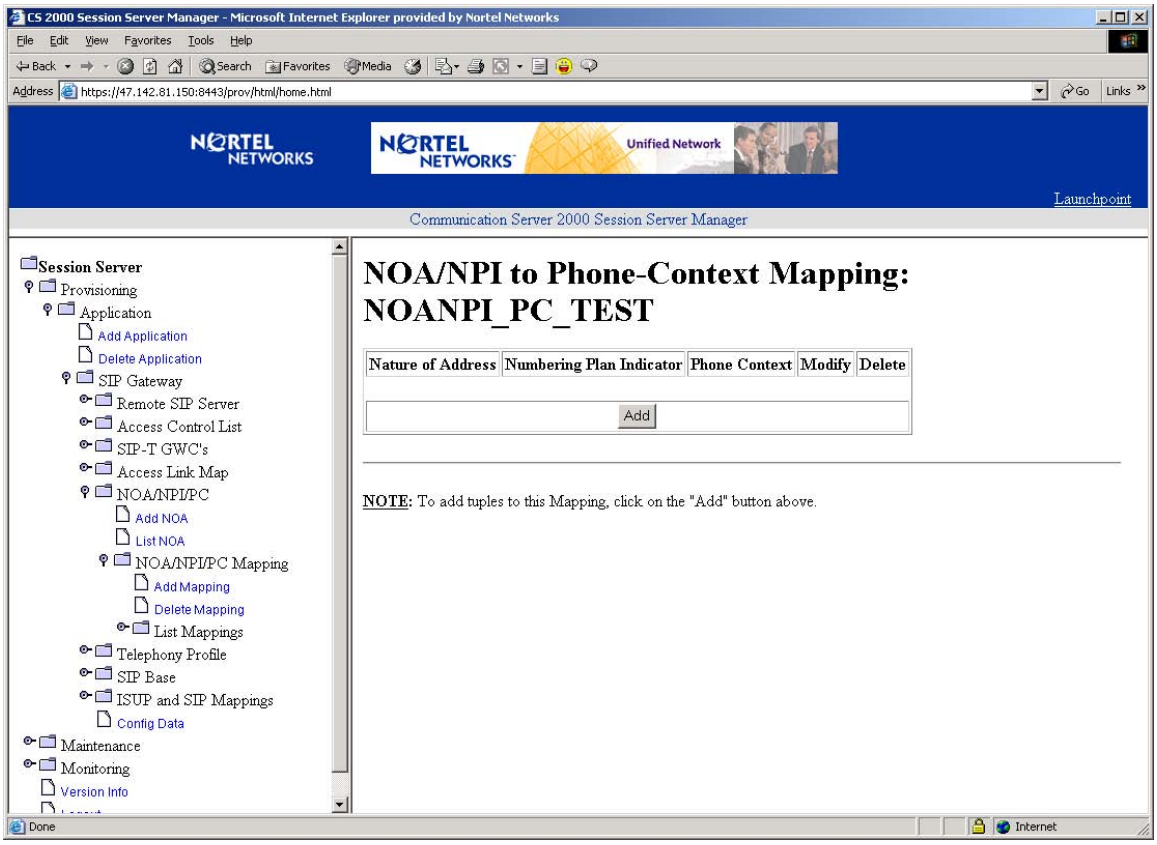


Figure 8 New Mapping NOANPI_PC_TEST View

Select Nature of Address and Numbering Plan Indicator from the pull down menus and type in the Phone Context name for this new tuple entry at the designated input areas. Click the Add button to add the new tuple.

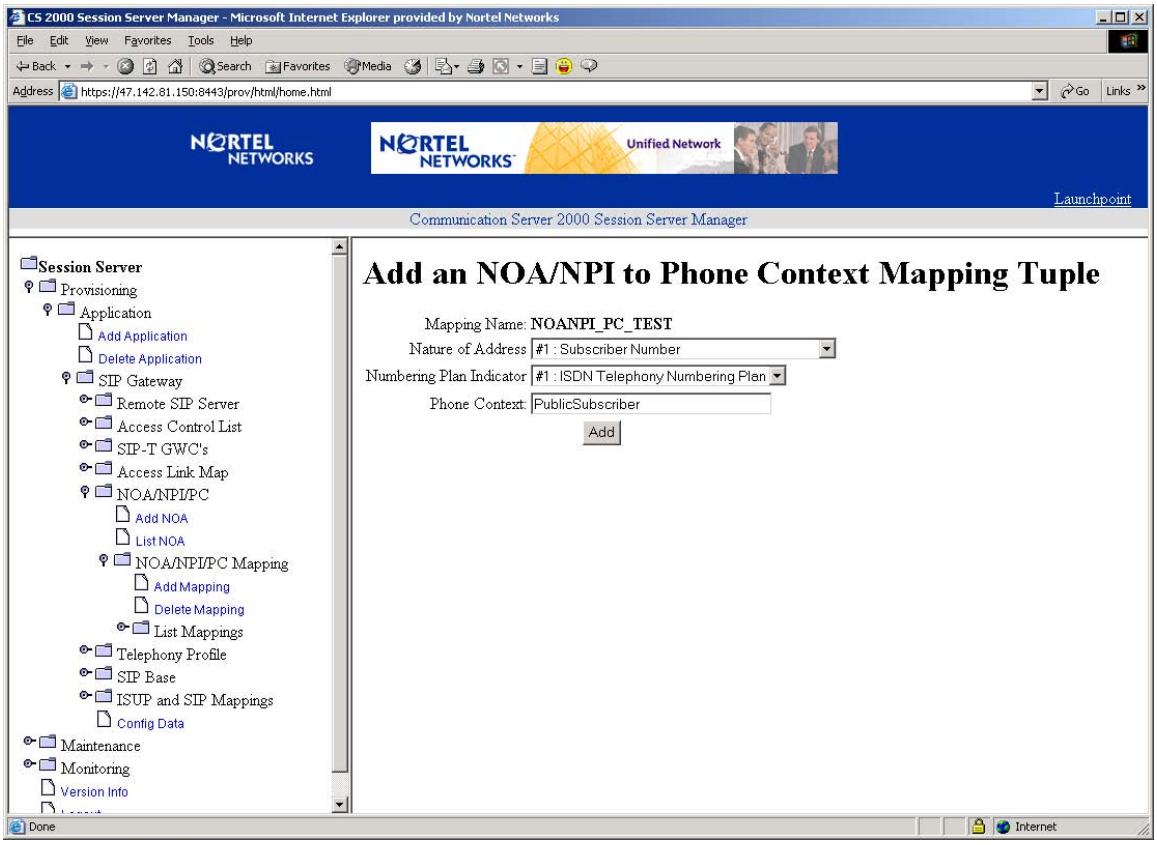


Figure 9 Add New Tuple to Mapping

If invalid selection is entered, a validation pop-up window will appear. Click OK to continue entering tuples for the mapping.

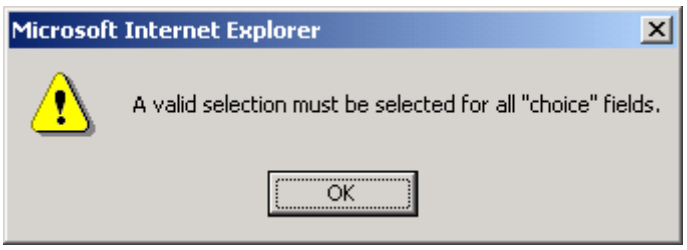


Figure 10 Invalid Selection Validation Pop-up Window

After each successful tuple addition for the mapping, the current list of tuples will be displayed.

To modify a tuple from the mapping, select Modify for the tuple.

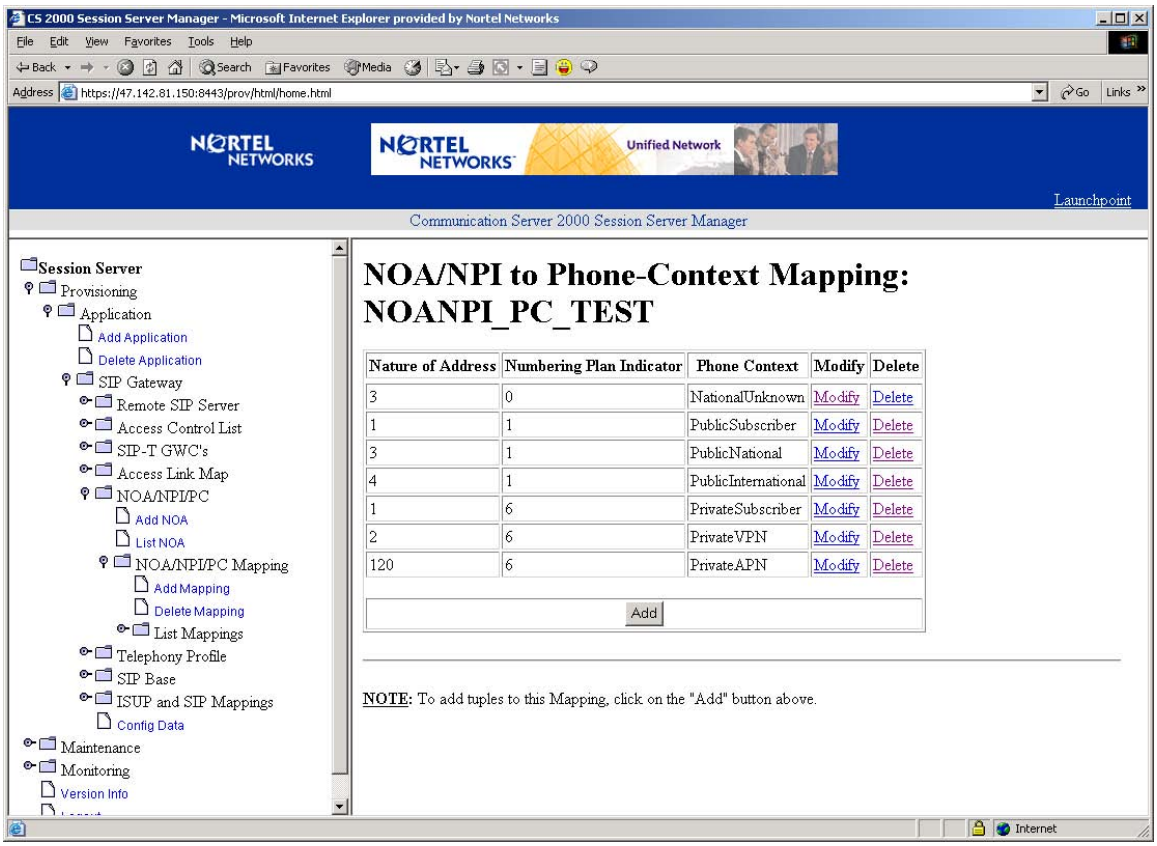


Figure 11 Tuple Listing for NOANPI_PC_TEST

The only tuple entity that can be modified is the Phone Context field.

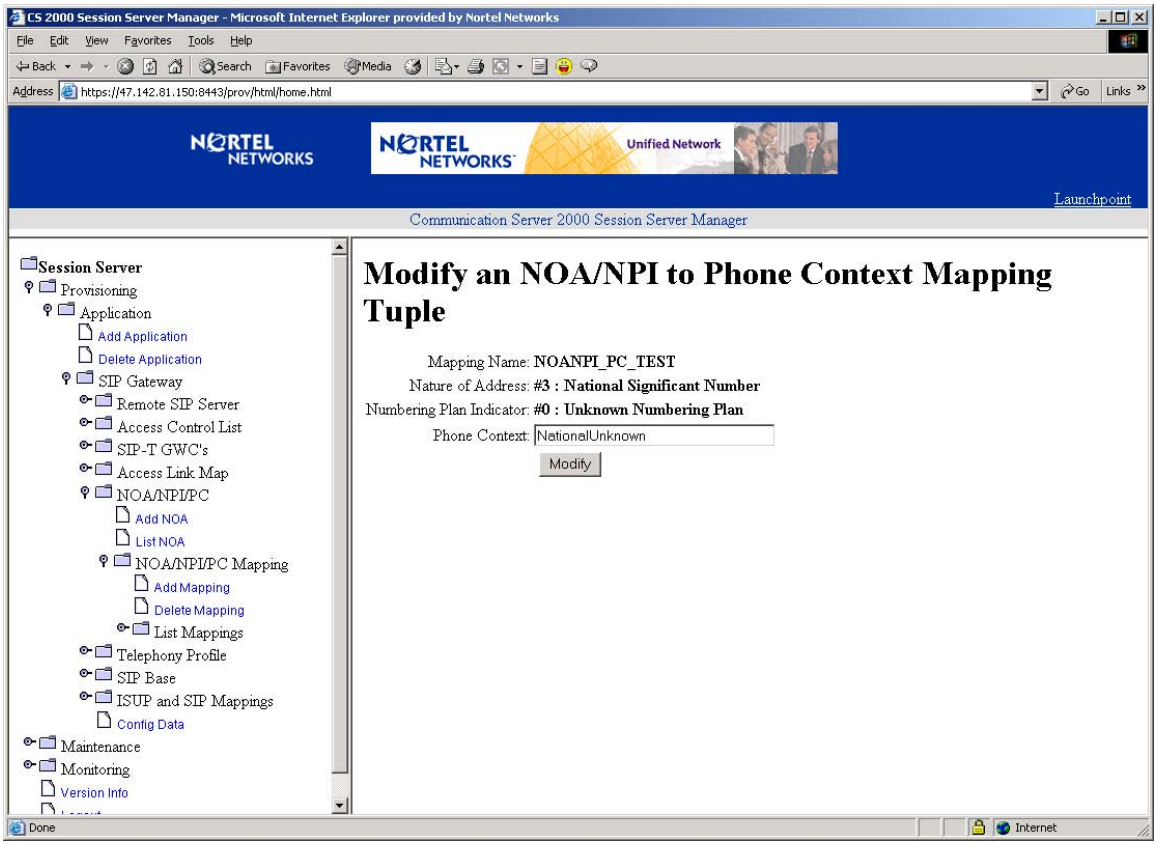


Figure 12 Modify a NOA/NPI to PC Mapping Tuple

Change the Phone Context field to the desired context then click the Modify button.

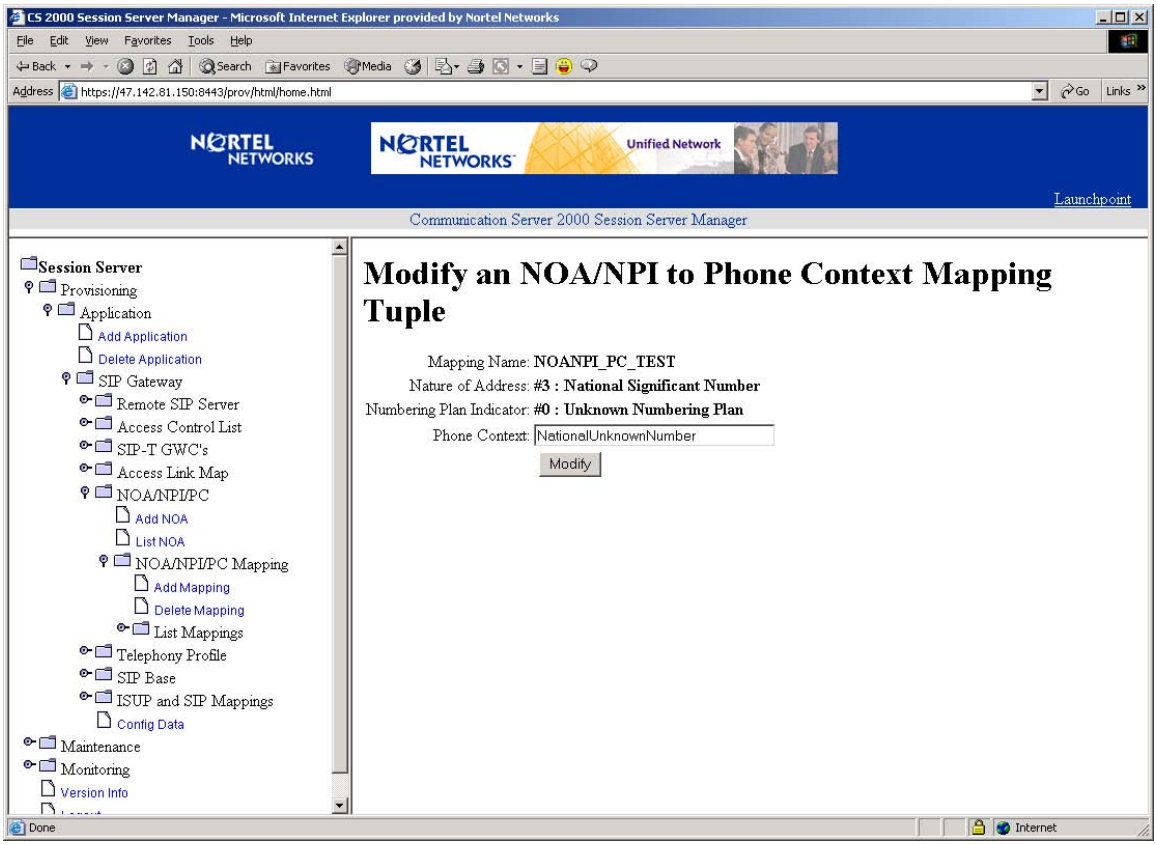


Figure 13 Modify Phone Context NationalUnknown

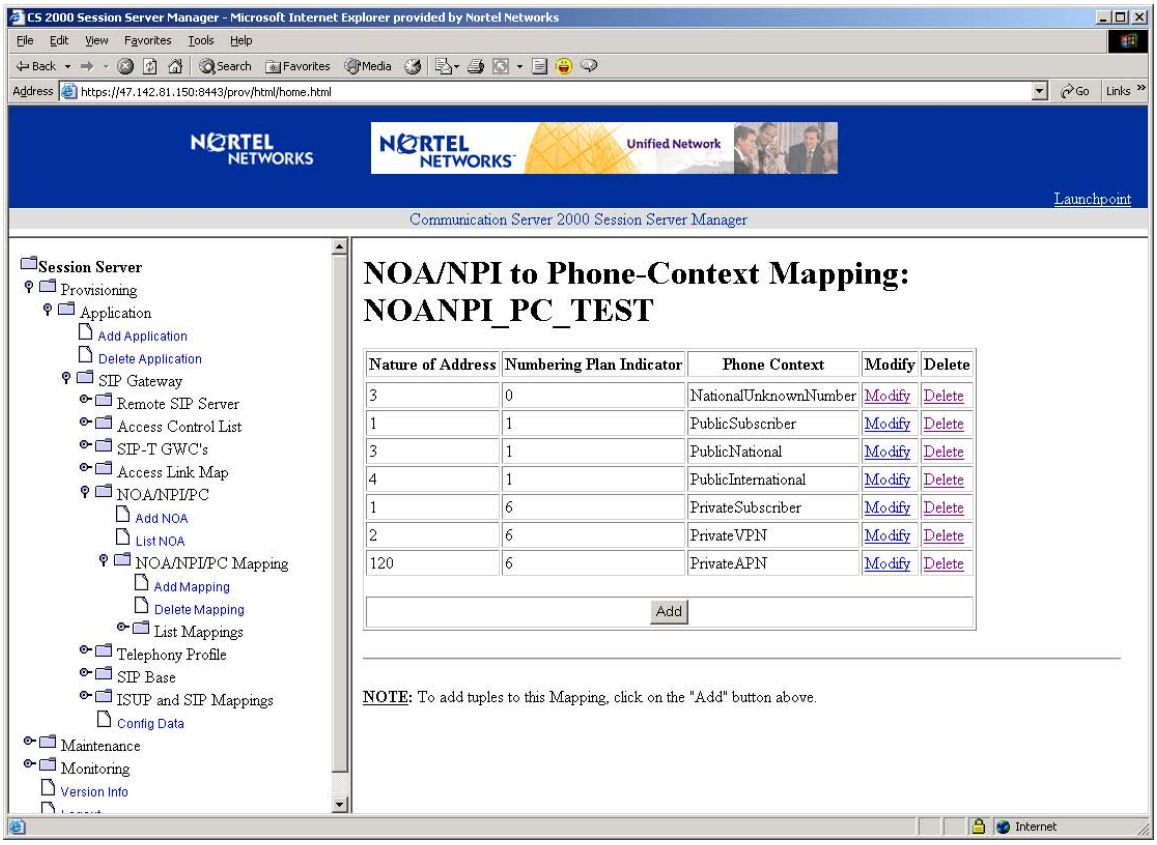


Figure 14 New Mapping Listing with Modified NationalUnknownNumber Tuple

To delete a tuple entry, click Delete for the tuple entry to be removed and select OK in the validation pop-up window.

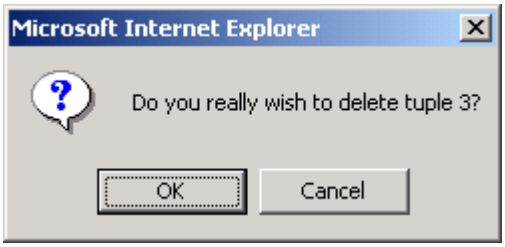


Figure 15 Delete Tuple Validation Pop-up Window

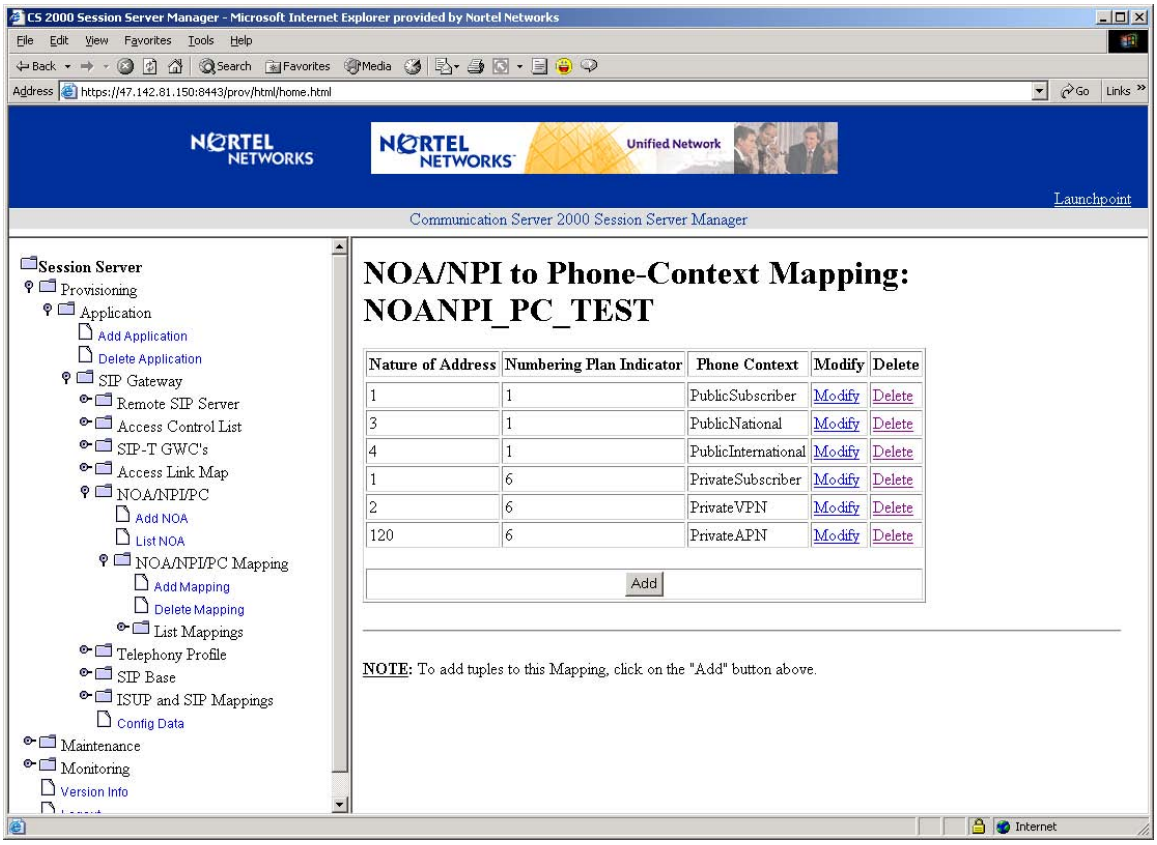


Figure 16 New Mapping Listing with NationalUnknownNumber Tuple Deleted

To view the list of phone-context mappings, select the List Mappings menu option.

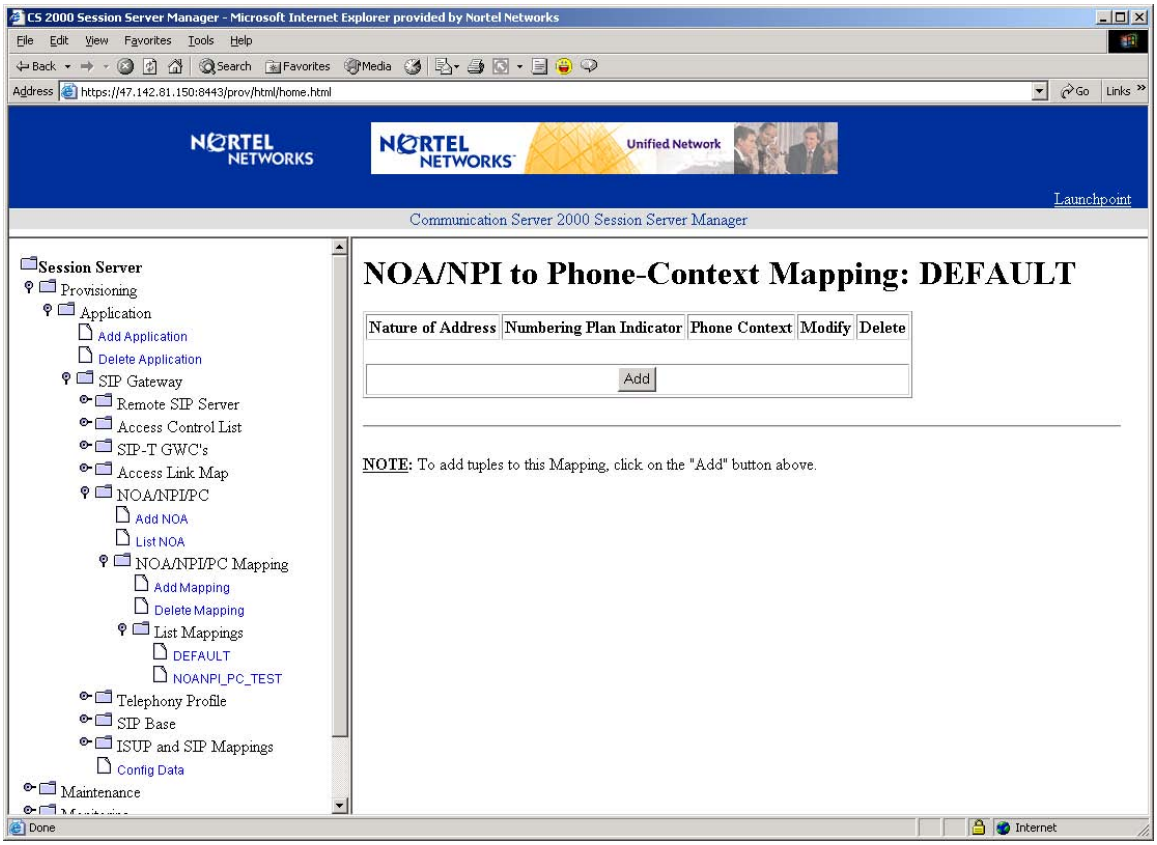


Figure 17 View of Phone-Context Mapping for DEFAULT

To view the tuples of a particular mapping, click on the mapping name under the List Mappings heading from the menu option section.

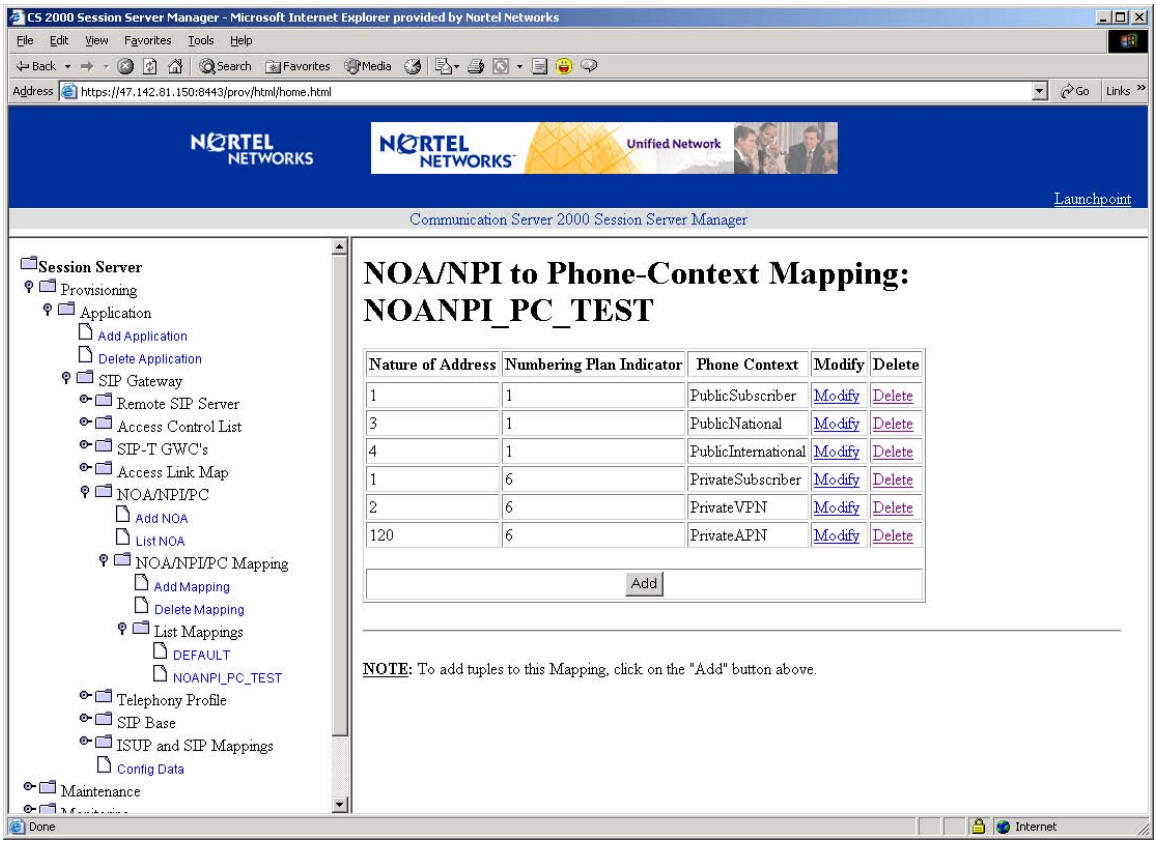


Figure 18 View of Phone-Context Mapping for NOANPI_PC_TEST

To access the section to delete a NOA/NPI to PC mapping, select the Delete Mapping menu option.

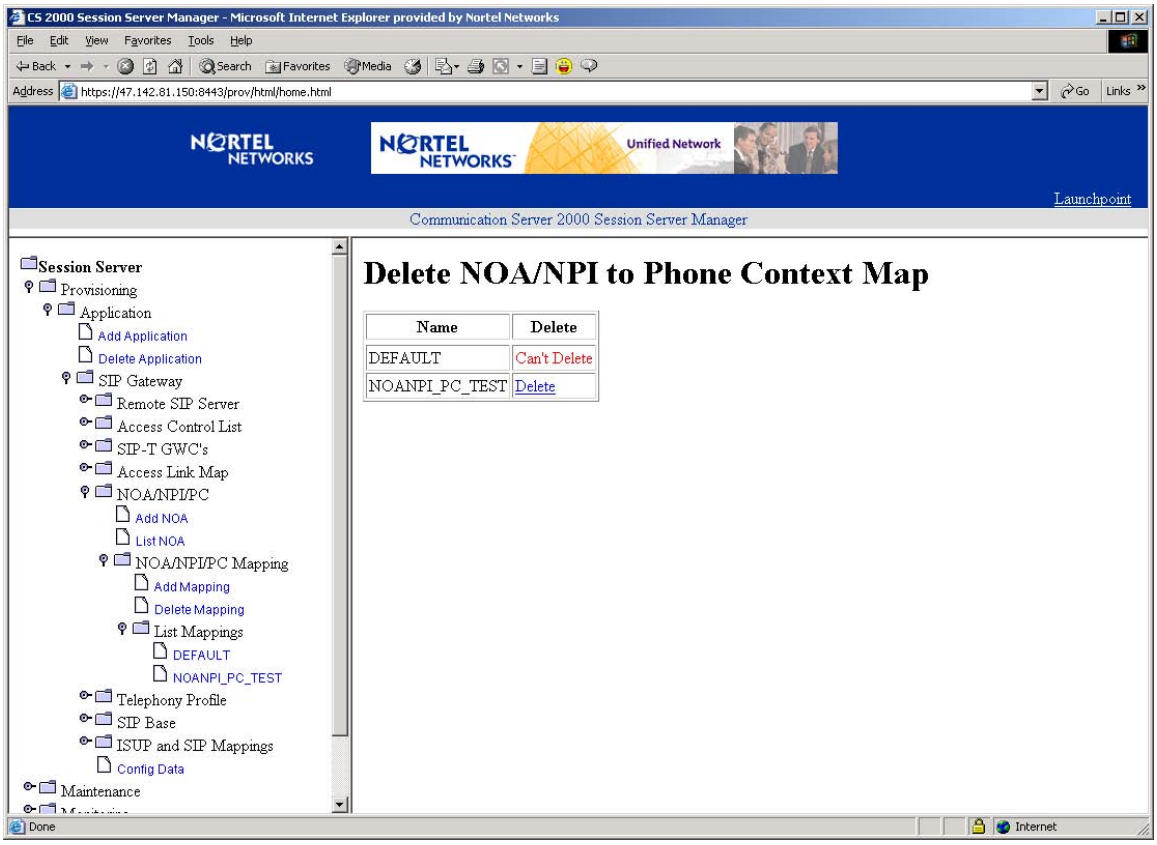


Figure 19 Delete NOA/NPI to Phone Context Map

To delete a phone context map, click Delete for the map entry to be removed and select OK in the validation pop-up window.

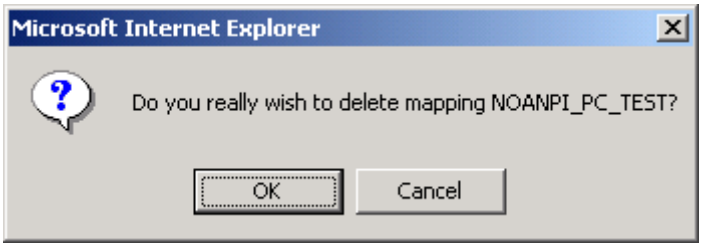


Figure 20 Delete Mapping Validation Pop-up Window

The phone context map has been removed.

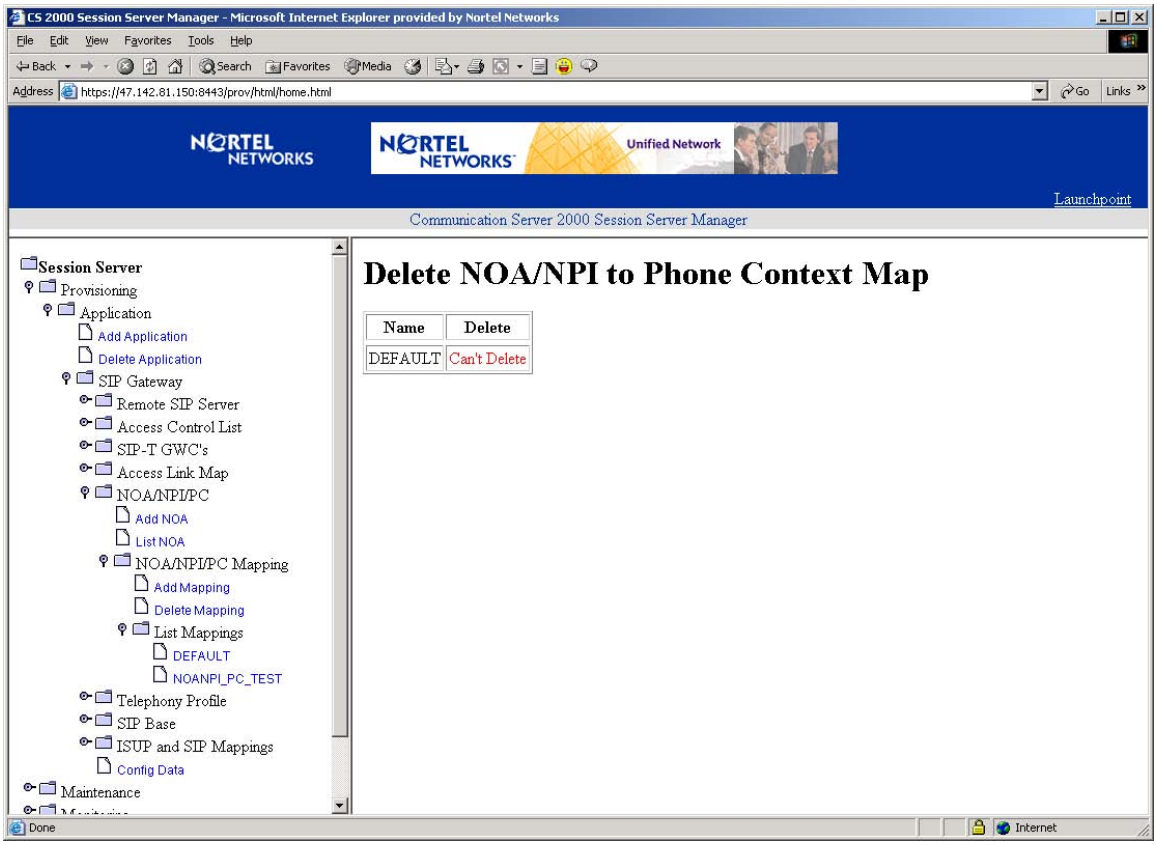


Figure 21 Delete NOA/NPI to Phone Context Map without NOANPI_PC_TEST Map

To refresh the map entries in the menu options column, select List Mappings menu option to hide mappings.

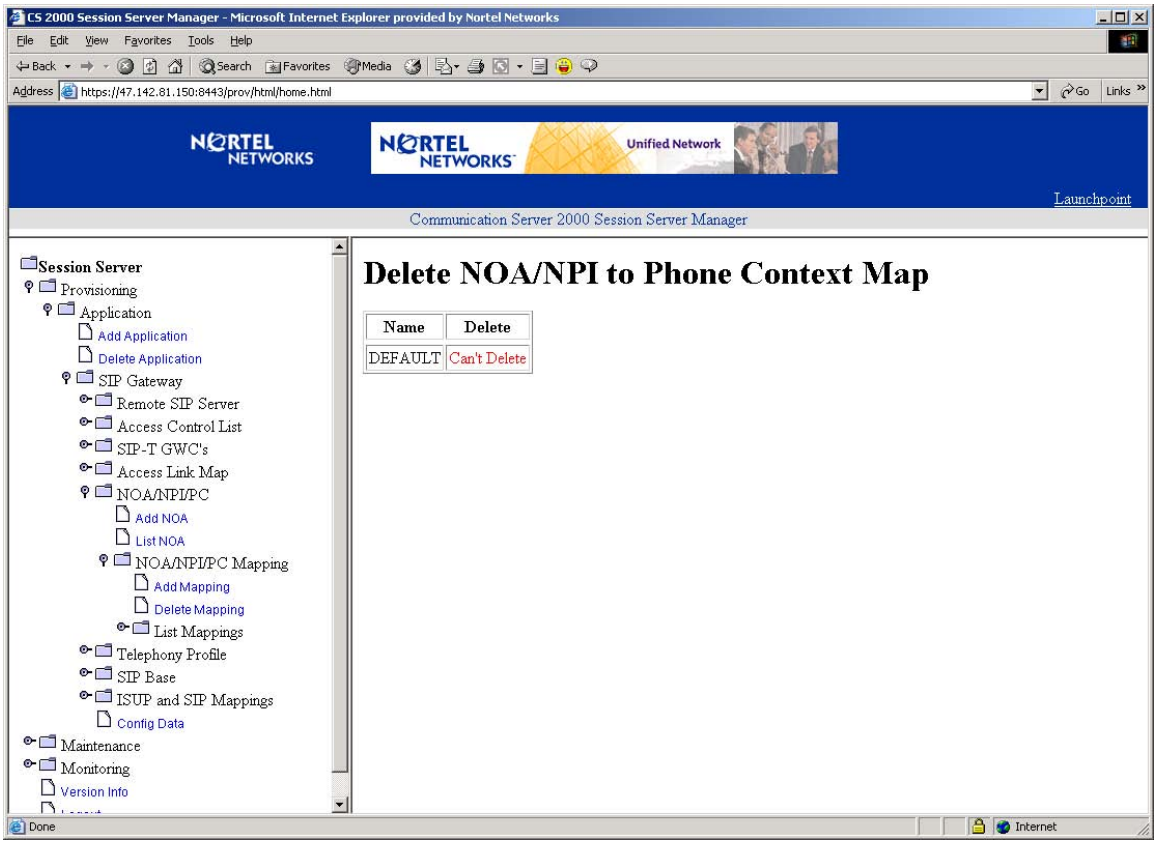


Figure 22 Hide List Mappings

To redisplay the new mappings, select List Mappings again.

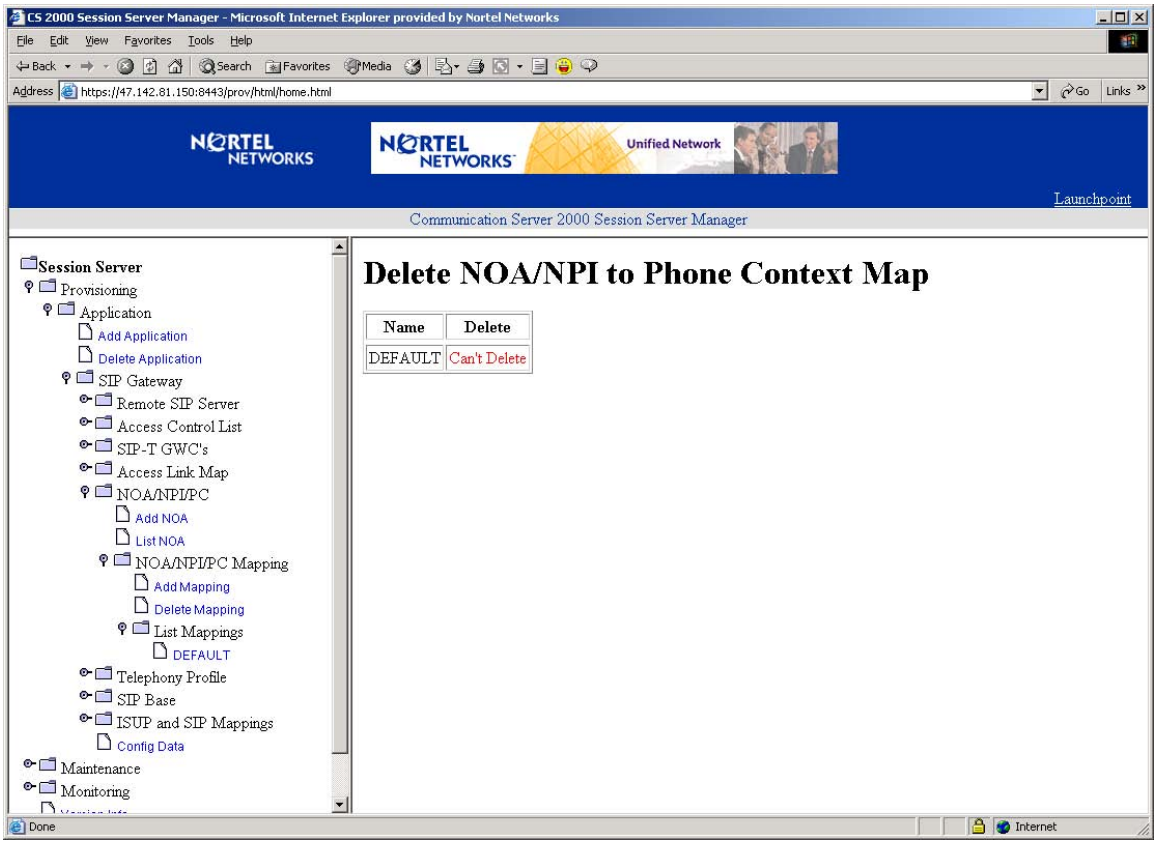


Figure 23 Display List Mappings

1.1.2.4 OOB DTMF Payload section access

Once logged in and having accessed the Succession Communication Server 2000 Session Server Manager link, select Provisioning -> Application -> SIP Gateway to display the Remote SIP Server section menu option.

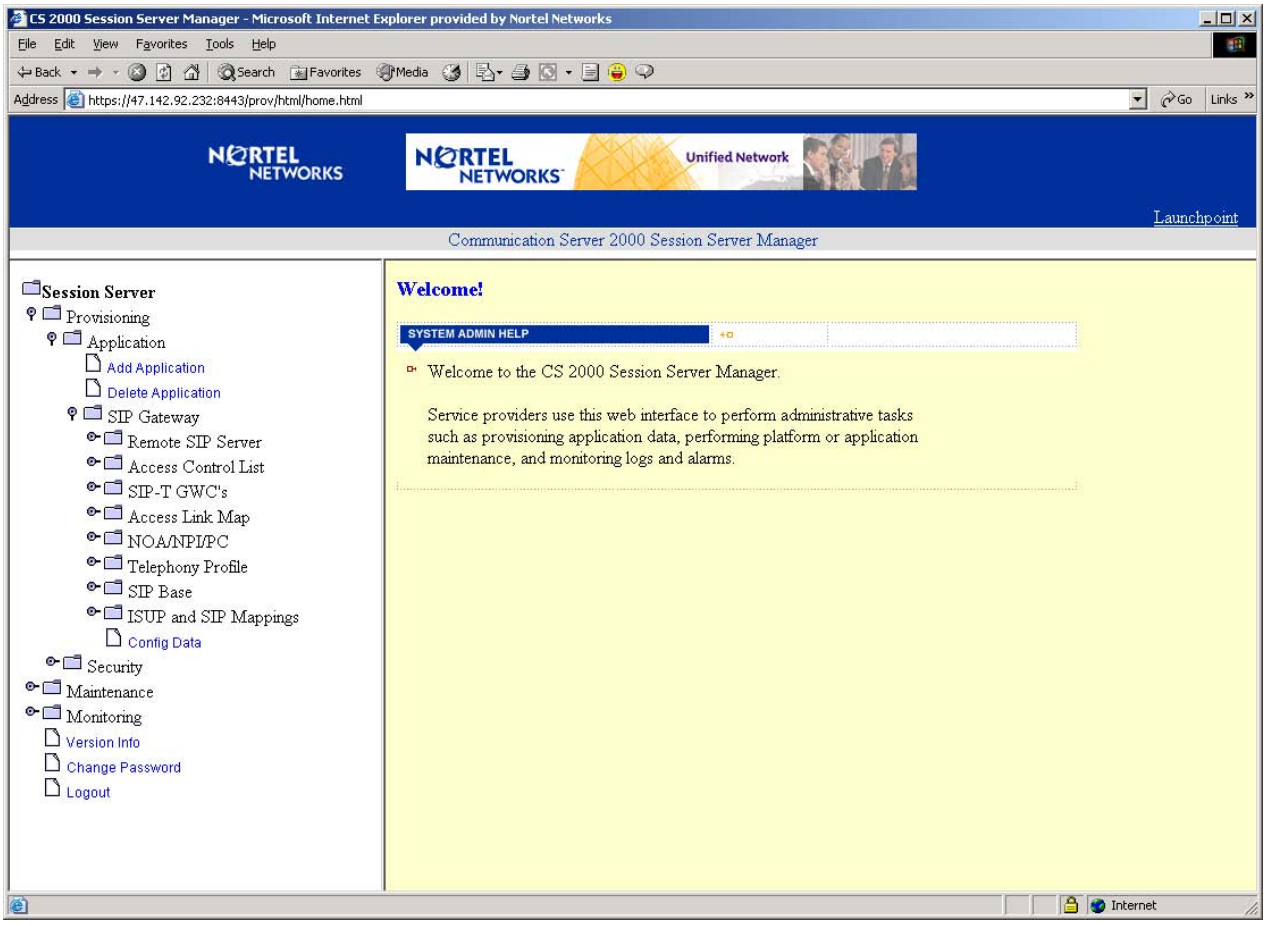


Figure 24 Remote SIP Server section access

Select Remote SIP Server menu option to display the Add Server and List Servers menu options.

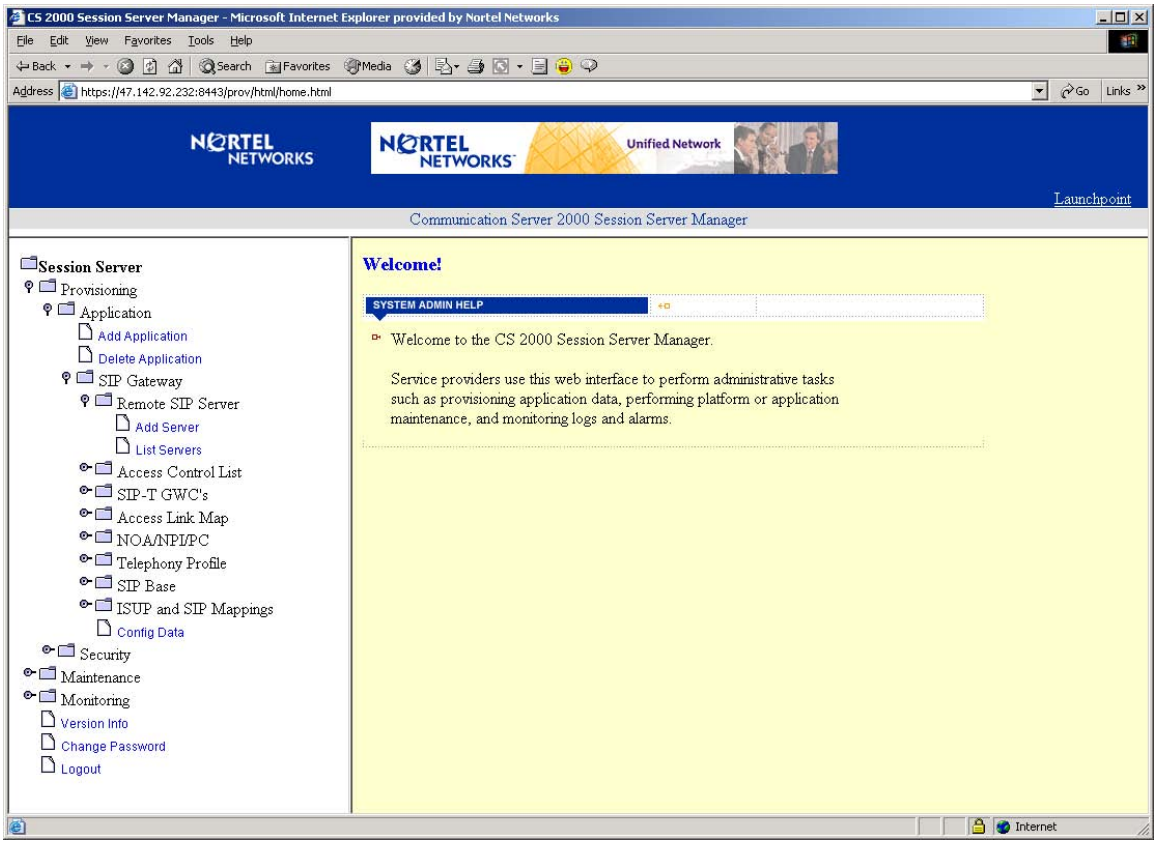


Figure 25 Remote SIP Server

Select List Servers menu option to view the current list of SIP servers.

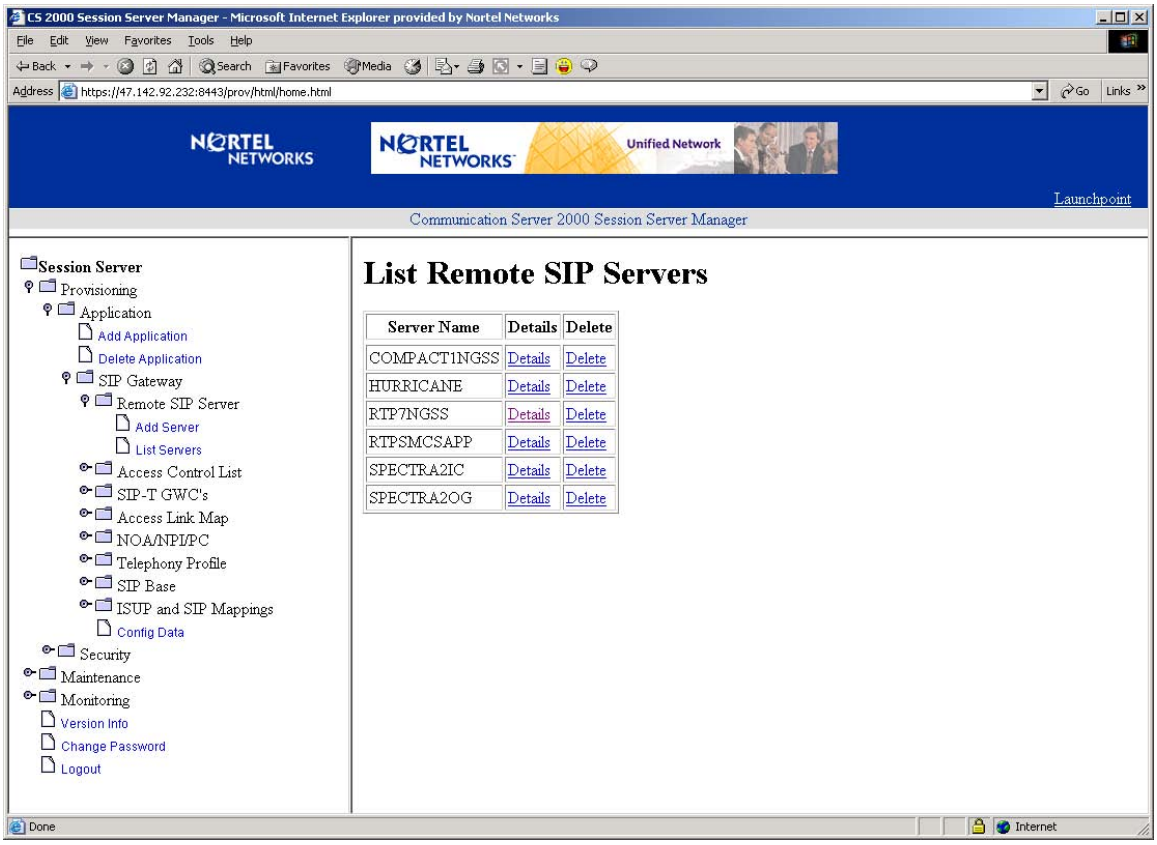


Figure 26 List Remote SIP Servers

To view the details of a particular SIP server, click Details of the Server Name to be viewed.

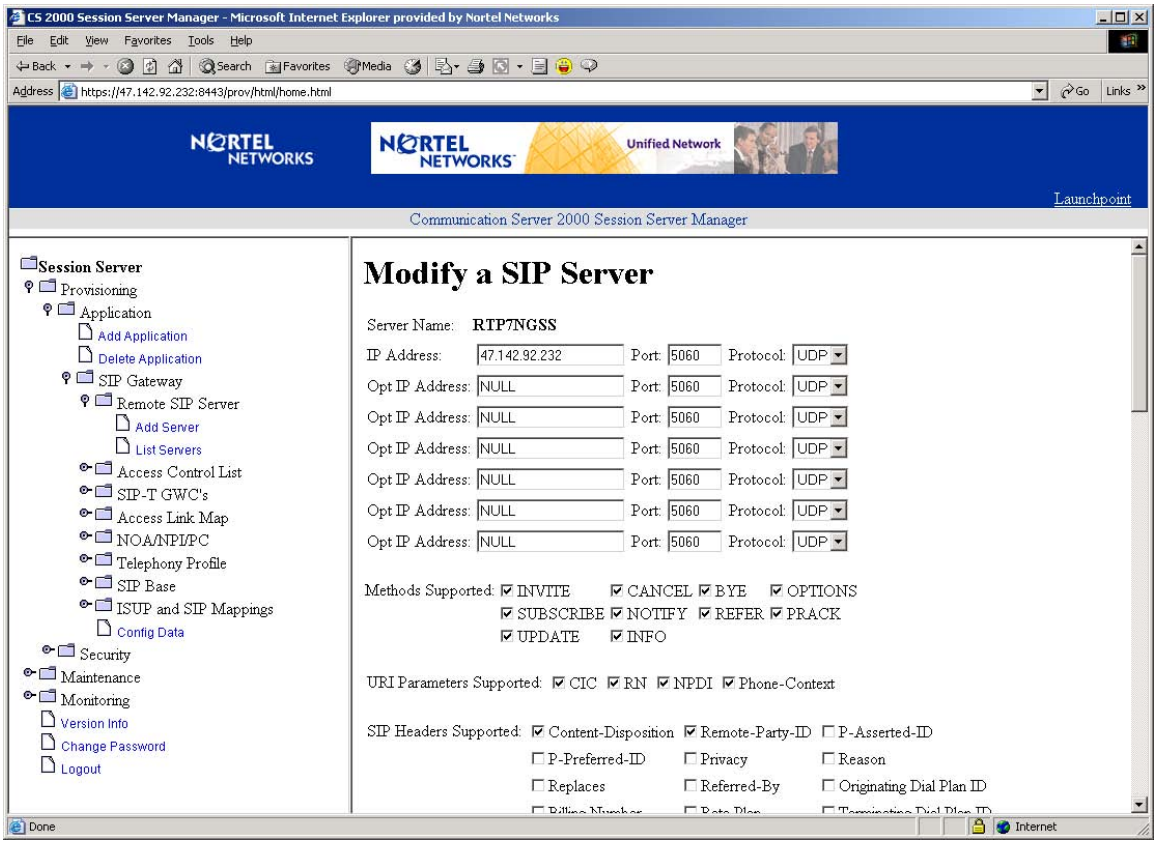


Figure 27 Modify a SIP Server

Scroll down to the Out of Band DTMF Payload option. Select application/vnd.nortelnetworks.digits from the pull down menu for the designated input area.

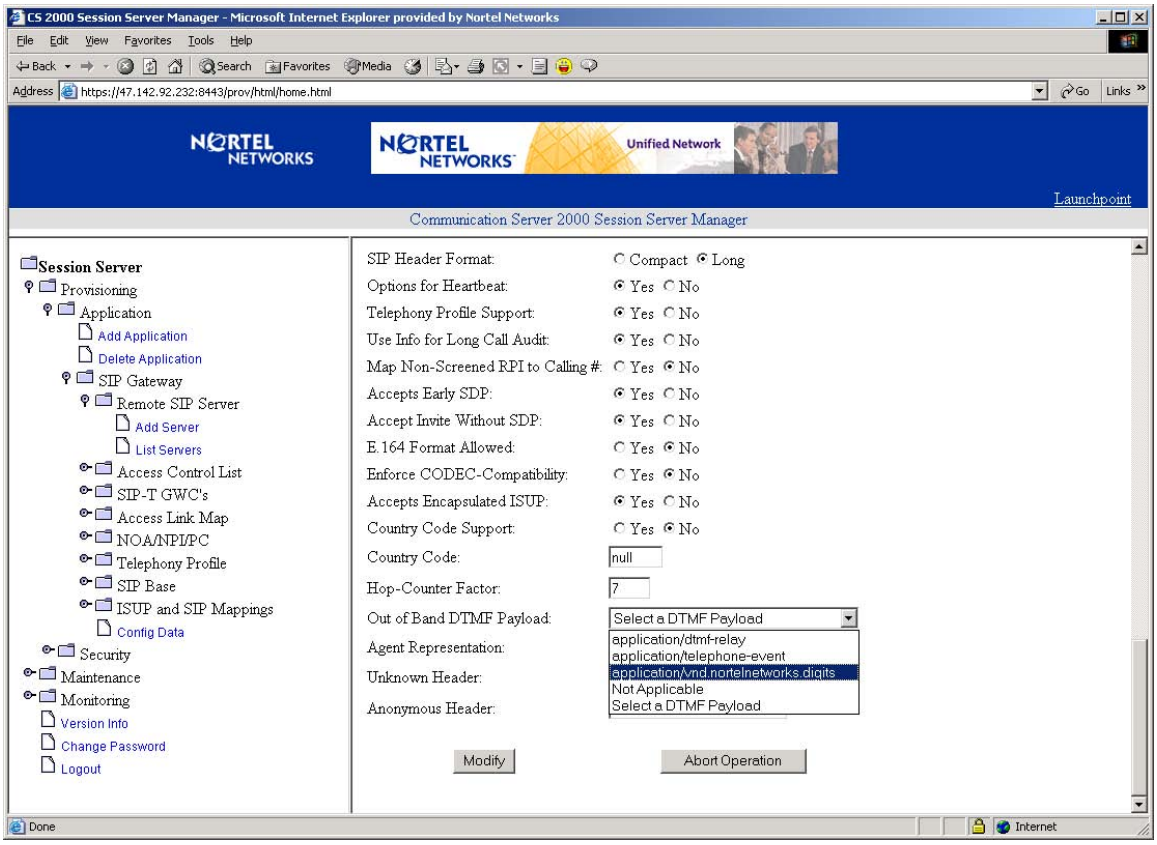


Figure 28 Out of Band DTMF Payload

To discontinue the change, click on the Abort Operation button and select OK in the abort the modification pop-up window.

Figure 29 Abort Modification Validation Pop-up Window

To accept change, click the Modify button and click OK in the modify validation pop-up window.

Figure 30 Modify SIP Server Validation Pop-up Window

To view the SIP server change, select Details of the SIP server that was changed.

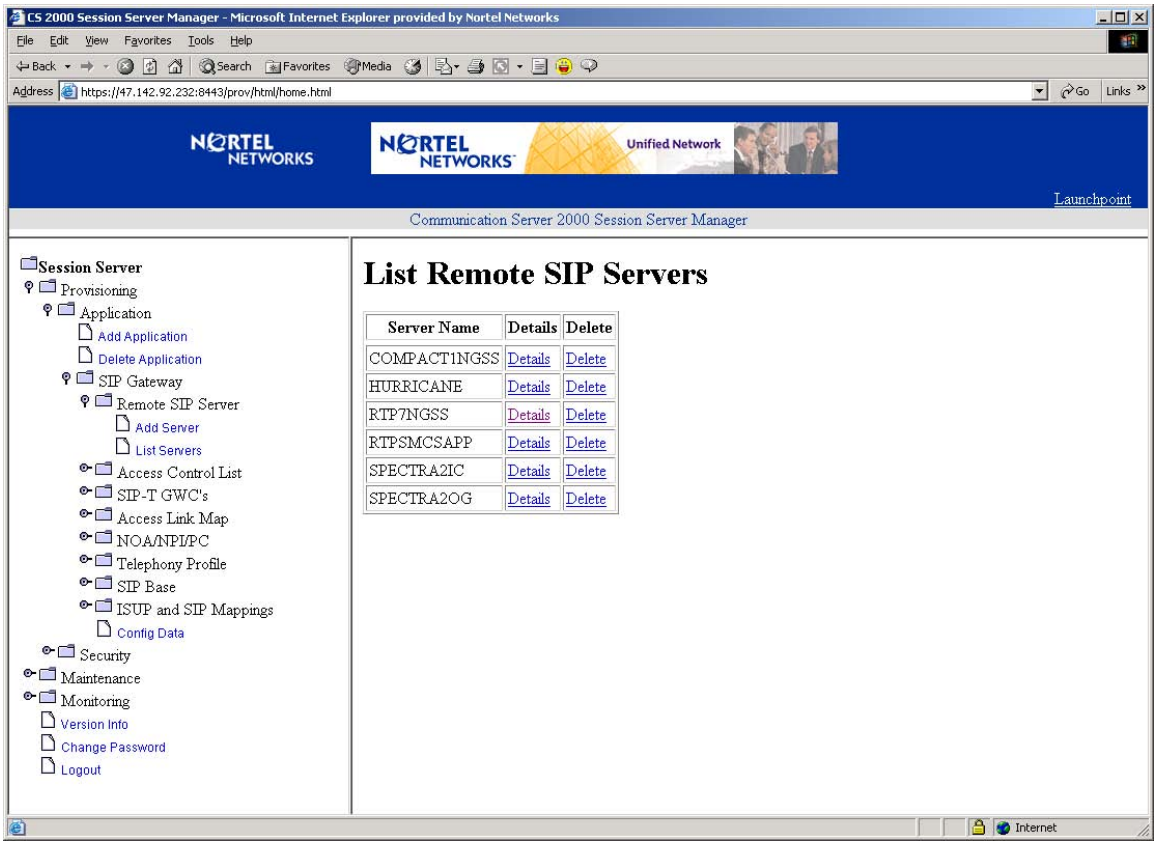


Figure 31 RTP7NGSS after Server Modification

1.1.3 Support for SIP INFO Method

Using SIP protocol, applications can establish and terminate multimedia sessions. Telephony applications that require mid session signalling, such as

voice mail and meet-me conference, can accomplish that task by using one of the following ways:

RFC2833 - This standard is for defining the mechanism to encode DTMF tones within the Gate Ways (GW) and has already been implemented by most GWs.

Use of SIP INFO Message: This method is used to collect and transport DTMF digits. This activity will implements the use of SIP INFO method in Next Gen Session Server (NGSS).

A trunk option has been defined in NGSS GUI to send Out-Of-Band (OOB) DTMF tones. This option is set only if the remote server does not support RFC2833.

1.1.3.1 Outgoing CS2K Calls

When a user presses a digit on the keypad, PVG GW informs Tandem GWC about the digit. Tandem GWC sends INFORM message to the SIP GWC with digit payload. SIP GWC sends a GCP message to the Session Server (NGSS) with the tone information. NGSS checks the trunk options and if the option is **vnd.nortelnetworks.digits** OOB signalling will be used. In this case the INFO message with the DTMF payload will be sent to the remote server.

Following is a sample of the INFO message sent to the remote server:

```
INFO sip:123456@47.104.11.31:5060 SIP/2.0
v: SIP/2.0/UDP 47.104.11.207:5060
t:
<sip:123456;phone-context=myContext@enterprise.com;user=phone>;ta
g=345496207
f: UserA <sip:userA@enterprise.com>;tag=1652960069
m: <userA@47.104.11.205:5060;transport=udp>
i: 351f114f_f46db6dfe9@zngcs01
CSeq: 79007 INFO
c: application/vnd.nortelnetworks.digits
l: 35
p=Digit-Collection
y=Digits
d=1
```

Note that for outgoing CS2K calls, CS2K will send the INFO with digits to MCS only in a 323-SIP_MCS inter-working when the originating 323 does not support RFC2833.

1.1.3.2 Incoming CS2K Calls

For incoming CS2K calls, once NGSS receives an INFO message, the trunk option is checked and if **vnd.nortelnetworks.digits** is present, the new INFO template is used to parse the message and extract the digits.

1.1.4 Support for Public and Private Name/Number Display

In MCS09/SN09, enhancements are being made to extended the concepts of Public and Private Name and Number display within Centrex customer groups across the MCS CD (Converged Desktop) services. Enhancements to MCS are made under the feature A00009905, “Private Public Name and Number Display”. Enhancements are made to display the Private Name / Number information to the called party within the same Centrex group and the Public Name/Number to the called party outside the Centrex group.

Directory Numbers within a Centrex customer group can be provisioned with a Public Display Name and a Private Display Name. Centrex features allow the Private Name and Number to be displayed on calls between parties within the same Centrex customer group. They also allow the Public Name and Number to be displayed when the parties are not in the same Centrex customer group, such as when one of the parties is a PSTN caller.

Using MBG over IT trunks allows Centrex customer groups and their related services to be extended to Directory Numbers hosted off of different DMS switches. In the following figure, if party A and party B are in the same Centrex group, the Private Name and Number can be displayed.

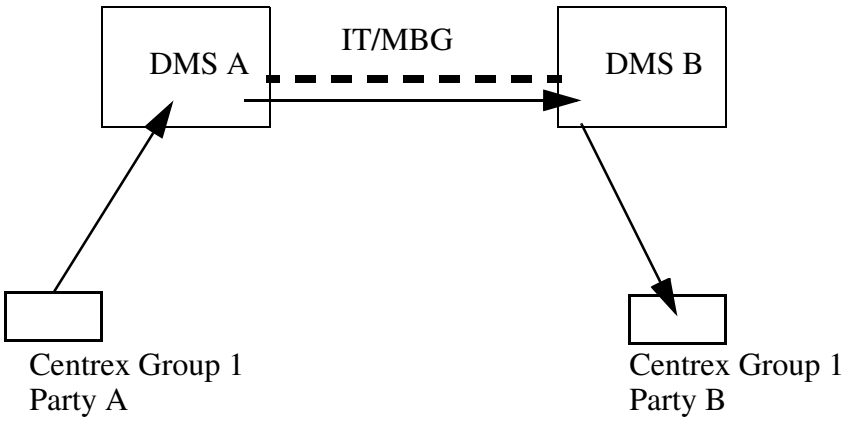


Figure 32 Extension of Centrex Groups using MBG

As in the following diagram, if one of the parties is a PSTN caller, the Public Name and Number can be displayed.

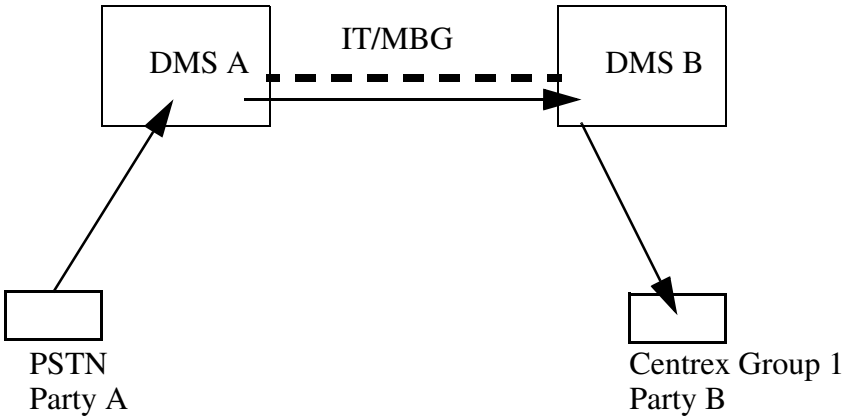


Figure 33 Call from outside the Centrex Group

The equivalent of a Centrex business group on the MCS system is a domain or sub-domain. A Private call is made within the domain or sub-domain. A Public call is one made outside the domain boundaries.

MCS CD functionality allows users to have an MCS Multimedia PC Client that can be used with a headset for VoIP telephony calls, as well as a PAD (Personal Audio Device) that can be an office telephone. The MCS PC Client has a display window that displays call status and can be used to control interactions between the Desktop telephone and the PC Client, such as controlling which phone to ring.

A basic diagram of a Converged Desktop system configuration is shown below.

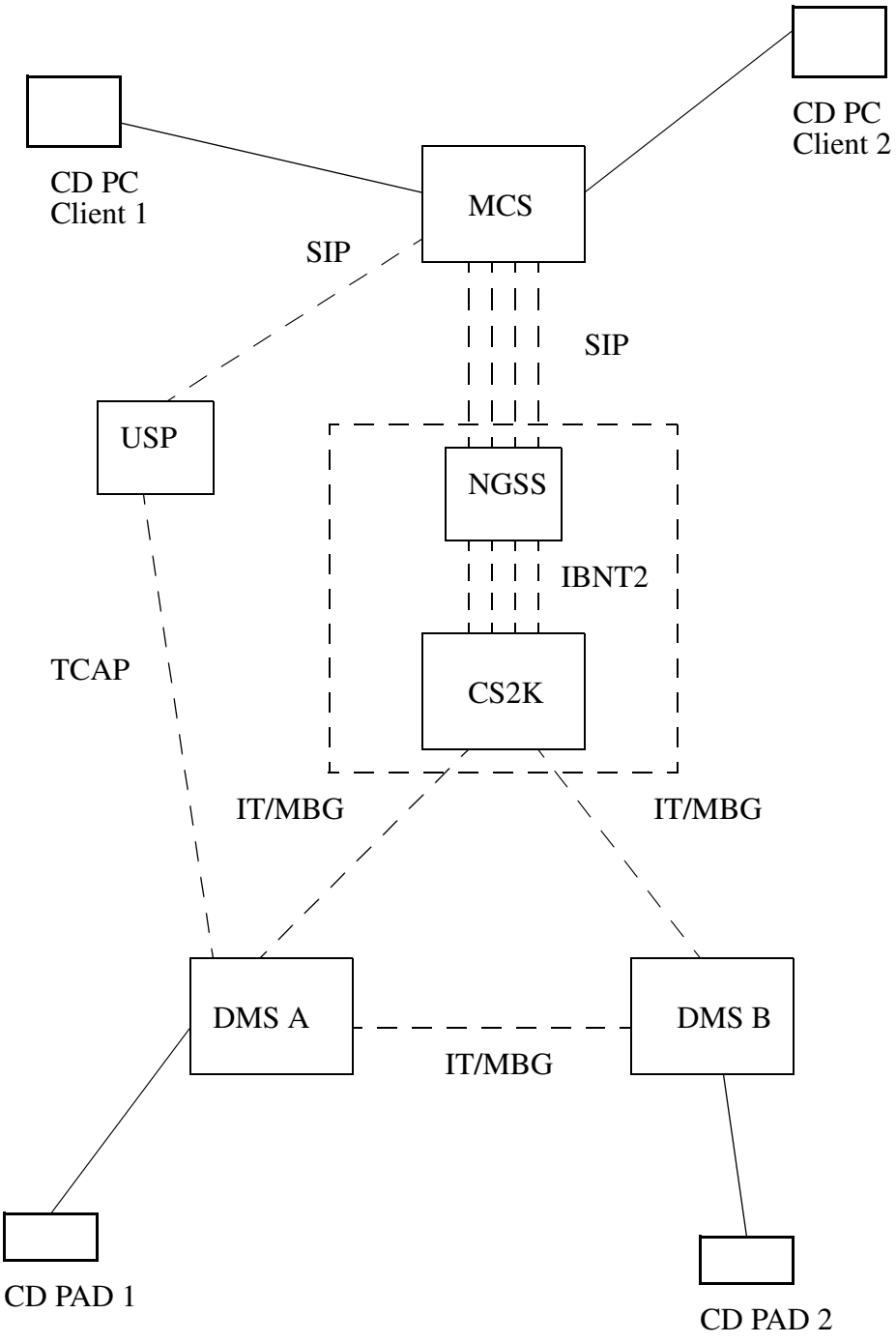


Figure 34 Converged Desktop Network Diagram

IT/MBG trunks are provisioned between DMS 100s and the CS2K to be shared among customer groups (the DMS end office could also be a CS2K). MBG allows members of the same Centrex customer group to be known across different DMSs. IBNT2 SIP trunks are provisioned between the CS2K and the MCS, one dedicated per customer group.

The NGSS acts as the interface between the MCS and CS2K DPT trunking. The NGSS communicates using GCP protocol on the DPT trunks through a SIPT Gateway Controller. It communicates with the MCS using SIP. The IT/MBG trunks are ISUP trunks.

The USP provides an SS7 TCAP interface for the DMSs, and a SIP interface for the MCS.

CD User 1 has a CD PC Client and a CD PAD, as does CD User 2.

In the CD environment, there exists a number of complex call flows. Within these call flows, the Name and Number Displays on the CD PADS and on the CD PC Clients need to be consistent in terms of whether the Private or Public displays are used. If the two CD PADs are within the same Centrex business group, the Private Name and Number displays should be maintained.

An example of a complex call flow is given in the figure below.

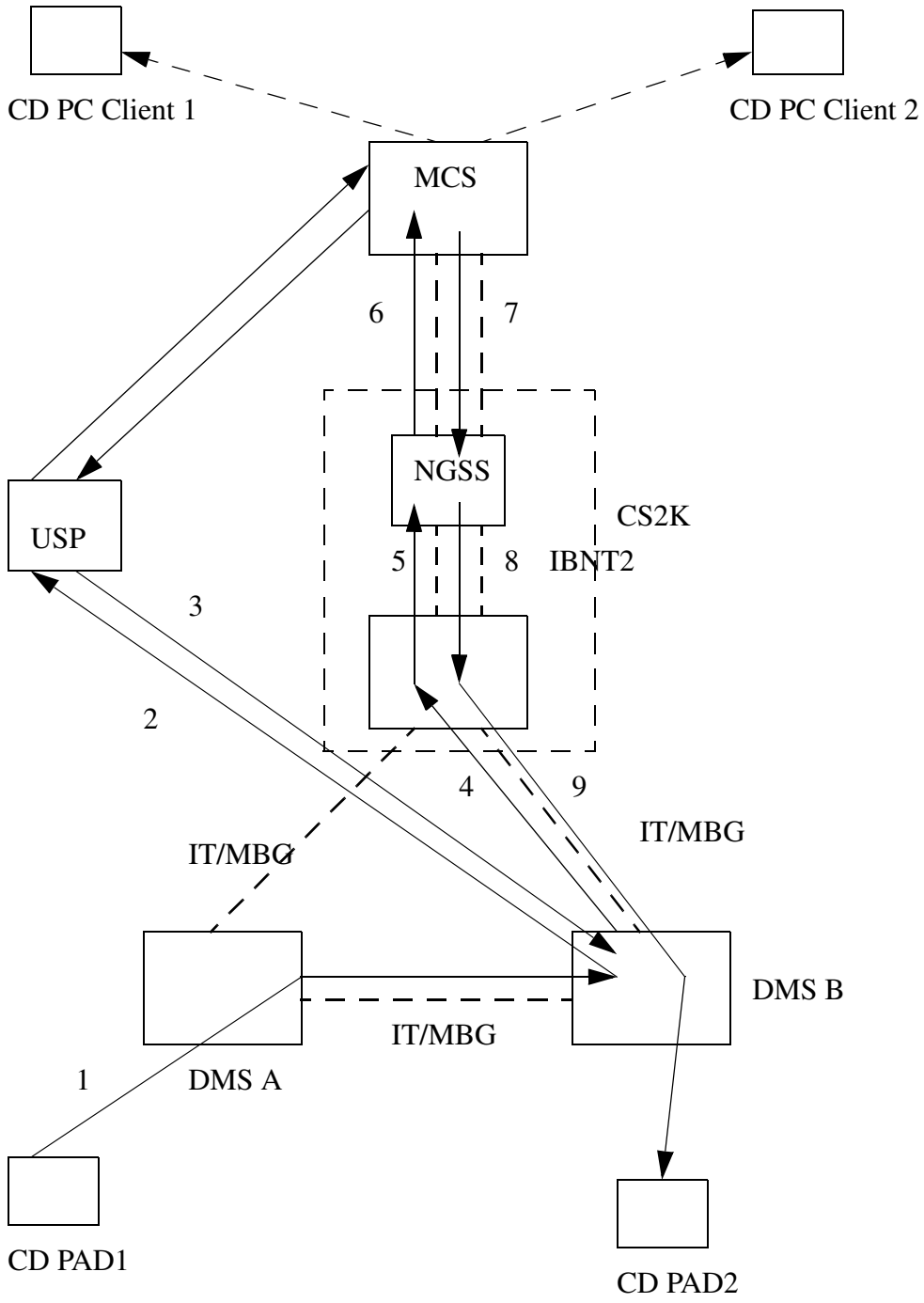


Figure 35 Converged Desktop System Call Flow

In this call, CD PAD1 and CD PAD2 are in the same Centrex group. The steps in the call flow are as follows:

In step 1, CD PAD1 calls CD PAD2. Since CD PAD2 is a converged desktop user, its Directory Number has an AIN TAT trigger associated with it.

This causes step 2, where a TCAP query is generated to the USP, which in communicating with the MCS returns in step 3 the SDN (Converged Desktop Service Directory Number) associated with the Centrex business group of the called party. This is the SDN that the MCS has associated with the sub-domain of the called party. This tells the DMS to route the call to the SDN.

In step 4 the call is routed to the SDN for the business group over an IT/MBG trunk to the CS2K. The identity of the business group is maintained across the ISUP IT trunk by the MBG parameter. At the CS2K in step 5, the call is routed over a dedicated IBNT2 trunk for the business group. In this step, the ISUP call setup information is carried to the NGSS through the GCP protocol. The NGSS converts the call setup information to a SIP INVITE message to be sent to the MCS in step 6. The SIP INVITE message contains an X-Nortel-Profile header that associates the call with the specific business group.

The MCS performs the logic to update the status of the CD PC Client displays. In this call scenario, it is determined that CD User 2 has indicated through configuration that he wants the call to be routed to his telephone, CD PAD2.

In step 7, the MCS routes the call to the NGSS over the route associated with the business group. In step 8, the NGSS routes the call over the IBNT2 DPT trunk associated with the business group to the CS2K. In step 9, the CS2K routes the call over an IT/MBG trunk to DMS B, which, which after making another TAT trigger query to the USP terminates the call the call to CD PAD2.

Since in this scenario both CD users are in the same Centrex business group, the CD PAD2 display will use the Private Name and Numbers. The CD PC Clients displays will also be Private.

A similar call scenerio is shown below, but in this case the calling party is not in the Centrex business group.

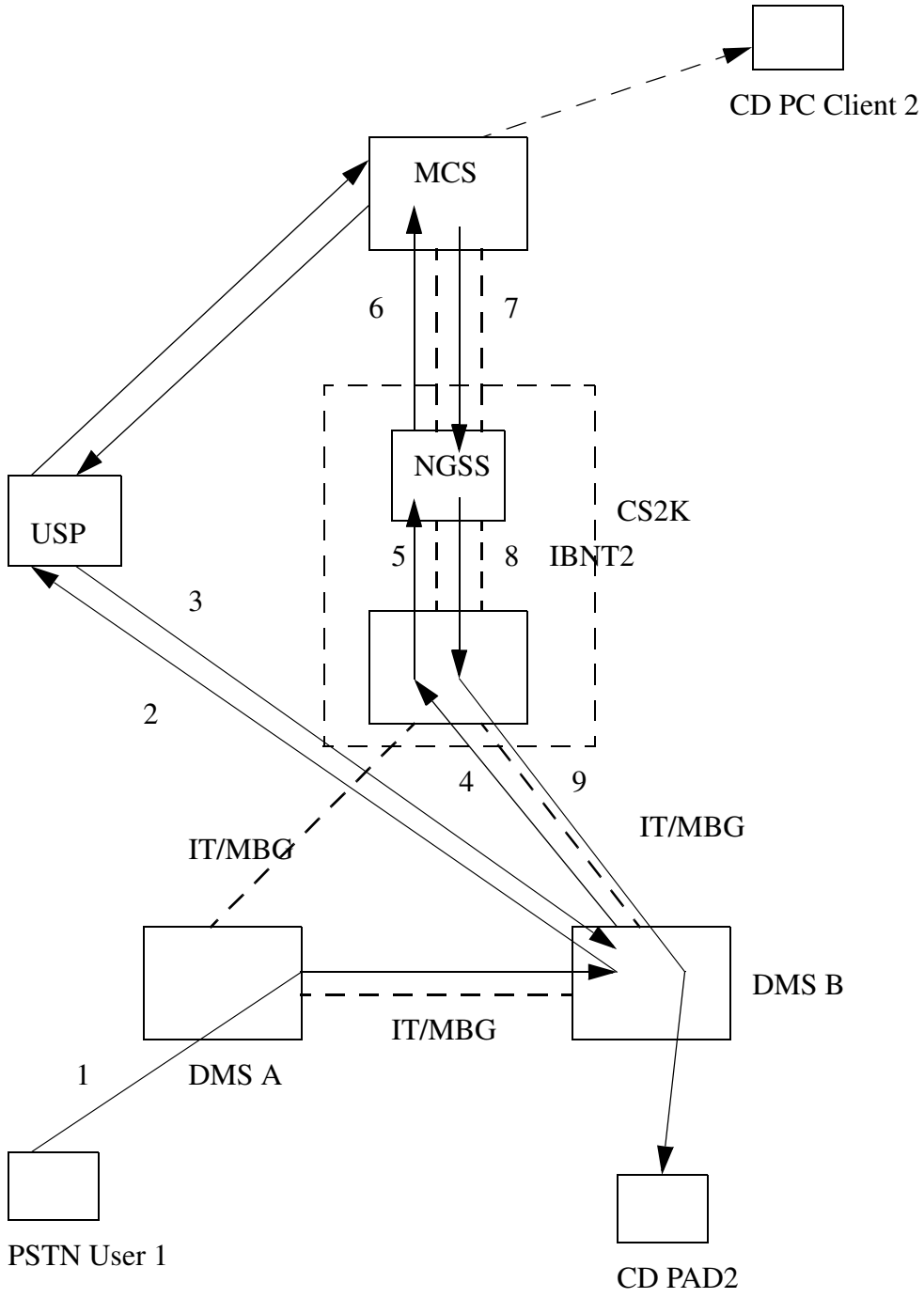


Figure 36 Call from PSTN User to Converged Desktop User

In this call scenario, a PSTN user calls a CD Centrex user; the CD PAD2 display will use the Public Name and Numbers. This display could be something like “PSTN”. The CD PC Client display will also indicate that the caller is outside the Centrex group.

For CD users, name provisioning on the MCS should be consistant with name provisioning on the DMS, since in some cases the MCS provisioned name may be displayed on the PAD.. Reverse translations are used on the DMS to determine the number of digits for the calling number display on the PAD. Display information is also impacted by the amount of available display area of the PAD.

To support Private/Public Name and Number displays in calls that cross between the DMS Centrex group arena into the MCS SIP domain arena, a combination of translations, including utilization of MBG over IT trunks and provisioning of dedicated IBNT2 trunks per Centrex group is used. Additionally, significant software changes are made on the MCS (see feature A00009905, “Private Public Name and Number Display”).

When a call is made to a CD user and a TAT trigger AIN query is launched, the MCS returns a CD Service DN that is in the same sub-domain as the called party number; the call is then forwarded to this Service DN. When the MCS presents a call to a PAD via the CS2K as part of a complex call, the MCS selects the outgoing route based on the original calling party. MCS provisioning routes outgoing calls within the same SIP domain as the original calling number over the dedicated IBNT2 trunk for the business group; CS2K translations will route the call over IT trunks with the associated MBG information for that business group . In addition to the IBNT2 trunks provisioned to serve each customer group, a dedicated “Public” IBNT2 trunk is provisioned. .Outgoing calls to phones outside the SIP domain of thel calling number are routed on the “Public” IBNT2 trunk. CS2K translations do not include MBG for calls coming over this trunk when routing the call over IT trunks.

The MCS can only determine that a call to a CD user is in the same business group if both parties are provisioned on the MCS as CD users. On a call from a non-CD user in the same business group as the called PAD, the MCS will treat it as a public call. In this case, the name and number will be correctly displayed, but some intragroup service logic may not work correctly.

When a call terminates to the PAD of a CD user, since it is actually being redirected by the MCS to the PAD, the display information may indicate that the redirecting party is the CD user itself. Likewise, when a CD user in converged desktop mode initiates a call from the PC Client, the associated PAD will be rung and the display may indicate the user itself as the calling and redirecting party.

A number of call scenarios exist between parties with at least one CD User involved. A summary of some of the expected display behavior in some of these call scenarios is given in the table below. Scenarios 1 -11 apply to Complex CD users; scenarios 12-14 apply to Simplex CD users. CD users are in Converged Desktop (CD) mode unless otherwise noted. Centrex CD users are in the same business group and are provisioned on the MCS in the same subdomain.

Table 2:

#	Calling Pary (A)	Called Party (B)	Calling PAD	Calling PC Client	Called PAD	Called PC Client
1	Centrex CD Phone	Centrex phone	dialed digits	No pop up window	CNam = Pvt(A) CNum = (A)Num	N/A
2	CD - from PC Client	Centrex phone	CNam = Pvt(A) CNum = (A)Num RName = Pvt(A) RNum = (A)Num	No pop up window	CNam = Pvt(A) CNum = (A)Num RNum = (A)Num	N/A
3	Centrex CD phone	Centrex CD phone	dialed digits	CNum = (B)Num CNam= Pvt(B)	CNam = Pvt(A) CNum = (A)Num RNum = (B)Num	CNum = (A) SIP User ID CNam = Pvt(A)
4	CD - from PC Client	Centrex CD phone	CNam = Pvt(A) CNum = (A)Num RName = Pvt(A) RNum = (A)Num	CNum = (B)Num CNam = Pvt(B)	CNam = Pvt(A) CNum = (A)Num RNum = (B)Num	CNum = (A) SIP User ID CNam = Pvt(A)
5	Centrex	Centrex CD phone	dialed digits	N/A	CNam = Pvt(A) CNum = (A)Num RNum = (B)Num	CNum = (A)Num CNam = Pvt(A)
6	CD from PC Client - not in CD mode	Centrex phone	N/A	dialed digits	CNam = Pvt(A) CNum = (A)Num	N/A
7	Centrex	CD - not in CD mode	dialed digits	N/A	CNam = Pvt(A) CNum = (A)Num RNum = (B)Num	CNum = (A)Num CNam = Pvt(A)

Table 2:

#	Calling Pary (A)	Called Party (B)	Calling PAD	Calling PC Client	Called PAD	Called PC Client
8	PSTN	Centrex CD phone	dialged digits	N/A	CNam = Pub(A) CNum = (A)Num RNum = (B)Num	CNum = (A)Num CNam = Pub(A)
9	Centrex CD phone	PSTN	dialed digits	N/A	CNam = Pub(A) CNum = (A)Num	N/A
10	CD - from PC Client	PSTN	CNam = Pvt(A) CNum = (A)Num RName = Pvt(A) RNum = (A)Num	N/A	CNam = Public CNum = (A)Num RNum = (A)Num	N/A
11	CD from PC Client - not in CD mode	PSTN	N/A	dialed digits	CNam = Public CNum = (A)Num	N/A
12	Centrex CD phone	Centrex CD phone	dialed digits	CNum = (B) SIP User ID CNam = Pvt(B)	CNam = Pvt(A) CNum = (A)Num	CNum = (A) SIP User ID CNam = Pvt(A)
13	Centrex	Centrex CD phone	dialed digits	N/A	CNam = Pvt(A) CNum = (A)Num	CNum = (A)Num CNam = Pvt(A)
14	PSTN	Centrex CD phone	dialed digits	N/A	CNam = Pub(A0 CNum = (A)Num	CNum = (A)Num CNam = Pub(A)

CNam = Calling Party Name
CNum = Calling Party Number
RNam = Redirecting Party Name
RNum = Redirecting Party Number
Pvt = Private
Pub = Public

Enhancements are also made to improve displays in call forwarding scenarios involving one or more CD users, to make the displays more similar to those of phones within a Centrex group where call forwarding is involved. The most

significant improvement is that the redirecting number displayed on the terminating phone will be the OCN, as within Centrex groups. The redirecting party name is displayed when available. Due to existing AIN limitations involving the TAT trigger and subsequent call forwarding to the CD Service DN,, the redirecting party name will not be available to be the terminating party when the forwarding party (OCN) is a CD user; the redirecting party number will still be displayed..

Call forwarding on a Centrex CD user can be assigned through traditional DMS services or also through the PC Client Personal Agent routing assignments. The following table contains some call forwarding scenarios involving CD users and their expected displays.

Table 3:

#	Calling Party (A)	Forwarding Party (B)	Forwarded to (C)	Terminating Phone Display	Terminating PC Client	Forwarding PC Client
1	Centrex	Centrex	Centrex	CNam = Pvt(A) CNum = (A)Num RName = Pvt(B) RNum = (B)Num	N/A	N/A
2	Centrex	Centrex	CD Centrex	CNam = Pvt(A) CNum = (A)Num RName = Pvt(B) RNum = (B)Num	CNum = (A)Num CNam = Pvt(A)	N/A
3	Centrex	CD Centrex (PAD)	CD Centrex	CNam = Pvt(A) CNum = (A)Num RNum = (B)Num	CNum = (A)Num CNam = Pvt(A)	CNum = (A)Num CNam = Pvt(A)
4	Centrex	CD Centrex (PAD)	Centrex	CNam = Pvt(A) CNum = (A)Num RNum = (B)Num	CNum = (A)Num CNam = Pvt(A)	CNum = (A)Num CNam = Pvt(A)
5	Centrex	CD Centrex (Personal Agent)	CD Centrex	CNam = Pvt(A) CNum = (A)Num RNum = (B)Num	CNum = (A)Num CNam = Pvt(A)	No Pop Up

1.1.5 Offer Answer SDP

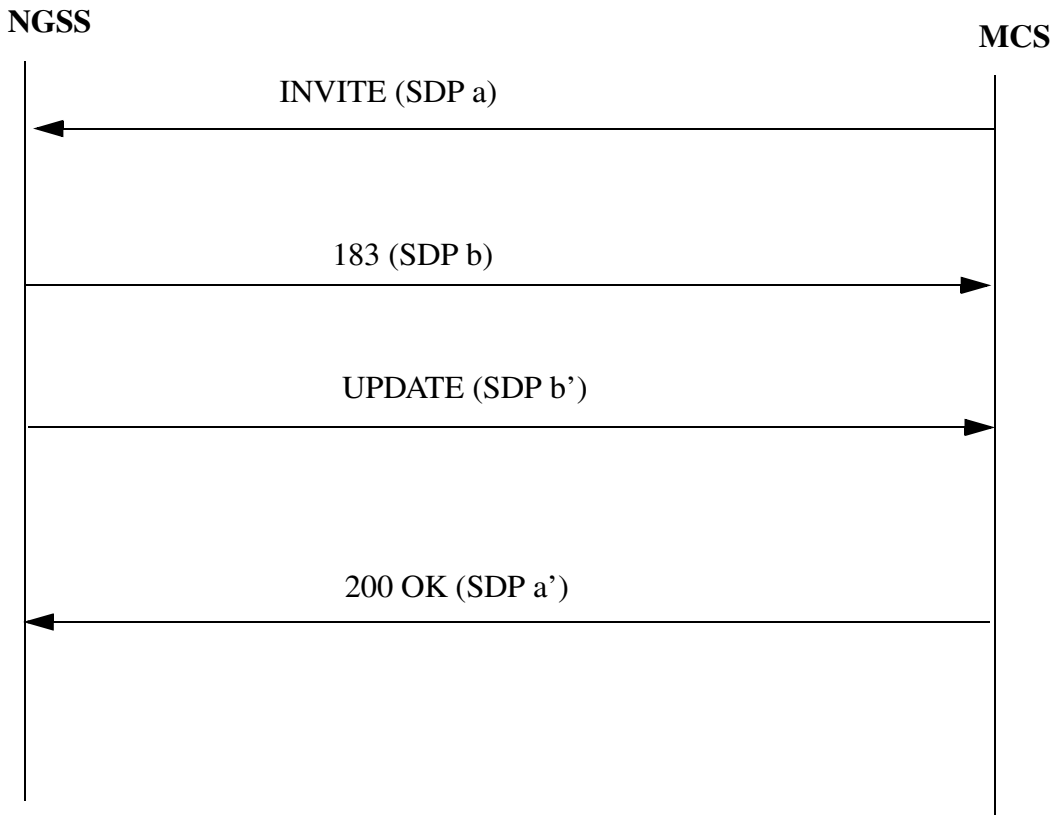
UPDATE method defined by RFC 3311 allows SIP entities to modify session attributes after initial offer answer has been exchanged. The session attributes can be modified before or after answer. Generally UPDATE is used to modify session attributes before answer as most SIP implementations use SIP re INVITE mechanism to modify session attributes after answer.

Currently NGSS sends UPDATE to modify session attributes before answer if the remote server configuration indicates that remote server supports UPDATE method. This is not the right means of deciding when to send UPDATE method. This activity improves on the design of when to send the UPDATE method as follows:

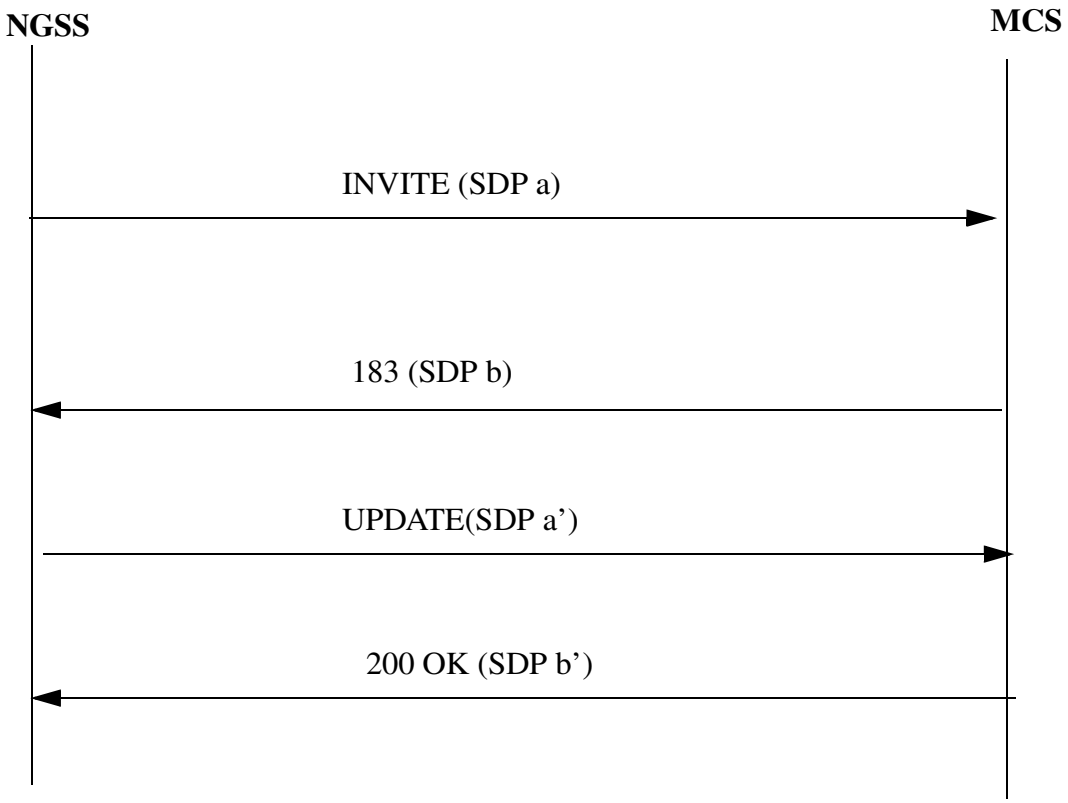
- The remote SIP node will basically indicate through means of Allow header when in a call UPDATE is allowed.
- NGSS will send UPDATE method when the remote server has indicated through messaging that UPDATE is allowed.
- NGSS will indicate that UPDATE method is allowed only after OFFER Answer SDP exchange has been completed.
- Due to backward compatibility with NGSSes prior to the SN09 release, that do not support UPDATE through messaging, UPDATE will still be supported through the GUI.

MCS uses the Allow header to indicate when UPDATE is allowed. NGSS will scan for Allow header for messages from the MCS and indicate in a call data block when UPDATE is allowed.

The call flow below indicates the interaction between the MCS and the CS2K on the usage of the UPDATE method.



a) UPDATE method accepted for processing by NGSS



b) UPDATE method sent out by the NGSS and accepted for processing by MCS

1.1.6 MCS Endpoints and Services

The following are the MCS endpoints and services that this feature will support.

1.1.6.1 MCS Endpoints

- MCS PC Client
- MCS i2002/i2004
- MCS PC Client Set
- RTP Media Portal
- AudioCodes Mediant 2000 SIP PRI Gateway
- Media Application Server
- Sipura IAD (Intergated Access Device)
- Ambit IAD (Intergated Access Device)

- Mediatrix PRI Gateway
- Rel 3.0 PC Client/Client Set

1.1.6.2 MCS Services

- Basic Call/incoming/G711
- Basic Call/outgoing/G711
- Basic Call/incoming/G729A
- Basic Call/outgoing/G729A
- Calling Number Delivery
- Calling Number Delivery Block
- Called Number Delivery
- Called Number Delivery Block
- Calling Name Delivery
- Calling Name Delivery Block
- Redirecting Name Delivery
- Redirection Name Delivery
- Original Called Number Delivery (OCdNo)
- CPL forking (Sim Ring)
- CPL Sequential Ringing
- Call Redirect
- Call Redirect Reason
- Call Reject With Reason
- Call Rejection on Unauthorized Request
- Call park against token
- Call park against user
- Call park auto retrieval
- Call retrieve against token
- Call retrieve against user
- Call Forwarding (CF)
- Call Forwarding Busy (CFB)
- Call Forwarding No Answer (CFNA)
- Call Forwarding Access Code (CFAC)
- Click to Call (C2C)

- Branding
- Hold/Retrieve (with Music On Hold)
- Hold/Retrieve (without Music On Hold)
- Ad-hoc Conferencing and Consultative Call Transfer
- Blind Call Transfer
- Meet-me Conference
- Call Park
- MCS Call Route Advancing
- Long Call Duration (MCS to CS2K)
- E911 (on CS2K)
- Message Waiting Indication (MWI)
- Call Pickup (CPU)
- Converged Desktop

1.1.7 CS2K Endpoints and Services

The following are the CS2K endpoints and services that this feature will support.

1.1.7.1 CS2K Endpoints

- IW-SPM (Interworking Spectrum Peripheral Module) with Legacy Lines
- Motorola CG4500 MTA (NCS)
- Arris TTM202/402 TTM (NCS)
- Mediatrix 1104/1124 (MGCP)
- Askey 4/12/30 port (MGCP)
- Ambit 1/16/32 port & MG1K (MGCP)
- Nuera gateway
- H.323 gateway
- CICM (Centrex IP Client Manager) gateway
- PVG (Passport Voice Gateway)

1.1.7.2 CS2K Services

- Basic Call/incoming/G711
- Basic Call/outgoing/G711
- Basic Call/incoming/G729A
- Basic Call/outgoing/G729A

- 3-Way Call (3WC)
- Message Waiting Indicator - Audible (MWT, STD sub-option only)
- Incoming MCS call to CS2K E911
- Call Forward
- Call Forward with Announcement
- (CFB) Call Forward Busy
- (CFD) Call Forward No Answer
- Call Forward of Call Waiting Calls
- (SCF) Selective Call Forward
- (CFU) Call Forwarding Universal
- Music On Hold (Call Hold)
- (CPK) Call Park
- (CPU) Call Pickup
- (CXR) Call Transfer
- (CWT) Call Waiting
- (CCW) Cancel Call Waiting
- 3 Party Conference
- Meet Me Conference
- (CNAMD) Calling Name Delivery
- (CNAB) Calling Name Delivery Blocking
- (CND) Calling Number Delivery
- (CNDB) Calling Number Delivery Blocking
- Called Number Delivery
- Called Number Delivery Block
- Redirecting Name Delivery
- Redirection Name Delivery
- Original Called Number Delivery (OCdNo)
- (MLH) Multi Line Hunt
- (NRAG) Network ring again
- (ARRDN) Automatic Recall Dialable Directory Number
- (AR) Automatic recall
- Long Duration (CS2K - MCS)

- AIN 0.1
- Delivery of Dialable Number (DDN)
- Warm Line
- CTX Automatic Dial
- IBS Last Number Redial
- IBS Call Forward D/A All Calls
- IBS Ring Again (Exec Ringback)
- IBS CTX Call Trace
- IBS Call Forward D/A Universal
- IBS Group Pick-up
- IBS Call Forward Busy Universal
- IBS Multiple Appearance Directory Number
- IBS CTX Public Name Display-Cms Set Only
- IBS Speed Call Short List
- IBS NCS Speed Call Short List
- IBS Message Waiting Line
- IBS Call Transfer with Recall
- IBS CTX Busy Lamp Field Key
- IBS Std Madn Sca Appearance
- IBS CTX Call Display 1501+ Lines ???
- IBS CTX Call Display 1-29 Lines ???
- Secondary Number on Ebs
- IBS Auto Route Sel-Per Line
- IBS CTX Call Display 501-1500 Lines ???
- NCS Call Display Over 1000 Activations ???
- IBS CTX Call Display 101-500 Lines ???
- NCS Visual M/W Ind On S/L Sets
- IBS Std Speed Call Long List
- IBS Acd Agent Incalls Key
- IBS Std Madn Mca Appearance
- NCS Call Display 1-500 Activations ???
- IBS CTX Perimeter Acd Mis Serv Bur Agent

- IBS CTX Enhance Ans Position
- IBS CTX Auto Call Back and Auto Recall
- NCS Madn 1-500 Activations ???
- CTX Ident-A-Call
- IBS Acd Queue Listed Number
- IBS CTX Network Acd (per Agent)
- CTX Distinctive Ringing Per Line Option
- Distinctive Ringing Enhanced Additional
- NCS Sp Call Long 1-500 Activations ???
- IBS CTX 1-100 Lines Visual Call Waiting
- IBS CTX Perimeter Acd Mis Serv Bur Que
- IBS UCD Listed Number 5 Yr
- IBS Custom Announcement In Co
- IBS UCD Listed Number
- Music External Source (Customer Premise)

1.2 Hardware Requirements or Dependencies

1.3 Software Requirements or Dependencies

1.4 Limitations and restrictions

SN09 CS2K Interworking with MCS 4.0 is not supported.

VRDN architecture will not be supported on SN09 CS2K.

1.5 Interactions

1.6 Glossary

Term	Description
New term	Definition

Product = CS 2000

A00009515 -- Out-of-Band interop with MCS

Functional Description

1: Applicable Solution(s)

PT-IP

1.1 Description

This activity will implement the support for Out of Band (OOB) SIP REFER signaling on the Session Server (formally known as NGSS).

REFER is a SIP method, which requests that the recipient REFER to a source provided in the request. It provides a mechanism allowing a party sending the REFER to be notified of the outcome of the referenced request. This can be used to enable many applications, including Click-to-Call.

A REFER placed outside the scope of the dialog created with an INVITE is called and an Out of Band REFER.

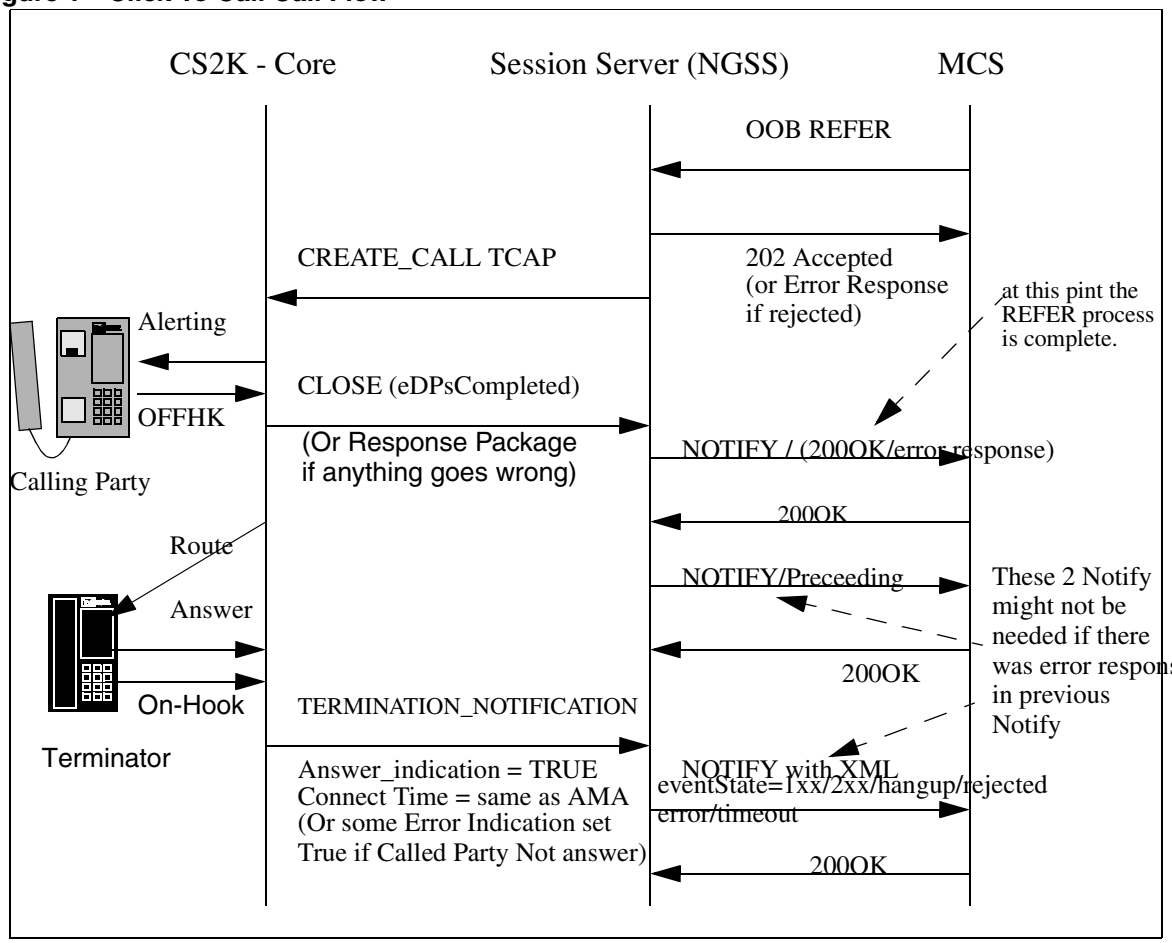
Out of Band SIP REFER support will address the following limitations with the current implementation of the MCS application Click-to-Call (C2C)

- The originator of the C2C ends up in the Termination Call MOdel (TCM) of the CS2K.
- Originating Call Manager (OCM) services and its feature interactions are bypassed (e.g. auth codes, acct codes, Denied Originations, PIC and other translation related services)
- Unnecessary TCM interactions on the originator of the C2C (like forwarding services.
- OCM updated incorrectly results in Incoming Call Memory (ICM) not being updated correctly, thus some features don’t function as designed.
- Since there are 2 distinct trunk-to-line calls with their media tied to MCS, this can cause issues around ring back and possibly tones, busy signal, even treatments not being heard by the originator. (The originator of the MCS call is already answered so the ringback request from the terminator is not propagated to the real originator).
- Billing is not captured correctly, since the call comes to the caller as an incoming terminating call rather than outgoing originating call.

1.1.1 Click-toCall flow using the new OOB REFER functionality

Following is a flow that illustrated the operation of C2C using the OOB REFER implementation as shown in Figure 1.

Figure 1 Click To Call Call Flow



1. Client invokes C2C on the MCS

2. MCS sends a OOB REFER msg to the Session Server. The REFER contains the following information which will be used in CreateCall NCAS message parameters:

- Mandatory Parameter - CallingPartyId (ReferBy): The DN of party A which is the logical originator who will be referred to Party B. CallingPartyId must be 10 digits
- Mandatory Parameter-CalledPartyId (ReferTo)
- Optional Parameter - ChargeNumber (ReferBy)

3. Session Server receives the OOB REFER request. It parses it and verifies that the REFER is NOT associated with any existing call context and thus it is an OOB REFER. Remote Server validation (provisioning data) is also performed at this point.

4. If the OOB REFER is accepted (i.e. passed the validation and authentication), the Session Server will send a 202 Response to the MCS. The Session Server responding to a REFER method will return a 400 (Bad Request) if the request contained zero or more than one Refer-To header field values.

5. NGSS then maps the REFER request to a create-call TCAP message with a Send_Notification attachment and sends it to the CS2K core via a NCAS link. For detailed description of NCAS link please see the documentation for the NA09 Activity A00007544.

The TCAP create-call is processed in the core as implemented for AIN under NA013 Activity A59011901.

6. A Create Call request is accepted by an analog user going off hook. It is rejected by the user not responding to the notification before a Create Call Timer (TCC) expires.Or if Create Call message has fatal protocol error; Create Call has invalid information in the parameters; Calling Party busy; SOC option is idle, etc., Session Server would receive some response back with cause reason. In this case, a NOTIFY message with appropriate payload content is sent to MCS OOB REFER process is over. Here is example NOTIFY with 503 service unavailable in the payload. Refer to the following table for the mapping between response of Create Call to SIP messages.

Table 1: Create Call response message to SIP response mapping

	Create-Call Response	**Mapping to SIP**
Termination_Notification	Answer_Indication	200OK
Termination_Notification	Busy_Indication: Destination Out of Order	502 Bad GAteway
Termination_Notification	Busy_Indication: User Busy	486 Busy Here
Termination_Notification	Busy_Indication: No Route to Destination	503 Service Unavailable
Termination_Notification	Busy_Indication: No Circuit Available	503 Service Unavailable
Response Package	Protocol Error: Missing Mandatory Parm	400 Bad Request
Response Package	Report Failure: CallingInterfaceBusy	486 Busy Here
Response Package	Report Failure: InappropriateUserInterface	484 Address Incomplete (if Calling Party is invalid) 503 Service Unavailable (if bearer compatibility)
Response Package	Report Failure: ResourceUnavailable	503 Service Unavailable

	Create-Call Response	Mapping to SIP
Response Package	Application Error: Missing Conditional Parm	503 Service Unavailable
Response Package	Application Error: Unexpected Communication	503 Service Unavailable
Response Package	Report Failure: RateTooHigh	503 Service Unavailable

7. When the core detects the user going off hook, it sends a CLOSE message to the Session Server with the cause value of eDPsCompleted and proceeds to route the call to the CalledPartyId.

8. Session Server decodes the CLOSE TCAP message. A NOTIFY/ 200OK msg is sent to the MCS indicating that the OOB REFER process is now complete. Subscription/context are closed at this point.

9. Once the 200OK is received by the Session Server another NOTIFY msg, this time with an XML event package, will be sent to the MCS to indicate that the call is proceeding[1]. The Call-ID in this NOTIFY msg will be the same as in all the prior messages.

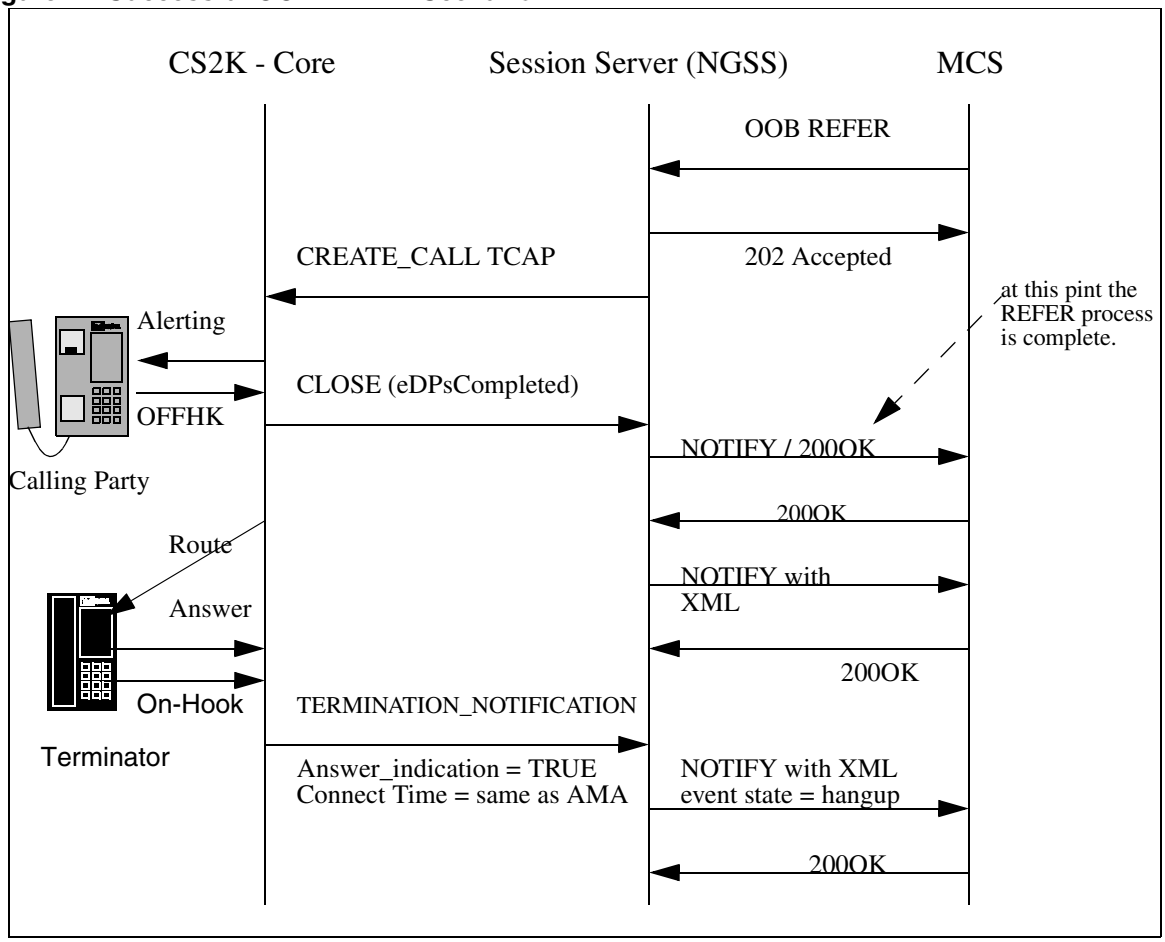
10. When the call returns to the NULL PIC, the core will send a Termination Notification msg to the Session Server with an appropriate termination indicator. If the call was answered by the Called Party the termination indicator would have Answer_Indication set to TRUE (Called Party has answered the call) and the connect time equal to the elapsed time of the call (same as the AMA record).

11. Once the Termination Notification message is received, Session Server will send the final NOTIFY to the MCS indicating that the call has been completed. In the event that the Answer_Indication is set to TRUE that notify msg will contain an events package indicating the event state of hangup.

[1] In the event that either 4XX or 5XX is received from MCS no further NOTIFY messages will be generated by NGSS and sent to the MCS. All resources pertaining to this call will be released on the NGSS

1.1.1.1 Successful OOB Refer Message Flow

Figure 2 Successful OOB REFER Scenario



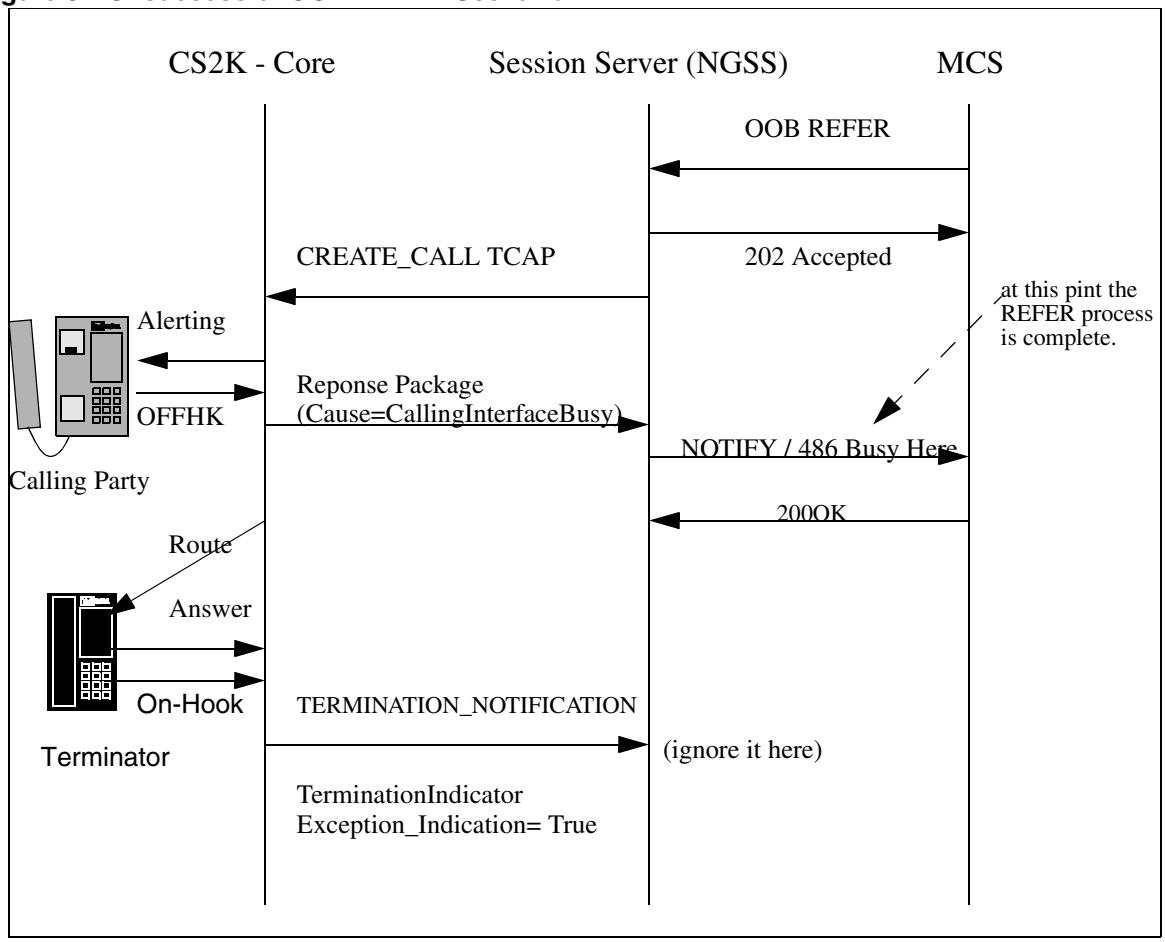

```
REFER sip:2149971908@47.104.26.49;user=phone SIP/2.0
t: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
f: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
Max-Forwards: 19
x-nt-corr-id: fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14
Allow: REFER,UPDATE
r: <sip:2149971914@cdcarrier.com;nt_service=c2c;privacy=id>
b: sip:2149971908@cdcarrier.com;
CorrelationID="fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14"
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
User-Agent: Nortel WCM 3.0.4.368
l: 0

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
From: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
```

```
CSeq: 53471 REFER
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:rega1908@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Max-Forwards: 70
Event: refer
Subscription-State: terminated;reason=noresource
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Type: message/sipfrag;version=2.0
Content-Length: 16

SIP/2.0 200 OK

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:convergeddesktop@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Max-Forwards: 70
EVENT: dialog
Content-Type: application/dialog-info+xml
Content-Length: 408

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4"
state="partial" entity="2149971914@cdcarrier.com">
     <dialog id="1" direction="initiator">
          <state event="1xx-notag">proceeding</state>
          <local-uri>sip:2149971908@cdcarrier.com;nt_service=c2c</local-uri>
          <remote-uri>sip:2149971914@cdcarrier.com</remote-uri>
     </dialog>
</dialog-info>

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:convergeddesktop@cdcarrier.com SIP/2.0
t: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
```

```
f: <sip:convergeddesktop@cdcarrier.com>
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10001 NOTIFY
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK0dce5e29aa278e1706738dc4eb313c1c
Max-Forwards: 20
EVENT: Dialog
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
l: 408
c: application/dialog-info+xml
<?xml version="1.0"?>

<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4"
state="partial" entity="2149971914@cdcarrier.com">
     <dialog id="1" direction="initiator">
          <state event="hangup">terminated</state>
          <local-uri>sip:2149971908@cdcarrier.com;nt_service=c2c</local-uri>
          <remote-uri>sip:2149971914@cdcarrier.com</remote-uri>
     </dialog>
</dialog-info>

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0
```

1.1.1.2 Calling Party User Busy Message Flow

Figure 3 Unsuccessful OOB REFER Scenario

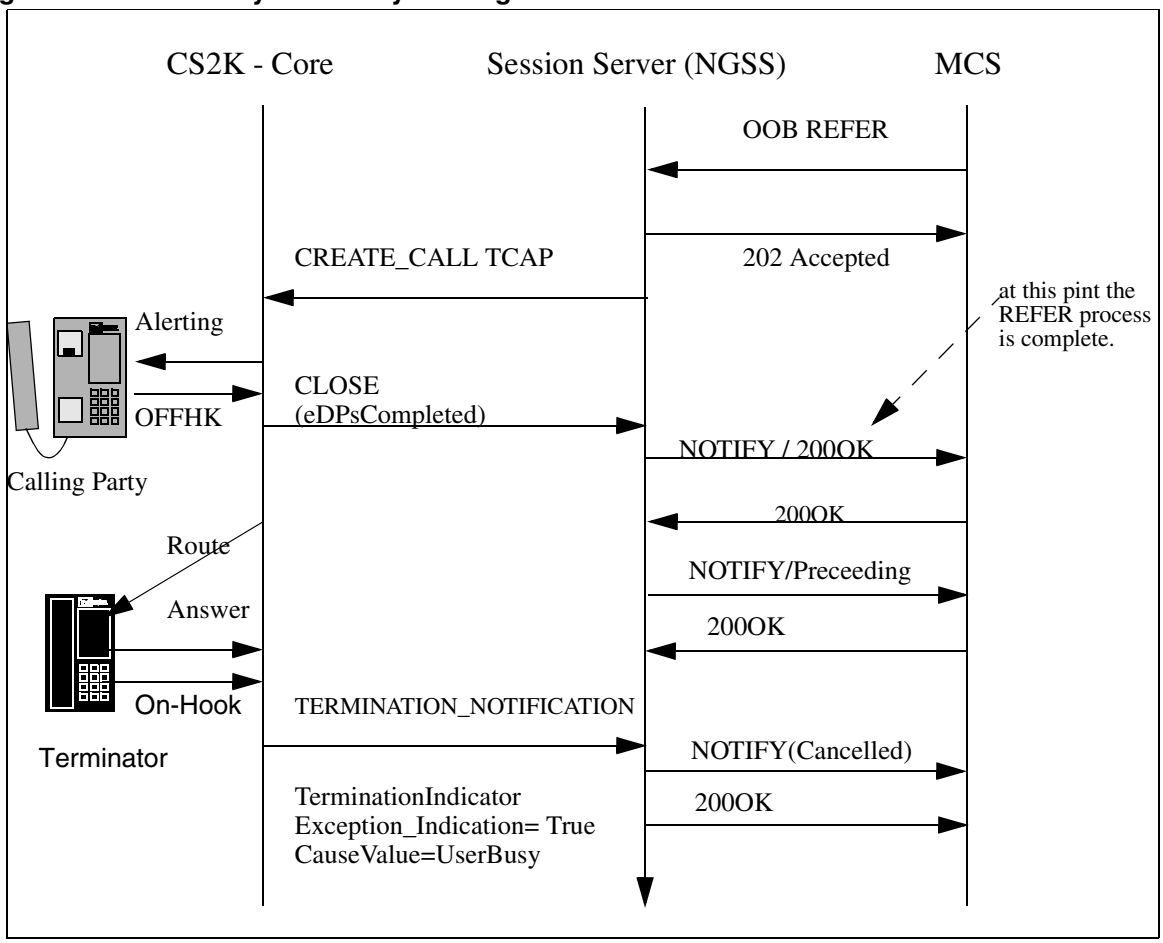



```
REFER sip:2149971908@47.104.26.49;user=phone SIP/2.0
t: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
f: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
Max-Forwards: 19
x-nt-corr-id: fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14
Allow: REFER,UPDATE
r: <sip:2149971914@cdcarrier.com;nt_service=c2c;privacy=id>
b: sip:2149971908@cdcarrier.com;
CorrelationID="fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14"
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
User-Agent: Nortel WCM 3.0.4.368
l: 0

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
From: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
```

```
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:rega1908@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Max-Forwards: 70
Event: refer
Subscription-State: terminated;reason=noresource
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Type: message/sipfrag;version=2.0
Content-Length: 16

SIP/2.0 486 Busy Here



SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0
```

1.1.1.3 Called Party User Busy Message Flow

Figure 4 Called Party User Busy Message Flow



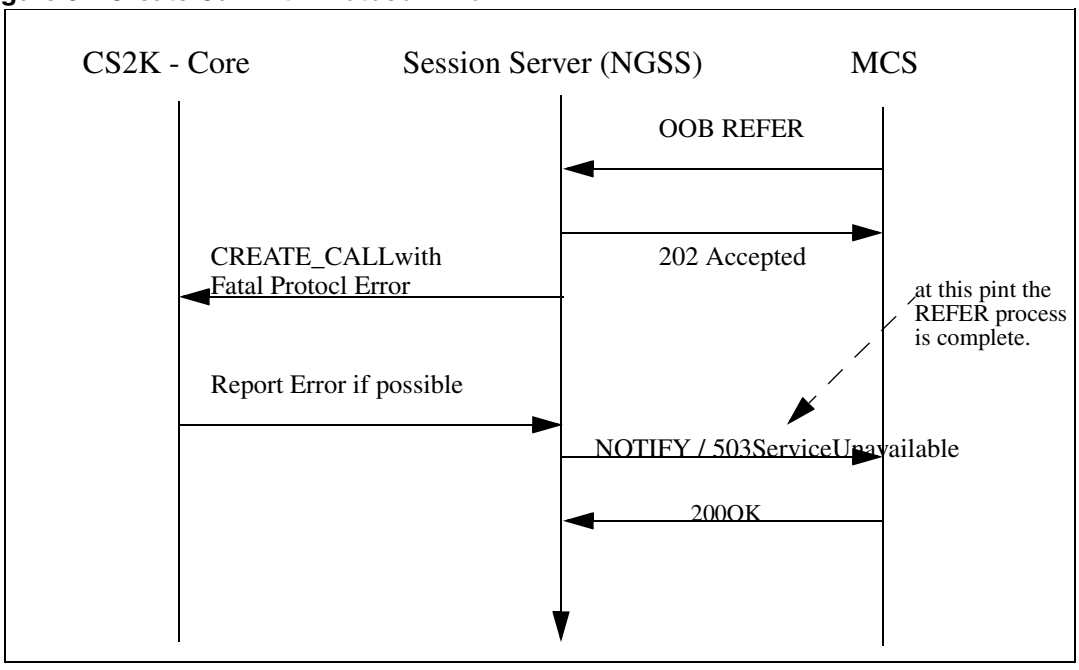

```
REFER sip:2149971908@47.104.26.49;user=phone SIP/2.0
t: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
f: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
Max-Forwards: 19
x-nt-corr-id: fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14
Allow: REFER,UPDATE
r: <sip:2149971914@cdcarrier.com;nt_service=c2c;privacy=id>
b: sip:2149971908@cdcarrier.com;
CorrelationID="fd2f534f3c96dab16e70a70d1a2210b69f9f3@47.104.26.14"
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
User-Agent: Nortel WCM 3.0.4.368
l: 0

SIP/2.0 202 Accepted
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
From: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
```

```
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 53471 REFER
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:rega1908@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Max-Forwards: 70
Event: refer
Subscription-State: terminated;reason=noresource
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Type: message/sipfrag;version=2.0
Content-Length: 16

SIP/2.0 200 OK

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: "rega1908" <sip:rega1908@cdcarrier.com;nt_service=c2c>;tag=804421795
From: "rega1908" <sip:rega1908@cdcarrier.com>;tag=1c20108
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 9999 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:convergeddesktop@cdcarrier.com SIP/2.0
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Max-Forwards: 70
EVENT: dialog
Content-Type: application/dialog-info+xml
Content-Length: 408

<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4"
state="partial" entity="2149971914@cdcarrier.com">
     <dialog id="1" direction="initiator">
          <state event="1xx-notag">proceeding</state>
          <local-uri>sip:2149971908@cdcarrier.com;nt_service=c2c</local-uri>
          <remote-uri>sip:2149971914@cdcarrier.com</remote-uri>
     </dialog>
</dialog-info>

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0

NOTIFY sip:convergeddesktop@cdcarrier.com SIP/2.0
```

```
t: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
f: <sip:convergeddesktop@cdcarrier.com>
i: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10001 NOTIFY
v: SIP/2.0/UDP 47.104.26.14:5060;branch=z9hG4bK0dce5e29aa278e1706738dc4eb313c1c
Max-Forwards: 20
EVENT: Dialog
k: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
l: 408
c: application/dialog-info+xml
<?xml version="1.0"?>

<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info" version="4"
state="partial" entity="2149971914@cdcarrier.com">
     <dialog id="1" direction="initiator">
          <state event="Rejected">terminated</state>
          <local-uri>sip:2149971908@cdcarrier.com;nt_service=c2c</local-uri>
          <remote-uri>sip:2149971914@cdcarrier.com</remote-uri>
     </dialog>
</dialog-info>

SIP/2.0 200 OK
Via: SIP/2.0/UDP
47.104.26.14:5060;branch=z9hG4bK5d4937f6ca3ddbcfc37faa8c48b1a775
To: <sip:2149971908@cdcarrier.com;nt_service=c2c>;tag=1330045952
From: <sip:convergeddesktop@cdcarrier.com>
Call-ID: fd2f534f42b869a516e70a360d8ca5e1e6e177@47.104.26.14
CSeq: 10000 NOTIFY
Contact: com.nortelnetworks.firewall,p-3rdpartycontrol,nosec
Content-Length: 0
```

1.1.1.4 Create Call with Protocol Error

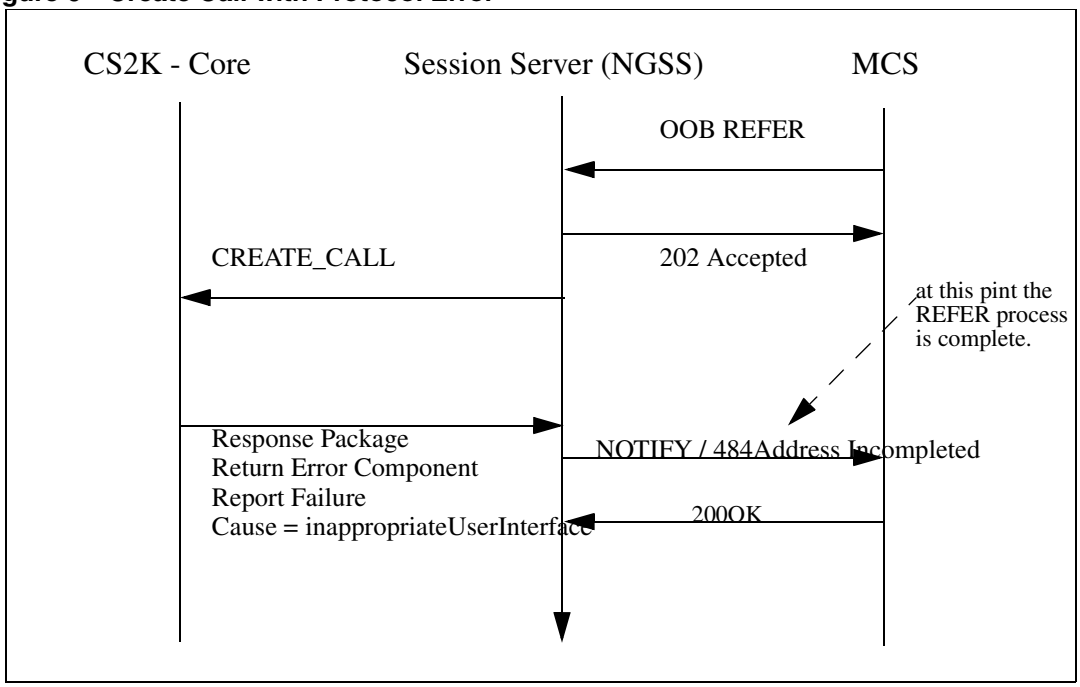
Figure 5 Create Call with Protocol Error



If a Create Call message contains a Protocol error, then it will be reported to the SCP if appropiate. NGSS will send final Notification to MCS with 503 Service Unavailable.

1.1.1.5 Create Call with Invalid Calling Party ID

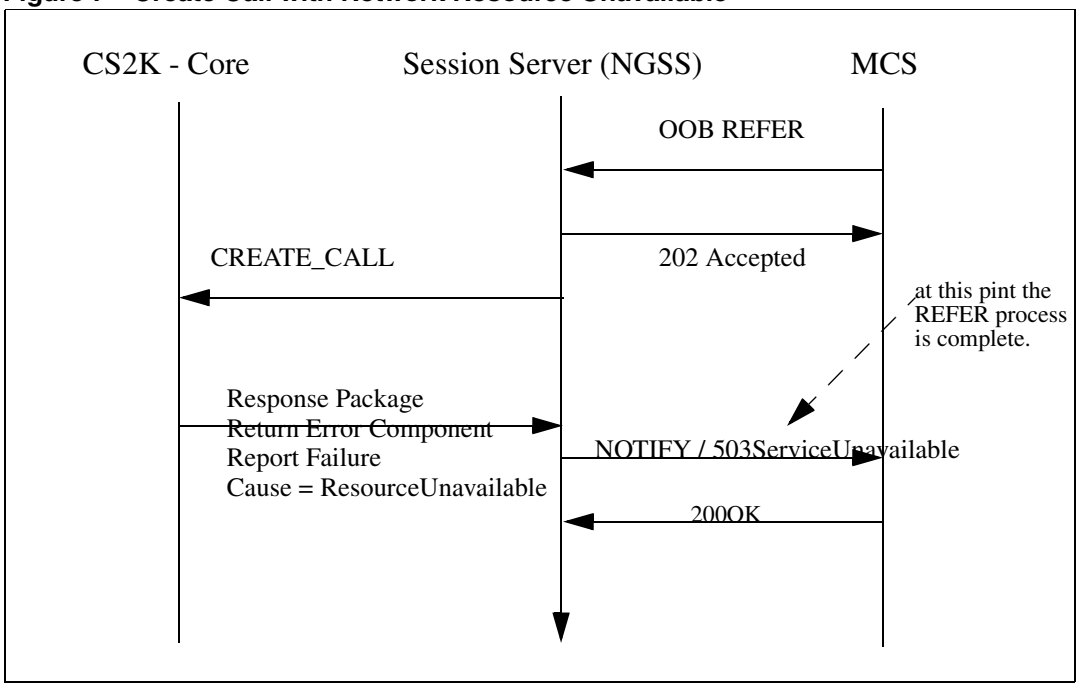
Figure 6 Create Call with Protocol Error



If a Create Call message contains a Protocol error, then it will be reported to the SCP if appropiate. NGSS will send final Notification to MCS with 484 Address Incompleted if it is Calling Party Invalid, or Notify with 503 Service Unavailable if it is invalid Bearer capability.

1.1.1.6 Create Call with Network Resource Unavailable

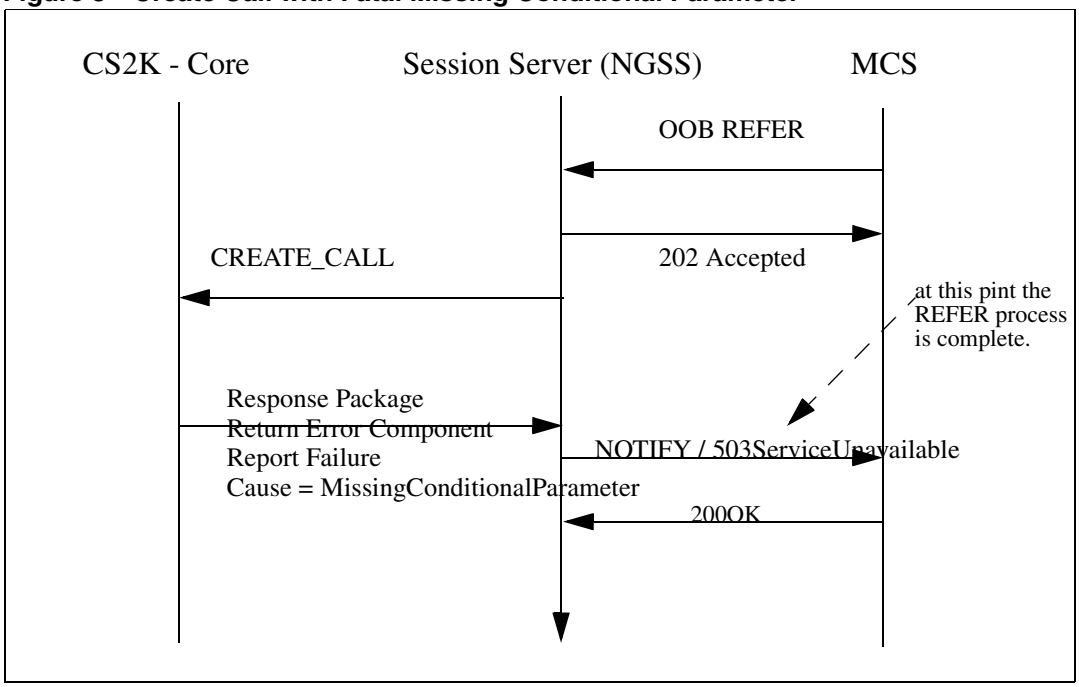
Figure 7 Create Call with Network Resource Unavailable



If Response Package returns failure as Resource Unavailable, NGSS would send final Notify message with 503 Service Unavailable to MCS.

1.1.1.7 Create Call with Fatal Missing Conditional Parameter

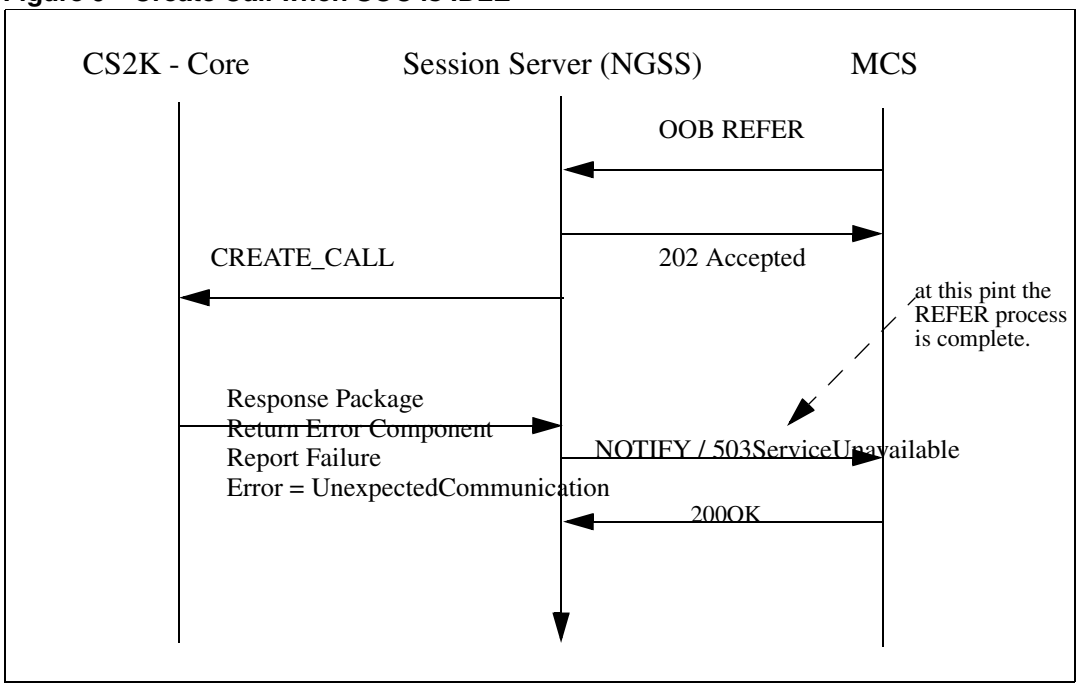
Figure 8 Create Call with Fatal Missing Conditional Parameter



If a Create Call message is determined to be missing an Optional parameter which is required then it is reported to the NGSS as a fatal Application Error with error as MissingConditionalParameter. NGSS then would send final Notify message with 503 Service Unavailable to MCS.

1.1.1.8 Create Call when SOC AIN00271 is IDLE

Figure 9 Create Call when SOC is IDLE



If a Create Call message is received when the SOC Option AIN00271 is IDLE then an Application Error with Error Cause set to Unexpected Communication is sent to NGSS. NGSS then would send final Notify message with 503 Service Unavailable to MCS.

1.2 Hardware Requirements or Dependencies

This feature doesn't introduce any new hardware requirements or dependencies

1.3 Software Requirements or Dependencies

Create Call must be enabled by SOC code AIN00271.

1.4 Limitations and restrictions

Following are the restrictions and limitations that apply to this feature;

- SIP Lines are not supported.
- NGSS standalone configuration, where the NGSS functions as converter from OOB REFER and TCP and the core is not running succession software and thus is not supported.
- List of agents not supported by this feature can be found in section 2.6.6 "Agent Support for Create Call"
- OFF Hook Delay Trigger (part of Info_Collected TDP) is not supported. See section 2.6.5. Interaction with AIN Triggers.

- TCAP messages from the CS2K to the Session Server can be lost during various maintenance actions (restarts, swacts.) which in turn could cause the Call Log on the MCS not to be updated correctly.
- International Calls are not supportedby this activity due to a limitation in the number of CDN digits that can be sent to the core.

1.5 Interactions/Interworking

1.5.1 Feature Interactions with the Originator (CallingParty)

1.5.1.1 Originating Restriction Features

When the originator has one of the following call originating restrictions, the **Create Call request is rejected** by sending the NGSS a Failure message with failureCause=inappropriateCallingInterface:

DOR (denied Origination)

SUS/RSUS (suspended/requested suspension)

In addition to the above originating restriction features, the following originators also result in failing the Create Call request (a Failure message with failureCause=inappropriateCallingInterface is sent to the SCP):

Hotline Features AUL (automatic line), and MAN (Manual Line)

A line with the ESL (Emergency Service Line) option

one of the following MADN groups:

MADN SCA (Single Call Arrangement)

MADN MCA (Multiple Call Arrangement)

MADN EXB (Extension Bridge)

MADN CACH

ACD

UCD

MeetMe Conference

Non Resident DN

A line with BC (Bearer Capability) option with values other than SPEECH or 3_1KHZ.

When the originator has one of these features active, it is considered interface busy thus no alerting is provided to the originator:

all variants of Call Waiting, including TCW (Talking Call Waiting)

all variants of Hold

1.5.1.2 Terminating Features on the Originator

When alerting the originator, terminating features **are not activated** since the alerting is a treatment that applied to the originator indicating the Create Call request, not a call that is terminating on the originator. These terminating features include:

- All variants of Call Forwarding
- SCMP (Series CoMPletion)
- Termination Restrictions like DIN (Denied Incoming), DTM (Denied Terminating), DND (Do Not Disturb), MBK (Make Busy Key), MSB (Make Set Busy), MSBI (Make Set Busy Intragroup), PLP (PLug uP), SUS/RSUS (suspended/requested suspension) and RMB (Random Make Busy).
- EBCR (Enhance Busy Call Return)
- Intercept Feature like FLEXI (Flexible Intercept)
- Messaging Features like CSMI (Call Screening/Monitoring Intercept), EMW (Executive Message Waiting), FTS (FAX-Thru Service), ISA (In-Session Activation), SCM (Selective Call Messaging), SDS (Special Delivery Service), SODS (Special Offering Decoupling of SDS), MWT (station Message WaiTing) and UVM (universal Voice Messaging).
- Call Message Feature for RES
- Call Pickup
- Hunting Features (a member of a hunt group as the originator is alerted for the Create Call request if not busy, however, if it is busy, no hunting is done and the case is handled as the originator being busy.)
- Hunt Group Overflow Routing like LOD (Line Overflow to DN) and LOR (Line Overflow to Route)
- DLCM (Dual Line Call Management)
- SimRing (Res Simultaneous Ringing)
- ACRJ (Anonymous Caller ReJection)
- SCA (Selective Call Acceptance)
- SCRJ (Selective Call ReJection)
- SCF (Selective Call Forwarding)

1.5.1.3 Account Codes

Attempt to activate Account Codes (First or Last flavours) features prior to Called Party answers are denied. That is, if a Create Call is requested to originate from a line that requires Account Code, the Account Code is bypassed and the call is routed to the Called Party without the input of the Account Code.

The Account Code Voluntary feature shall be permitted to activate after flashing during an active call established through the Create Call functionality.

Note: Warning! It is assumed that the SCP/Adjunct is a "Trusted Node" and has authenticated the user request for Create Call functionality. The SCP/Adjunct provides Account Code data collection capabilities if the Service Provider deems them necessary.

1.5.1.4 Authorization Codes

Attempt to activate Authorization Codes (First or Last flavours) features prior to Called Party answers are denied. That is, if a
Create Call is requested to originate from a line that requires Authorization Code, the Authorization Code is bypassed and the call is routed to the Called Party without the input of the Authorization Code.

The Authorization Code Voluntary feature shall be permitted to activate after flashing during an active call established through the Create Call functionality.

Note: Warning! It is assumed that the SCP/Adjunct is a "Trusted Node" and has authenticated the user request for Create Call functionality. The SCP/Adjunct provides Account Code data collection capabilities if the Service Provider deems them necessary.

1.5.1.5 Authorization Code Immediate Dialing (ACID)

The ACID feature removes the seven second pause between the input of authorization codes and second dial tone. When an IBN subscriber dials a correct authorization code, including the correct security digits, the ACID feature assumes that no more authorization code digits are to be dialed. It then proceeds immediately to the next stage of call processing without waiting for an octothorpe (#) or interdigit time-out.

The interactions with this feature is the same as Create Call interactions with Authorization Codes.

1.5.1.6 Station Specific Authorization Codes (SSAC)

SSAC has the same interactions as authorization codes.

1.5.1.7 CRL (Code Restrictions)

Any DN that is blocked for the customer group through CRL is not blocked when a call is routed to that DN by the Create Call functionality.

1.5.1.8 SOR (Station Origination Restrictions)

The SOR feature determines whether the call should be restricted. SOR restrictions fall into one of the following four categories:

— calls permitted based on NCOS

— only intragroup calls or calls on an exception list are allowed

— only intragroup calls are allowed

— only calls on the exception list are allowed

— no calls are allowed

1.5.1.9 Toll Restriction Features

At the alerting originator phase, the originator is not checked against Toll Restrictions, that is, even if the originator has Toll Restrictions, the SSP will still alert the originator. When the originator accepts the call, the SSP then attempts to route the call to the called party -- this is when the Toll Restrictions are checked and applied to the call.

Toll Restrictions include:

- CTD (carrier toll denial)
- Equal Access Enhanced Carrier Toll Denial
- FCTDNTER (InterLATA Full Carrier Toll Denial)
- TDN (Toll Denial)
- TDV (Toll Diversion)

1.5.1.10 Features Treated as Interface Busy

When the originator has one of these features active, it is considered interface busy thus no alerting is provided to the originator:

- all variants of Call Waiting, including TCW (Talking Call Waiting)
- all variants of Hold

1.5.1.11 Call Waiting During Alerting Originator

When a call is terminating on an interface which is being notified as an originator of a previously received Create Call message, the SSP shall treat the call as terminating party busy. All call waiting features including SCWID (Spontaneous Call Waiting Identification, DSCWID (SCWID with Disposition) are not activated.

1.5.1.12 No Barge-in on Create Call

The SSP do not Barge-in on a call while attempting to service a Create Call request. In other words, when the originator is being alerted for a Create Call request, Barge-In features like executive busy override (EBO) and directed call pickup with barge in (DCBI) cannot be activated.

1.5.1.13 Feature Activation after Originator Accepts Create Call

Once the originator accepts the Create Call request by going offhook, the originator is able to activate any features that can be activated through normal call setup.

1.5.1.14 Distinctive Ringing Features

When optional parameter ControllingLegTreatment is included in the Create Call message, the value specified in this parameter overrides the switch based Distinctive Ringing features.

1.5.1.15 Feature Activation after the Calling Party accepts Create Call

Once the originator accepts the Create Call request by going offhook, the originator is able to activate any features that can be activated through normal call setup.

1.5.2 Feature Interaction during routing to Called Party

1.5.2.1 Terminating Features

Terminating features on the Called Party are activated and function the same way as the call has been initiated by the originator through going offhook and dialing the digits.

1.5.2.2 Calling Number/Name Display/Blocking

The presentation status in the Calling Party ID in the Create Call message overrides calling number/name display/blocking features.

1.5.2.3 Distinctive Ringing Features

When optional parameter PassiveLegTreatment is included in the Create Call message, the value specified in this parameter overrides the switch based Distinctive Ringing features.

1.5.2.4 UCD (Uniform Call Distribution) Call Queuing

If the Called Party ID maps to a station in a UCD group, the call created through the Create Call functionality is terminated to that station.

1.5.2.5 Direct Inward System Access (DISA)

when the Called Party ID maps to a DISA DN, it behaves the same way as if the user had dialed the DN.

1.5.2.6 Preset Conference

A call can be routed to a Preset conference DN through a Create Call request.

1.5.2.7 MeetMe Conference

A call can be routed to a MeetMe conference DN through a Create Call request.

1.5.2.8 Expensive Route Warning Tone

When routing to the Called Party, the Expensive Route Warning Tone is not heard.

1.5.2.9 Flash

When routing to the Called Party, before the call terminates on the Called Party, flash is not allowed. Flash after terminating on the Called Party is allowed.

1.5.2.10 Flexible Calling (FC)

When routing to the Called Party, before the call terminates on the Called Party, FC is not allowed. FC after terminating on the Called Party is allowed.

1.5.2.11 PVN (Private Virtual Network)

While routing to the Called Party, attempting to start the PVN feature results in FNAL treatment to be applied to the call.

1.5.2.12 MCDN (Message Center Directory Number)

While routing to the Called Party, attempting to start the MCDN feature results in FNAL treatment to be applied to the call.

1.5.2.13 E800

If the Called Party ID in the Create Call message is an E800 number, the SSP shall activate the E800 service and query the E800 database.

1.5.2.14 AIN TFS

If the Called Party ID in the Create Call message is an AIN TFS number, the SSP shall query the SCP.

1.5.2.15 Emergency 911

If the Called Party ID in the Create Call message contains digits ‘911’, which correspond to the emergency service, the SSP shall route the call using the E911 service.

1.5.3 Interactions with AIN Triggers

- **When Alerting the Calling Party** - When alerting the originator for a Create Call request, all AIN triggers encountered (e.g., terminating triggers like TAT, T_No_Answer and T_Called_Party_Busy triggers) are ignored and queries to the SCP are not sent.
- **Calling Party goes OFFHK** - When the originator accepts the Create Call request by going offhook, any AIN triggers encountered at the Orig_Attempt TDP and Info_Collected TDP are ignored and queries to the

SCP are not sent. **Off Hook Delay Trigger** is part of the Info_Collected TDP and thus will be IGNORED.

- **Routing to Destination** - After the originator accepts the call, the CS2K attempts to route the call to the called party of the Create Call message. During the routing phase, any triggers that may occur result in queries to be sent to the SCP.

1.5.4 Agent Support for Create Call

The Calling Number in a Create Call message must be a local line agent. This is by definition of the Create Call Message. Only agents supported by AIN may be the Calling Number. The following additional restrictions are placed upon which line agents are supported as Create Call Originators:

- ISDN PRI agents are not supported (PRI is considered to be a trunk)
- ISDN BRI agents are not supported
- Coin lines are not supported
- Attendant Consoles are not supported
- Virtual Agents are not supported.
- ADSI terminals are supported as an analog agent
- Party lines are not supported.
- Hunt group members are supported, but no hunting is done.

1.5.4.1 TOD (Time Of Day routing)

The route taken by Create Call can be affected by Time of Day(TOD) Routing.

1.5.4.2 Simplified Message Desk Interface (SMDI)

The Called Party in the Create Call message can be a line served by SMDI.

1.5.4.3 Series Completion (SCMP)

A call created through the Create Call functionality can terminate to an SCMP group and does not affect the SCMP terminating algorithm.

1.5.4.4 Hunt Groups

If the Called Party ID in the Create Call message corresponds to one of the following Hunt Groups, then the call is terminated on first available member of the Hunt Group:

- BNN (Bridged Night Number)
- DLH (Distributed Line Hunt)
- DNH (Directory Number Hunt)
- KSH (Key-Set Short Hunt Group)
- MLH (Multiline Hunt)

- MPH (Multiple Position Hunt)
- NSDN (Night Service Directory Number)

1.5.4.5 Feature Groups

A call established through the Create Call functionality can route either as FGB, FGC or FGD.

A call established through the Create Call functionality can not be routed as FGA.

1.5.4.6 MADN (Multiple Appearance Directory Nymber)

When the Called Party ID included in the Create Call message maps to one of the following MADN group, the call terminates on the MADN group:

- MADN SCA (Single Call Arrangement)
- MADN MCA (Multiple Call Arrangement)
- MADN EXB (Extension Bridge)
- MADN CACH

1.5.4.7 SimRing

When CalledPartyID parameter in the Create Call message is a pilot DN, then SIMRING is activated and the Call proceeds normally.

1.5.4.8 PLP (PLug uP)

When the Called Party has the PLP feature activated, a call created through the Create Call functionality is not allowed to terminate on the Called Party.

1.5.4.9 SUS/RSUS (suspended/requested suspension)

When the Called Party has the SUS/RSUS feature activated, a call created through the Create Call functionality is not allowed to terminate on the Called Party.

1.5.4.10 RSDT (restricted dial tone) with state in-effect

When the Called Party has the RSDT feature activated, a call created through the Create Call functionality is not allowed to terminate on the Called Party.

1.5.4.11 CLASS Outgoing Call Memory

When a call is originated via the Create Call request, the SSP does not update the outgoing Memory Slot (OMS), regardless whether or not the call is diverted through triggering while routing to the Called Party.

1.5.4.12 LNR (Last Number Redial)

Attempt to invoke LNR on a call established through the Create Call functionality shall result in calling the number the originator dialed before the Create Call request.

1.5.4.13 AR (Automatic Recall)

Attempt to invoke AR on a call established through the Create Call functionality shall result in calling the number the originator dialed before the Create Call request.

1.5.4.14 ACB (Automatic Call Back)

When an attempt to establish a call through a Create Call request fails due to the Called Party's interface busy status, invoking ACB from the originator of the Create Call message shall result in calling the number the originator dialed before the Create Call request.

1.5.4.15 Ring Again Features

- **Call Back Queuing (CBQ)**: CBQ cannot be invoked when the call encounters a busy facility while routing the Called Party of a Create Call message.

  Note: CBQ (also known as on-hook queuing) provides a ring back to the on-hook calling line when a facility that the call is queued against becomes available. CBQ can be activated by the caller after receiving no circuit treatment, expensive route warning tone, or during the off-hook queue tone or announcement.

- **Nodal ring again (RAG)**: Attempt to invoke RAG on a call established through the Create Call functionality shall result in calling the number the originator dialed before the Create Call request.

- **Network ring again (NRAG)**: NRAG is applicable when the ring again feature is networked across different switching nodes. From a user point of view, NRAG and RAG operate the same way for Create Call.

1.5.4.16 Dynamic Control Routing (DCR)

Dynamic Control Routing may encounter while routing to the Called Party.

1.5.4.17 ACD (Automatic call distribution) Termination

Automatic call distribution (ACD) permits calls to be evenly distributed to a number of designated ACD agent positions. When all positions are busy, new calls are queued and a ringing tone or announcement can be returned to the caller.

A call can be routed to an ACD DN through the Create Call request and ACD functionality is not impacted.

Parameter Calling Party Id in the Create Call message is not used to update the display of EBS sets with the ACD option.

1.5.4.18 SMDR (Station Message Detail Recording)

All calls that would normally generate SMDR records will continue to do so when the call is created through the Create Call functionality.

1.6 Glossary

Term	Description
AIN	Advanced Intelligent Network
DN	Directory Number
SOC	Software Optionality Control
TCC	Create Call Timer
TID	Terminal ID
CPID‘	Call Processing ID
GAME	Generic AIN Messaging Environment
TCAP	Transaction Capabilities Application Part
SS	Session Server (AKA NGSS)
SIP	Session Initiated Protocol
NCAS	Non-Call-Associated-Signaling
C2C	Click to Call
C2D	Click to Dial
SCP	Service Control Point or Signaling Control Protocol
SSP	Service Switching Point

2: Fault Management for A00009515

2.1 Logs

New NCAS class log will be generated by the SIP Gateway Application under this activity. It will be generated for the following event: OOB Refer is Rejected.

This log can be viewed via the SIP Gateway Maintenance web browser interface on the Session Server Manger - SIP Gateway application web page.

No alarms will be generated in connection with this.

2.1.1 NCAS LOGS

New customer log that will be generated by this feature:

- NCAS501 - OOB REFER REJECTED

2.1.1.1 NCAS501 OOB REFER Rejected

Log NCAS501 “OOB REFERREJECTED” is generated when an Out-of-Band REFER Request that has been received by the Session Server does not validate and this the request can not be accepted.

Log Title: OOB

Name: NCAS 501

Description: OOB REFER REJECTED

Event Type: Trouble

FORMAT: For the NCAS 501 log, the following are values/explanations of the variable values:

- alarmLevel = NONE
- componentID = NCAS
- category = Communications
- description = OOB Refer Rejected
- probable cause = Incorrect Header
- specific cause = ReferTo or ReferBy Header Incorrect
- correlationIdList = None
- neVendorSpecificInfo = None
- technologySpecificInfo = None
- reportName = NCAS
- reportNum= 501
- eventType = TBL
- label = OOB

ACTION: Verify Header Population

Product = CS 2000

A00009520 -- Trunk blocking tools for MG4K and GWC on SN09

Functional Description

1: Applicable Solution(s)

PT-AAL1, UA-IP

1.1 Description

When a MG4K-ATM or GWC goes into overload, some trunks on that node need to be busied to offload traffic. In the current system, it provides the capability to busy whole trunk group or all members on a specific MG4K-ATM/GWC node. However, there is no way to busy specific trunks on an individual MG4K-ATM/GWC.

This feature enhances the existing post command under MAPCI TTP level to provide the following functions:

- Busy a specific trunk group on an individual MG4K-ATM gateway;
- Busy a specific trunk group on an individual GWC.

A new post type ‘I’ is introduced under MAPCI TTP level by this feature. When post command with type ‘I’ is entered in the command, it posts the trunks in the existing post set. If there is no existing post set, it returns error. The following is the error example:

The following is an example on how to post the trunk members of TRUNK_EXAMPLE on GWC 32.

```
                IOD          PM    CCS    Lns    Trks   Ext    APPL
                OCC  B       PMLOAD  3   RS  SYSB    42C..  2Crit   .
                *C*             *C*    *C*    *C*    *C*    *C*
TTP
 0 QUIT         POST      DELQ         BSYQ       DIG
 2 Post_        TTP 27-0102
 3 SEIZE        CKT TYPE    PM NO.       COM LANG    STA S R  DOT TE  RESULT
 4
 5 BSY
 6 RTS
 7 TST
 8
 9 CktInfo
10 CktLoc
11 Hold          NO CKT, SET IS EMPTY
12 NEXT          TTP:
13 RLS
14 Ckt_
15 TrnslVf_
16 StkSdr_
17 Pads
18 Level_
  TESTER
Time  15:32  > POST D GWC 32; POST I G TRUNK_EXAMPLE
```

1. *POST D GWC 32; // create a post set which contains all the trunks on GWC32;*
2. *POST I G TRUNK_EXAMPLE; // Post only the trunks whose CLLI are TRUNK_EXAMPLE in the post set.*

Only post type ‘D’ and ‘G’ are allowed to follow the type ‘I’. Only DEQ name ‘GWC’ and ‘SPM’ are allowed to follow the post type ‘D’ if it is after the type ‘I’. This feature is based on the existing BSY functions for trunks on GWC and SPM.

The trunks that supported by this feature are ISUP, PTS and PRI on GWC and MG4K-ATM.

1.2 Hardware Requirements or Dependencies

N/A

1.3 Software Requirements or Dependencies

N/A

1.4 Limitations and restrictions

- Only trunks on GWC and MG4K-ATM are supported by this feature.

1.5 Interactions

- A set of trunks must be posted prior to to ‘POST I’ command.

1.6 Glossary

Term	Description
CLLI	Common Language Location Identifier
DEQ	Digital EQuipment
TTP	Trunk Test Position
PTS	Per Trunk Signalling
PRI	Primary Rate Interface
ISUP	ISDN User Part
MG4K	SMG4000
ATM	Asynchronous Transfer Mode
GWC	Gateway Controller

Product = CS 2000

A00009530 -- H248 and xUA NAT traversal for CPE Gateways

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

1.1.1 Introduction

Small trunk gateways, such as the Audiocodes Mediant 2000 (M2k), are being deployed as Customer Premises Equipment (CPE). This is being done in order to connect TDM PBXs to packet telephony networks, as we expect that there will be many such older TDM PBXs in service for a number of years to come.

Various protocols are used to control these gateways. Within the scope of this feature, H.248 is used for control of the bearer path. Call control signalling can be via protocols such as ISDN PRI, or DPNSS. These signalling protocols are backhauled from the gateway to the CS2k over an SCTP connection. Currently, neither the H.248, nor the SCTP protocol can work over a NAT

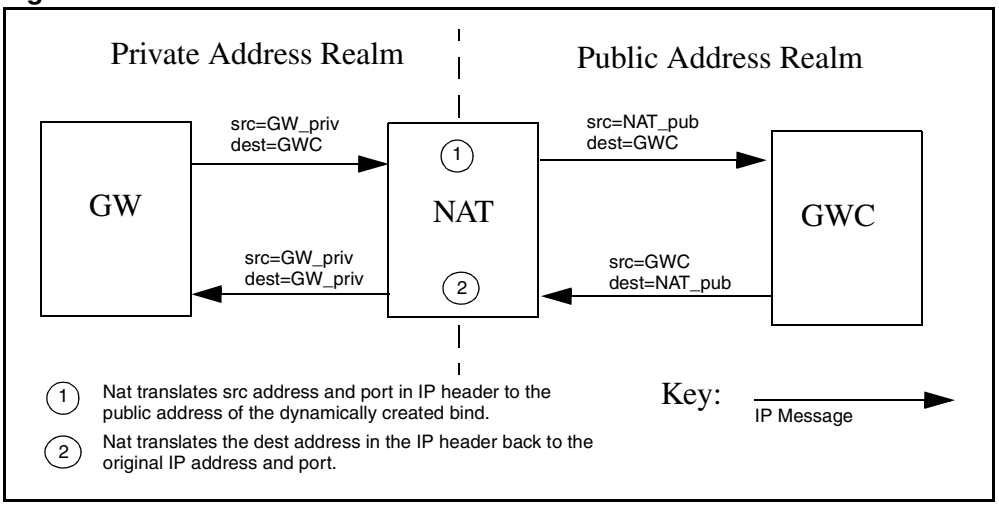
without special datafill in place. This feature will enable these protocols to work automatically when the gateway is located behind a NAT. Note that the CS2k and GWCs must remain within the core network.

1.1.2 Operation

NAT systems are in common use throughout IP networks today. They allow use of private addresses within a network by translation of IP addresses within the IP header. CPE gateways may well be connected via a NAT, so this needs to be a supported configuration for the CS2k.

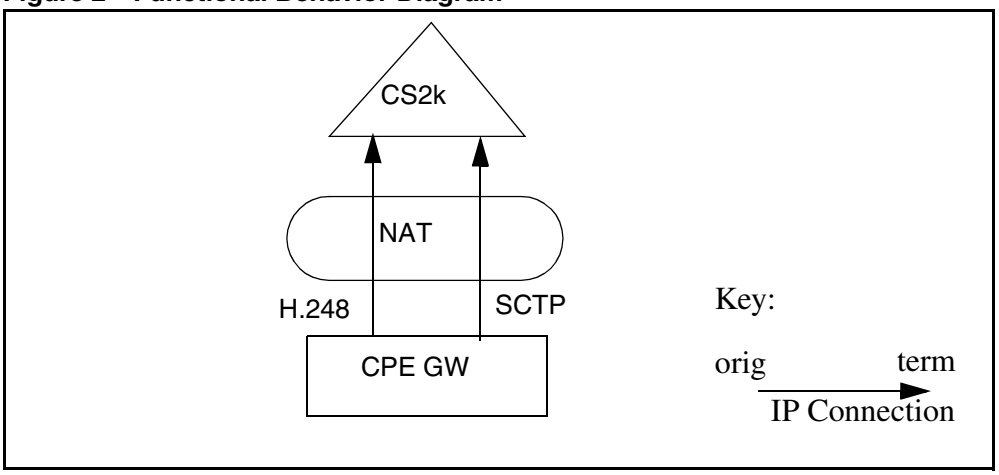
Figure 1 illustrates a simple case of NAT operation. The NAT creates a dynamic bind in response to the initial message from the gateway. This allows messages to pass in both directions between gateway and GWC. The NAT bind will be removed if there is no traffic over it for a specified period of time. In order to avoid this happening to an established connection, we need to ensure a minimum traffic level over the link. SCTP has an inbuilt heartbeat mechanism which will perform this function. For H.248, the gateway should use the Inactivity Timeout package to do this.

Figure 1 CPE GW Connected via a NAT



Without special NAT configuration, incoming IP connections are not possible to a host behind a NAT. So, in order for a connection to traverse a NAT, it must originate from within the NAT zone. For us, this means that the connections must be initiated by the gateway rather than the CS2k. The figure below shows both H.248 and SCTP connections being originated from a CPE gateway.

Figure 2 Functional Behavior Diagram



In a normal, non-NAT, setup, H.248 connections are already initiated from the gateway, but SCTP connections are done from GWC to GW. This is changed by this feature for gateways behind a NAT.

When the CS2k receives an incoming connection from the gateway, the connection will appear to be from the NAT's public IP address, rather than the gateway. As we cannot be sure of this address when provisioning the gateway, we need to rely on the GWC to determine the IP address and port by extracting them from the IP headers. This process is known as IP auto discovery, and has already been implemented for small line gateways using the MGCP protocol. This was done by feature 59034470 - "CS2000 Support for IP Discovery". When an IP address of 0.0.0.0 or a port of 0 is provisioned for a gateway, the GWC will attempt to automatically discover the true values. This feature extends support for this functionality to the H.248 and SCTP protocols.

1.1.3 H.248 Support

In order for H.248 to traverse a NAT, the following must be set up:

- The MID of messages sent by the gateway must match the provisioned name of the gateway on the CS2k. The FQDN of the gateway is suggested for use here.
- The gateway should NOT include the "AD" (ServiceChangeAddress) parameter in the H.248 ServiceChange message the it sends to the GWC.
- The GW must be provisioned with an IP address of 0.0.0.0 unless the public IP address that the NAT will use is known.
- The GW must be provisioned with a H.248 protocol port of 0 unless the public port that the NAT will use is known.
- The NAT/VPN that the GW resides behind must be specified when the GW is provisioned, via the 'adjacent Network Zone' field in the 'associate Gateway' dialog.

- The gateway must support the H.248 Inactivity Timeout package, and use it to maintain a minimum traffic level over the NAT. This traffic level must be sufficient to prevent the NAT bind timing out.

1.1.4 SCTP Support

In order for SCTP to traverse a NAT, the following must be set up:

- The gateway must attempt to initiate the SCTP connection to the GWC.
- The INIT message used to initiate the SCTP association must contain a Host Name Address parameter. The contents of the parameter must match the provisioned name of the gateway on the CS2k.
- The GW must be provisioned with an IP address of 0.0.0.0.
- The NAT/VPN that the GW resides behind must be specified when the GW is provisioned, via the 'adjacent Network Zone' field in the 'associate Gateway' dialog.
- The gateway must send SCTP heartbeat messages in order to maintain a minimum traffic level over the NAT. This traffic level must be sufficient to prevent the NAT bind timing out.

1.2 CS2M Provisioning Support For NAT Traversal

The CS2M platform is modified to allow the provisioning of adjacent Network Zones against the Audiocodes GW. This is done by enabling existing functionality currently supported for small line and H.323 type GWs.

For completeness the following figures show the newly enabled functionality for the Audiocodes GW.

Figure 3 shows the Associate Media Gateway dialog for the Audiocodes GW. The Internet Transparency selector box is enabled allowing an adjacent Network Zone to be optionally associated with the GW.

Figure 4 shows the GW list panel from the CS2M provisioning GUI. Here an Audiocodes GW has been previously added with an adjacent ITRANS Network Zone. The “Adj ITRANS MB” field is showing the Network Zone associated with the GW.

Figure 5 shows the input XML for the assocMG OSSGate interface. Here the itransMiddleboxName tag value pair has been specified to request an ITRANS Network Zone be associated with the new AUDIOCODES GW.

Figure 6 shows the Change GW - Change Adjacent ITRANS Network Zone dialog.

Figure 7 shows the changeAssocMB OSSGate XML interface as used to change the Network Zone associated with a GW.

Figure 3 Associate Media Gateway Dialog Showing IP-VPN / LBL Selection Box

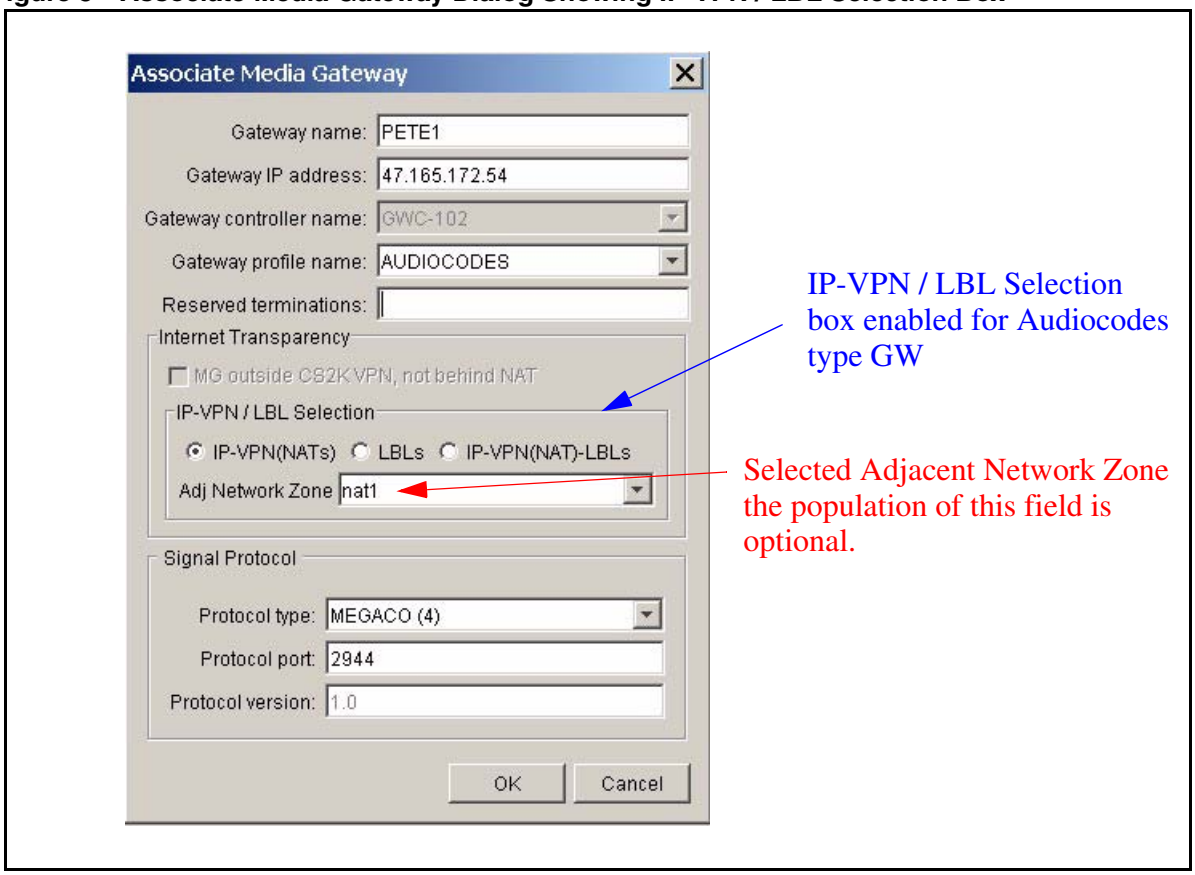


Figure 4 Adjacent Network Zone For Audiocodes GW Shown In GW List

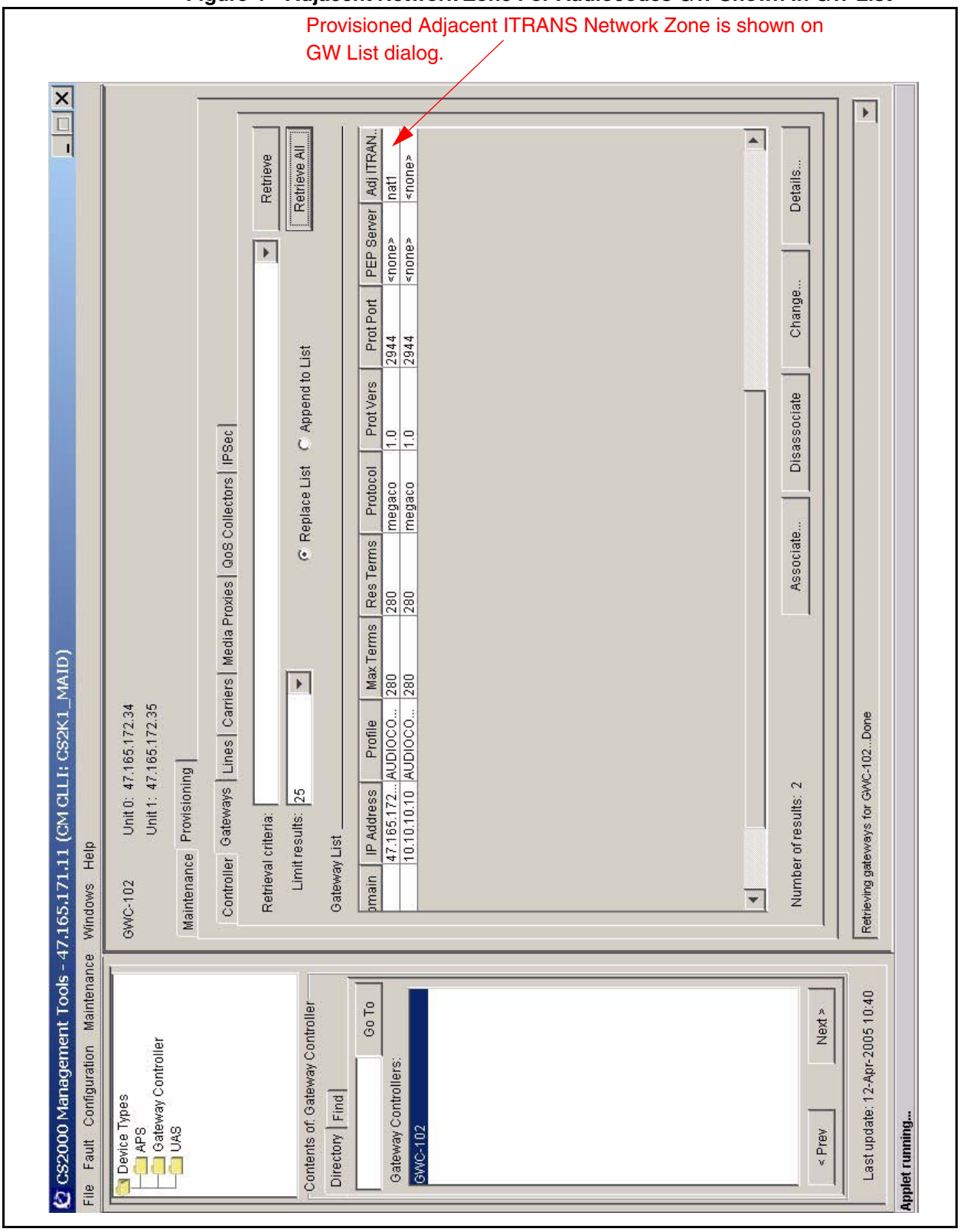


Figure 5 OSSGate assocMG Request Specifying adjacent ITRANS Network Zone

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <assocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>PETE1</mgUIName>
          <mgProfileName>AUDIOCODES</mgProfileName>
          <mgIpAddr>2.2.2.2</mgIpAddr>
          <mgProtocolType>4</mgProtocolType>
          <mgProtocolVersion>1.0</mgProtocolVersion>
          <mgProtocolPort>2944</mgProtocolPort>
          <gwcUIName>GWC-102</gwcUIName>
          <itransMiddleboxName>nat1</itransMiddleboxName>
        </Parameters>
      </assocMG>
    </Methods>
  </Command>
</CommandList>
```

adjacent ITRANS Network Zone to be associated with this Audiocodes GW. This field is optional

Figure 6 Change Gateway - Change Adj ITRANS Zone

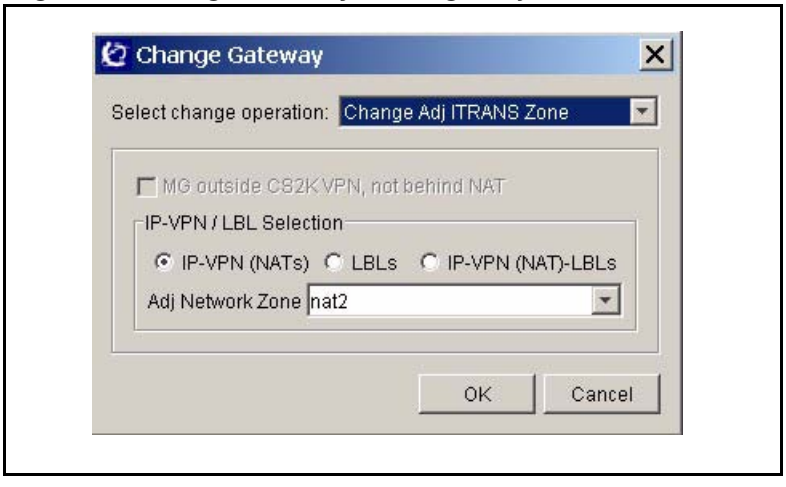


Figure 7 OSSGate changeAssocMB Request For Audiocodes GW

```
<?xml version="1.0" encoding="UTF-8"?>
<CommandList>
  <Command>
    <Interface>ITransIf</Interface>
    <Methods>
      <changeAssocMB usn="1" version="1.0">
        <Parameters>
          <MGname>PETE1</MGname>
          <itransMiddleboxName>nat2</itransMiddleboxName>
        </Parameters>
      </changeAssocMB>
    </Methods>
  </Command>
</CommandList>
```

1.3 Hardware Requirements or Dependencies

Not applicable.

1.4 Software Requirements or Dependencies

The software load on the gateway must be capable of fulfilling the gateway requirements in the “H.248 Support” and “SCTP Support sections above. The 4.6 version of software for the Audiocodes Mediant 2000 gateway will satisfy these requirements.

1.5 Limitations and restrictions

Currently support for this feature is limited to the Audiocodes gateway profile. Support for other gateway profiles will require an integration activity.

1.6 Interactions

Not applicable.

1.7 Glossary

Term	Description
SCTP	Stream Control Transmission Protocol
NAT	Network Address Translation

Product = CS 2000

A00009550 -- CBM-NPM Patching Convergence

Functional Description

1: Applicable Solution(s)

PT-IP, UA-AAL1, DMS

1.1 Description

Prior to SN09, two software tools exist to administer software updates associated with SSPFS-based software; Core Billing Manager (CBM) Software Installation Manager (SIM) and Network Patch Manager (NPM).

Prior to SN09, SIM is used to maintain software updates associated with the CBM software in TDM, Wireless, and Succession configurations. In those configurations, SIM is also used to administer SSPFS-based patches on the CBM Solaris-based machines.

The intention of this feature is to integrate the CBM SIM functionality into NPM, and to support a single patch manager for the whole network to administer software updates for TDM/Wireless and Succession configurations. The NPM user interface is utilized as a central location for administering all software updates. For SSPFS based patches, the NPM is used in TDM/Wireless and Succession configurations for patch maintenance and administration. Also, for Core Element (CEM) based applications delivered with CBM, NPM is used for patch maintenance and administration.

Figure 1 SN09 TDM/Wireless Behavior

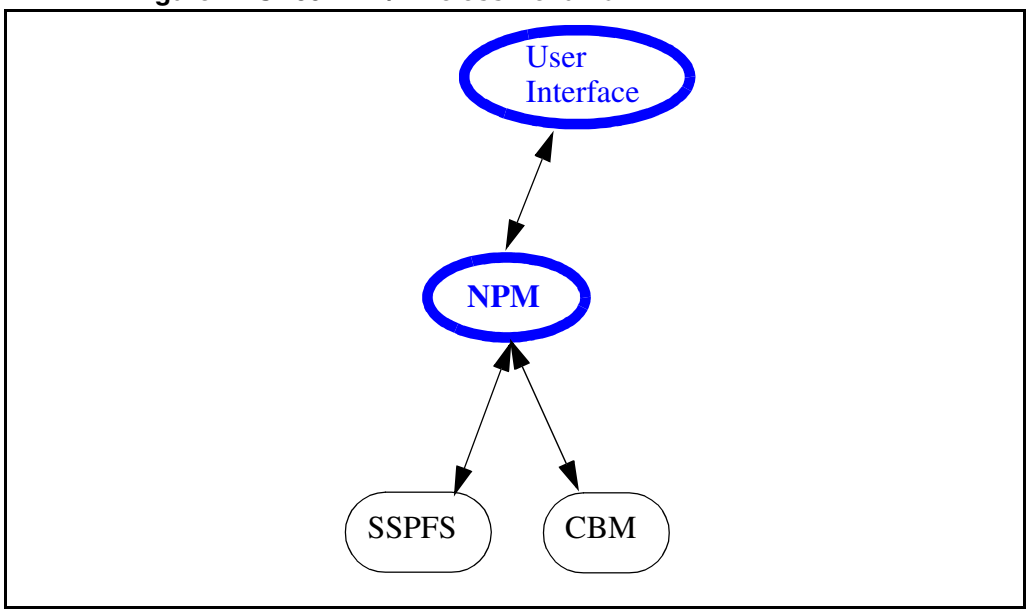
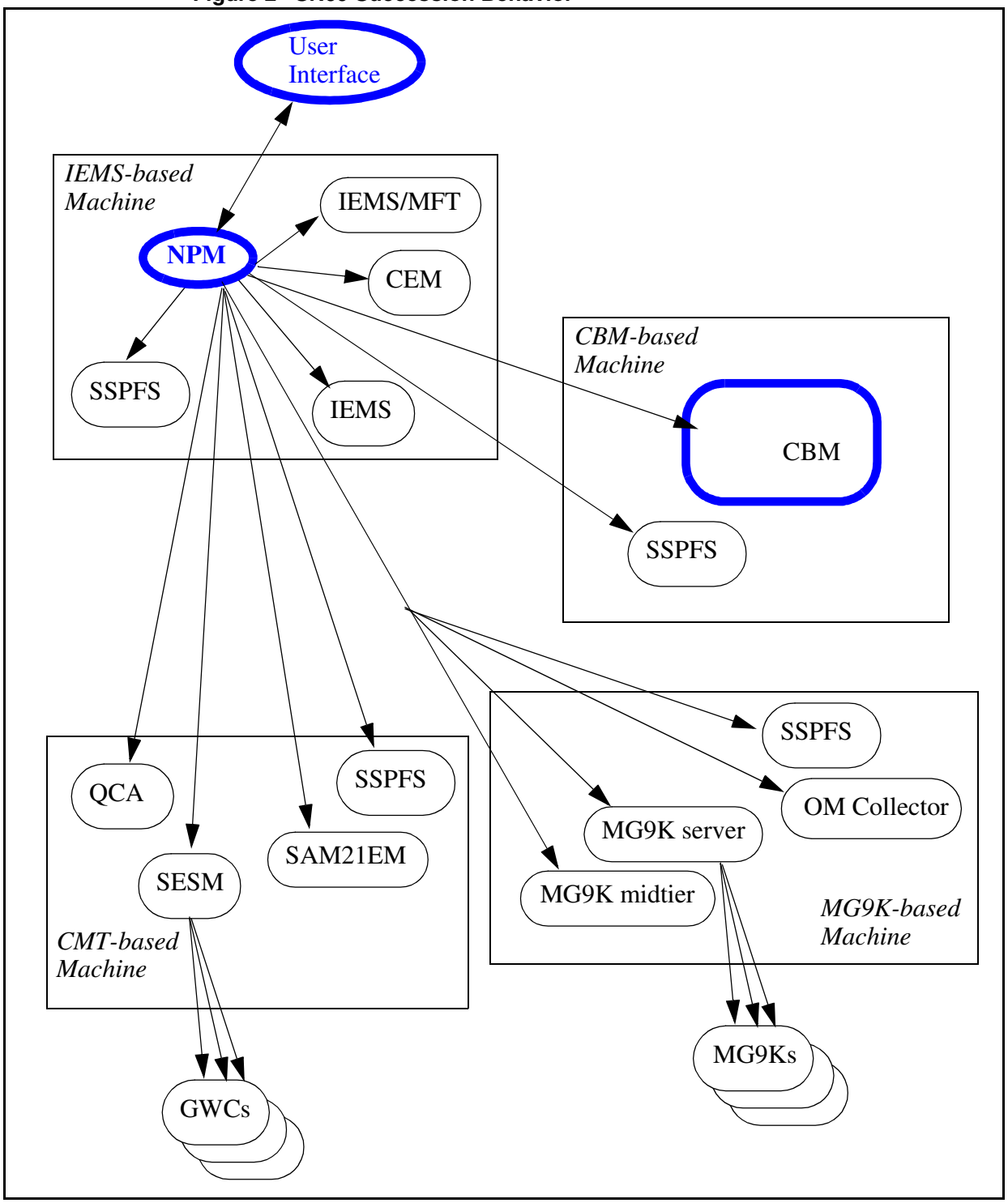


Figure 2 SN09 Succession Behavior



1.1.1 Cumulative Patching

CBM patches are cumulative. For CBM related applications, each patch

delivers the entire package content and subsequent patches contain the fixes that prior patches introduced. For CEM related packages, each patch delivers the file of the package that has changed and subsequent patches contain all previously changed files. Both approaches allows a customer to apply only the latest patch if desired since it will contain all of the fix content included in previous patches. CBM patches are delivered by RPS. There is only one Released patch at any given point in time for a particular package, unless it is the first patch for the package which can be at Verified or Released status. After a patch is Released for a package, all previous patches are set to Superseded in RPS and will no longer be delivered.

NPM is the patch management system to apply and remove CBM patches and perform maintenance patching activities on the CBM applications. All patching functionality available in NPM is available for CBM patching.

With this methodology of patching, if 3 patches have been released for a given package, and all 3 have been downloaded to a customer site, the customer can choose to physically apply patch 1, patch 2, and patch 3, or the customer can choose to apply patch 3 only. If only patch 3 is applied, this essentially results in having patch 1, patch 2, and patch 3 applied. If only patch 3 is applied, patch 1 and patch 2 cannot be removed individually. NPM will store a relationship attribute that indicates patch 3 is temporary (T) and patches 1 and 2 are bound (B). If only patch 3 is applied, when patch 3 is removed, patch 2 and patch 1 are also removed.

1.1.2 Multiple Devices

CBM registers with NPM as multiple patchable devices. A unique load name is associated with each device. The load name is used for patch calculation purposes. Patches are applied to and removed from a device. Devices are restarted to enable or disable patches. In a high availability (HA) or clustered environment, 2 instances of the device will appear; one instance for the active side and one instance for the inactive side. In a HA environment, customers have the option to apply patches on both sides individually, or request both sides be patched in one transaction.

An example CBM deviceid is CBM_BILLING.

1.1.3 Patching Maintenance

When the patchable CBM applications are installed, the NPM automatically becomes aware of them. CBM devices appear in reports and the device list of the NPM GUI or CLUI. The following functions that exist for other targets are now available for CBM devices.

- apply
- remove
- audit

- restart
- set/report creation
- plans/automation
- alarms

1.1.3.1 CBM Patch Application and Removal

Like existing OAM Java-based applications such as SESM, SAM21EM, or IEMS components, the CBM requires 2 steps for application and 2 steps for removal of patches.

application

- apply command from the NPM GUI or CLUI (sets patch to applied/disabled and stages patch for actual patch application)
- restart command from the NPM GUI or CLUI on CBM device (sets patch to applied/enabled after restarting the device)

removal

- remove command from the NPM GUI or CLUI (sets patch to removed/enabled and prepares patch for actual patch removal)
- restart command from the NPM GUI or CLUI on CBM devices to disable the patch (sets patch to removed/disabled after restarting the device)

When CBM is running in a clustered configuration, the 2 step application and removal of patches is necessary on the active side of the SSPFS-based machine, and only for those devices which have running applications on the inactive side. A restart from the NPM GUI or CLUI of a CBM device is required to enable or disable patches only for those devices which have running applications. When a patch is applied to or removed from CBM device which has no running applications, the patch is automatically enabled or disabled.

The apply and restart operations from the NPM GUI and CLUI can be automatically scheduled via NPM plans (autoapply and autorestart).

NPM will not automatically reboot a machine for a patch that has a reboot required.

1.1.4 Patchid

The patchid format for CBM patches can have up to 32 alpha-numeric characters. An example CBM patchid is NTBASE220203-01. The patchid of the second version of that patch is NTBASE220203-02.

1.1.5 Patch File Format Modifications

The patch file format is modified with this feature. The following additions and changes have been made.

- A new **H** record is introduced to track patches that cannot be applied when the given patch is applied. This would happen in the case of a patch that had previously depended on a patch which became obsolete. Once a dependency is obsolete, any new patches cannot depend on that. This new record is stored in the ADM section of the patch file. Zero to many of these records can exist.

  H ANTI_PREREQ <patchid> where patchid is the name of the patch that cannot be applied when the given patch is being applied.

1.1.5.1 Patch Delivery to Customers

RPS is used to deliver CBM patches to customers. NPM has a Patch File Receipt System (PFRS) setup that allows the customer to configure where to have patches delivered for NPM to retrieve, and where to deliver an inform report for RPS to use for patch calculation purposes. RPS will deliver CBM patches based on a calculation of the load name associated with a patch and the load name associated with the device on site. Information on PFRS setup can be found in the online NPM GUI or CLUI help.

RPS delivers only the latest version of a patch for a given software package. Once a new version of a patch is released, all previous versions are Superseded and are no longer delivered. The customer needs to only apply the latest version of a patch since it includes in it all previous software changes.

1.1.5.2 Online Help

NPM provides the user online help via the GUI or CLUI. A CLUI help document is also available in the NpmCluiHelp.PDF document on the NPM server machine at /opt/nortel/NTnpm/documents.

1.2 Hardware Requirements or Dependencies

A windows based PC machine is required to use the NPM GUI.

1.3 Software Requirements or Dependencies

The SN09 CBM load is required to interact with NPM.

1.4 Limitations and restrictions

1.4.1 Patch Dependencies and Maintenance Releases

In SN09, patch dependencies are permitted between patches applicable to different devices. A CBM patch can have a dependency on an SSPFS patch. If an SSPFS maintenance release (MR) is created and contains a dependent SSPFS patch, the CBM software that requires the now built in SSPFS patch will also have to build a new MR on top of the SSPFS MR. If this is not done,

some other type of software delivery strategy will need to be implemented for the CBM load that contains the patch with a dependency.

1.4.2 Patch Dependencies and Obsolete Patches

A CBM patch can have a dependency on a patch in the SSPFS device. If a patch dependency is created between a CBM patch and an SSPFS patch, and the SSPFS patch becomes obsolete, all CBM patches that depend on the obsolete SSPFS patch must be removed from customer sites. Once an SSPFS replacement patch is downloaded and applied, a new CBM patch is created that depends on the replacement patch, and then delivered to customers. If obsoleting an SSPFS patch is determined to be too disruptive, a new SSPFS patch should be written on top of the bad SSPFS patch and delivered to the customer.

1.5 Interactions

None

1.6 Glossary

Term	Description
NPM	Network Patch Manager
CEM	Core Element Manager
RPS	Regional Patch Selector
CBM	Core Billing Manager
HA	High Availability
GUI	Graphical User Interface
CLUI	Command Line User Interface

Product = CS 2000

A00009822 -- General Security Log When the User Logs Out

Functional Description

1: Applicable Solution(s)

PT-AAL1, PT-IP, UA-AAL1, UA-IP, PT-AAL2

1.1 Description

The Client Session Monitor tracks and records the authentication's, client starts and client stops of the users within the system. For SN09, those applications which begin reporting client start and stops are MG9kEM and CS2M.

The Client Session Monitor allows the end security user to view reports that display which client application sessions are currently active and for what user. It will also provide the reporting ability to view historical data regarding client application usage by user, date or device. The historical data includes start and end times of client sessions, source ip, destination ip, application name and reason for the session end.

The Client Session Monitor also provides interfaces for the clients to retrieve the last time a given user successfully authenticated against the system. This feature modifies the common launch page to display this last successful authentication time - as well as the sspfs LoginAuthentication GUIs.

The Client Session Monitor Reporting Utility is launchable via the IEMS client as well as direct URL or a cli interface provided on the server.

1.2 Hardware Requirements or Dependencies

This feature is available only on IEMS Central SS systems.

1.3 Software Requirements or Dependencies

SN09 IEMS Central SS software
Oracle

1.4 Limitations and restrictions

Only successful user initiated authentications which are authenticated via the IEMS SS are recorded. Any authentication which is performed locally will not be recorded in the Client Session Monitor.

In the case where a client session appears to still be active via the report - but the security user knows the session to no longer be active - the security user can mark that session as completed. Marking a session as completed will not cause any actions outside the realm of this report. It will simply update the session activity in the database - it will not force a user off - end their session - etc. If a user is still active and their session is marked completed, when the user truly ends the session - the row will be updated with that action's end time.

1.5 Interactions

None

1.6 Glossary

Term	Description
CS2M	Call Server 2000 Manager
IEMS	Integrated Element Manager Server
IEMS Central SS	IEMS Central Security Server
MG9kEM	Media Gateway 9000 Element Manager

2: Fault Management for A00009822

2.1 Fault management strategy

This feature logs the interaction with Client Session Monitor. A security log is generated when the Client Session Monitor processes the notification of the authentication and client lifetime events. Logs are generated as per the MFT Logging Guidelines(FW3.3 Loggin Service Guidelines).

2.2 Fault management tools and utilities

2.2.1 Faults, Alarms and Logs

The logs output are information only logs.

Security logs are generated for registering successful authentications to the Client Session Monitor. If the Client Session Monitor can not decrypt the information received to register authentication or client lifetime events, an information log is output. Security logs are generated when the clients indicate a successful login and logout.

2.3 Logs

2.3.1 Formats

The format of a security log is

Date Logger Src_usr Src Dst Stat Evnt_type Cmd Message

2.3.2 Explanation

2.3.2.1 Authentication

When the Client Session Monitor interface is called to register an authentication event, the following example log is output to the security log

Mar 31 18:27:48 wnc0y0nr PROG=CSNotifierEngine.java SRC.USR=rtpu SRC=47.142.122.200 STAT=Success EVNT.TYPE=USER_ACT_Security

CMD=SESSION_AUTHENTICATED MESSAGE="User Authenticated: SID = 53, LastLoggedIn=Last login: Thu Mar 31 18:28:00 EST 2005 from 47.142.211.68 to 47.142.122.200"

This is an information log only, no action is required.

2.3.2.2 Client start

When the Client Session Monitor interface is called to register a client start event, the following example log is output to the security log:

Mar 31 18:18:10 wnc0y0nr PROG=CSNotifierEngine.java SRC.USR=rtpu SRC=47.142.122.200 STAT=Success EVNT.TYPE=USER_ACT_Security CMD=SESSION_START MESSAGE="doSessionStart Successful: SID = 52"

This is an information log only, no action is required.

2.3.2.3 Client stop

When the Client Session Monitor interface is called to register a client stop event, the following example log is output to the security log:

Mar 31 17:55:19 wnc0y0nr PROG=CSNotifierEngine.java SRC.USR=UNKNOWN SRC=47.142.122.200 STAT=Success EVNT.TYPE=USER_ACT_Security CMD=SESSION_STOP MESSAGE="doSessionEnd Stopped: SID = 42, Reason = User Exit"

This is an information log only, no action is required.

2.3.2.4 Could not decrypt

When the Client Session Monitor interface can not decrypt the information received, the following example log is output to the security log:

Feb 21 18:30:33 comp5iems CSM:class_security.ver02 SRC_USR="rtpo" STAT=”Fail”EVNT_TYPE=”USER_ACT_Security” CMD=”SESSION_Authentication” MESSAGE=”RegisterClientSessionStopCould not decrypt message”

2.3.2.5 Mark done

When the Client Session Monitor receives a request to manually mark an active session as stopped (.e.g. the Mark Done from the GUI is executed), the following example log is output to the security log:

Apr 2 07:17:28 wnc0y0nr PROG=CSNotifierEngine.java SRC.USR=UNKNOWN SRC=47.142.211.35 STAT=Success EVNT.TYPE=USER_ACT_Security CMD=SESSION_STOP MESSAGE="doSessionEnd Stopped: SID = 237, Reason = Admin Marked Done"

2.3.2.6 SID not valid

When the Client Session Monitor interface is called to register a client start or stop event and the session Id is not valid, the following example log is output to the security log:

Feb 21 18:30:33 comp5iems CSM:class_security.ver02 SRC_USR="rtpo" STAT=”Fail”EVNT_TYPE=”USER_ACT_Security” CMD=”SESSION_Stop” MESSAGE=”RegisterClientSessionStop dropping invalid session stop because SID not valid: SID=5678”

2.3.3 Field descriptions

Table 2: MFT Security Log Fields

Field Name	Type	Max	Max length Syslog	Definition	Required
Date	*Date*		*15 +1*	*ISO 8601 standard format expressed as yyyyMMddhhmmssZ in java.text.Simple-DateFormat notation. This field is expected in all logs*	*Mandatory*
Level	*String*	*16*	*5*	*ASCII expression of logging level and not an integer.*	*Mandatory*
Logger	*String*	*256*		*ASCII expression of the logger name as chosen by the application that does the logging*	*Mandatory*
Src_usr	*String*	*128*	*8+32+3*	*The source user name or identification*	*Mandatory*
Src	*String*	*256*	*39+1*	*The value should contain the source device’s host name, or its IP address and (optionally) the port number.*	*Mandatory*
Process	*String*	*32*	*32+1*	*The value should contain the process name and process ID for the process on the device that generated the message.*	*Mandatory*
Msg	*String*	*1024*	*4+64+3*	*The log message itself.*	*Mandatory*
Stat	*String*	*32*	*5+7+3*	*The state or status of the process. Possible values: Failure, Success, Start or End*	*Mandatory*
Log_type	*String*	*64*	*9+11+3*	*Type of the log message. Possible values: Trace, Application, Security, Exception*	*Mandatory*
Dst	*String*	*256*	*4+39+3*	*The address of the destination in the same format as the source*	*Mandatory*

Table 2: MFT Security Log Fields

Field Name	Type	Max	Max length Syslog	Definition	Required
Doc	*String*	*1024*	*4+64+3*	*The name of the accessed resource*	*Mandatory*
Mid	*String*	*64*	*4+64+3*	*The concept is to log message identifiers instead of actual messages so that the message identifier can be used to look up a language specific form of the message in display tools*	*Mandatory*
Src_offend	*String*	*256*	*11+39+3*	*The address of the originating device generating information which triggered a security log event in the same format as the source*	*Optional*
Dst_usr	*String*	*128*	*8+32+3*	*The destination user name or identification*	*Optional*
Src_mail	*String*	*128*	*9+32+3*	*The source email address*	*Optional*
Vol	*Integer*		*4+10+1*	*The number of bytes*	*Optional*
Vol_sent	*Integer*		*9+10+1*	*The number of bytes sent*	*Optional*
Vol_rcvd	*Integer*		*9+10+1*	*The number of bytes received*	*Optional*
Cnt	*Integer*		*4+10+1*	*The number of articles, files, events*	*Optional*
Cnt_sent	*Integer*		*9+10+1*	*The number of articles, files, events sent*	*Optional*
Cnt_rcvd	*Integer*		*9+10+1*	*The number of articles, files, events received*	*Optional*
Host	*String*	*256*	*5+39+3*	*The name of the host that issues the log*	*Optional*
Host_type	*String*	*64*	*10+32+3*	*The device type from which the log was generated*	*Optional*
Prog_file	*String*	*256*	*10+32+3*	*The name of the program source file from which the log was generated*	*Optional*
Prog_line	*Integer*		*10+10+1*	*The line number of the Prog_source file*	*Optional*
Tty	*String*	*16*	*4+16+3*	*The tty field describes the user's physical connection to the host*	*Optional*
Prot	*String*	*64*	*5+8+3*	*The protocol field specifies the protocol used*	*Optional*
Cmd	*String*	*1024*	*4+64+3*	*The command field is an issued command*	*Optional*

Table 2: MFT Security Log Fields

Field Name	Type	Max	Max length Syslog	Definition	Required
Evnt_type	*String*	*64*	*10+32+3*	*The evnet type field specifies the type or classification of the event*	*Optional*
Src_oid	*String*	*64*	*8+64+3*	*The object identifier is a unique registration number for a device, which will be part of the X.500 directory*	*Optional*
Log_date	*String*		*15+1*	*The original date of the log message. Used when logs are spooled and held before being sent by the logging service to the final destination*	*Optional*

2.3.4 Action

No immediate action required

2.3.5 Associated OMs or PMs

None

2.3.6 Additional information

None

2.4 Alarms

None

2.5 Related documentation

FW3.3 Logging Service Guidelines

http://knowledgeonline.ca.nortel.com/sws/livelink.exe?func=ll&objId=3018691&objAction=browse&sort=name

3: Configuration for A00009822

3.1 Hardware and Software Requirements

The server piece of this application at this time requires an oracle database server to be in place on the server machine.

3.2 Initial Configuration

SN09 IEMS Central SS software

Oracle

3.3 Memory Requirements

The statistics that follow were taken at a stressed state. The database was populated with 6000 session entries and a CSM Report Client was configured to pull this data every 10 seconds.

RAM Usage: 10 M (1 M with 200 records)

Note: CSMEngineNotifier & CSMEngineReport are servlets. They reside within the Tomcat process and therefore we are not adding in the existing JRE overhead calculations.

Application Code Disk Usage: 2066 K (du -s -k /opt/nortel/CSReport)

Application Data Disk Usage: 0

The CSM design heavily utilized the database for storage retention. We do not keep any custom CSM data in the /data partition.

Application Database Usage:

The CSMDB_TS - with 6000 entries - used 720,896 Bytes.

3.4 Upgrade Considerations

At this time, this feature will not impact upgrades.

3.5 Data schema

A new tablespace called CSM_TS will be added to the oracle database server on the authentication machine to support this feature. In this tablespace will reside two tables, Activity & Version.

3.6 Element Management

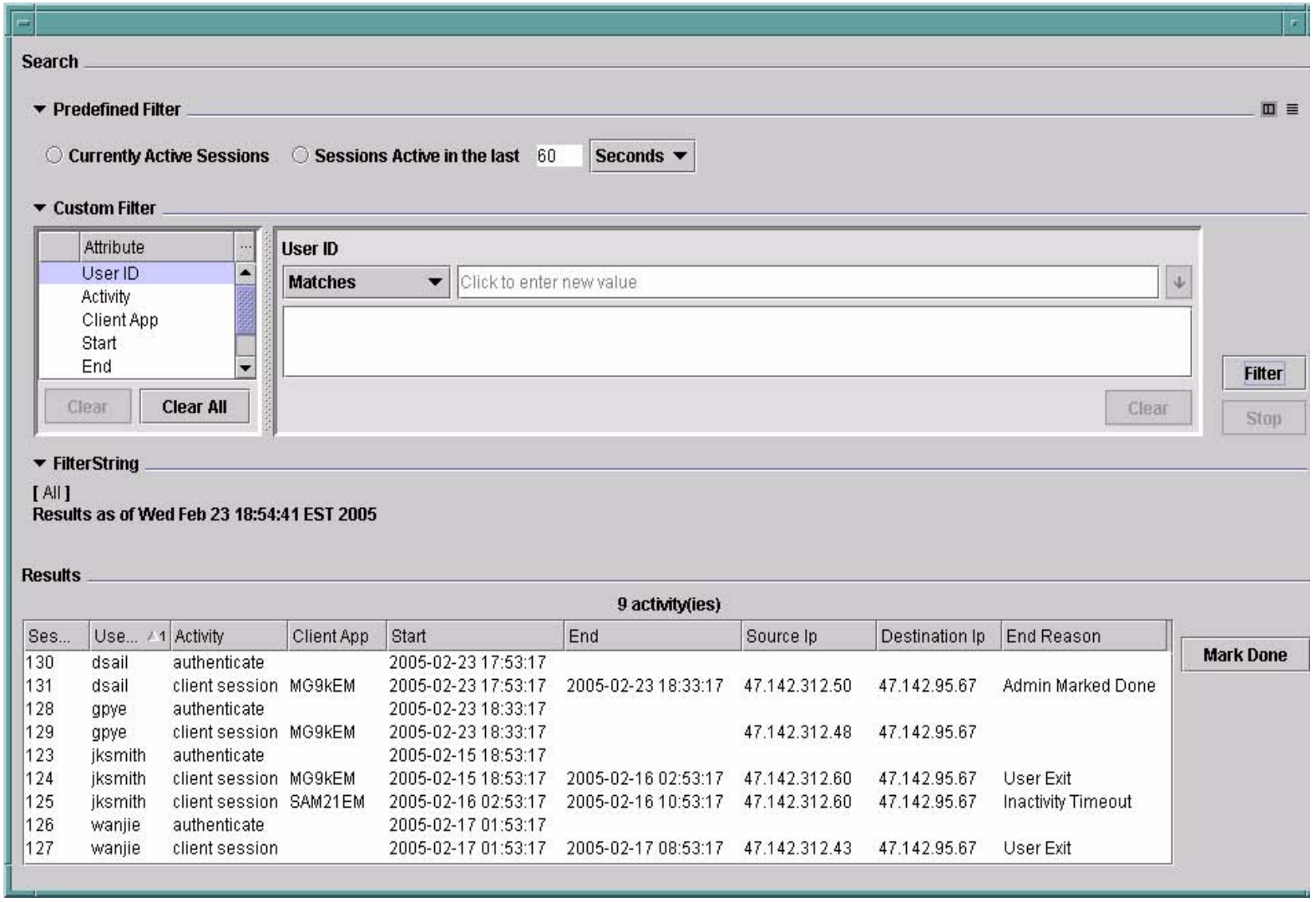
3.6.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Client Session Monitor	New

3.6.2 GUI information

3.6.2.1 GUI name: Client Session Monitor



3.6.2.1.1 Functional description

The CSM GUI client provides a report that will give the security user the ability to view the historical client sessions for the users. The report will by default populate with the currently active sessions. However, the user has the ability to configure the display criteria. The report will refresh the displayed contents once every 60 seconds.

The CSM GUI client can be launched via a menu on IEMS or directly accessing the URL (jnlp) for the client. The CSM GUI is hooked into the common LoginServlet code. If a user has an authentication session active, the GUI will be displayed. However, if an authentication session is not active, the user will be prompted for user and password via the common login dialog.

Once logged in the users group levels will be checked - the GUI report can only be viewed by those users which are in the SEC* group. Any user not in that group will not be allowed entry to the report. Also, the ability to mark a client session as ended will only be accessible to those users of the group SECADM.

3.6.2.1.2 GUI usage and implications

This UI will be used to display current client application sessions as well as historical lifetime of client application sessions by user.

When the GUI first is displayed - the report shown will be for all current application sessions. This report will update every 60 seconds to maintain accuracy. The user has the ability to modify the filter (search) criteria for the report. If the users wishes to change a criteria they simply modify the filter parameters and hit the ‘Filter’ button. This will repopulate the list with the data matching the new filter criteria. The criteria the report is generated with - and the time of generation - are clearly displayed in the FilterString area.

In setting the filters, the user may choose either to use a predefined criteria or to create a custom criteria from the available attributes. The two predefined criteria filters available are ‘currently active sessions’ and ‘activity within the last <timeperiod>’.

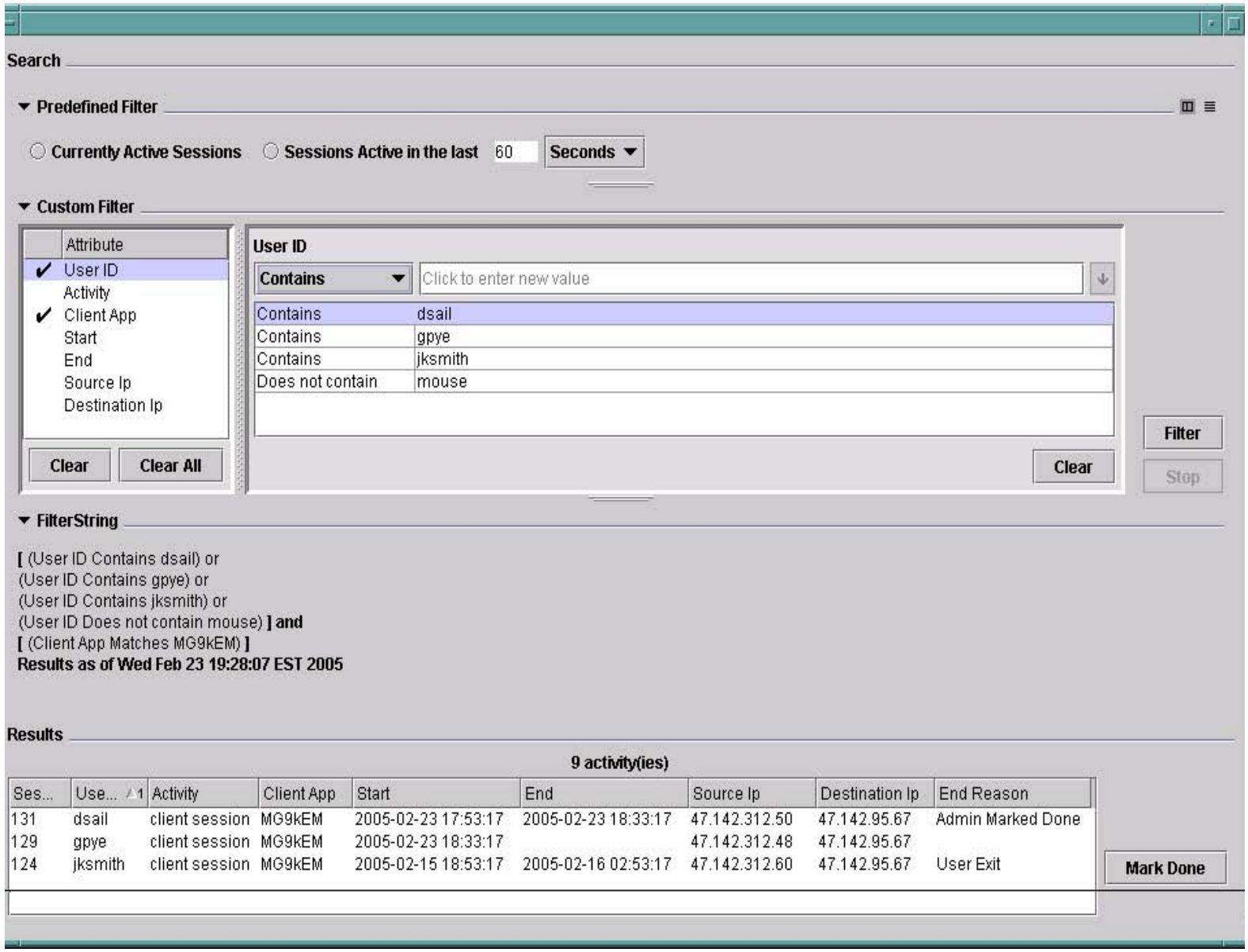
The predefined filter ‘currently active sessions’ will populate the custom filter area with the correct settings to query on active sessions. The user then hits ‘Filter’ and the report will update with this criteria.

The predefined filter ‘activity within....’ allows the user to request the report display all activity that has occurred in an interval prior to the report generation. The user may enter the numeric value for the time interval and the period type from a choice option of “Seconds”,”Minutes”,”Hours”,”Days”. Once the user has selected their settings - they simply hit the “Filter” button and the report will update.

The “Custom Filter” area allows a user to build a custom criteria from the available attributes. For fields which are strings such as UserID, Activity, ClientApp, SourceIp and DestinationIp the criteria that can be used to match on are “Matches”, “Does not match”, “Contains”, “Does not contain”, “Starts with”.

For fields which are dates such as Start Activity and End Activity - the matching criteria are “Matches”, “Does not match”, “Before”, “After”, “Between”. The date requires the date format of YYYY-MM-DD HH:MM:SS. The exception is that the term “Current” can be entered in the field to indicate the current time and the turn “Null” can be entered to indicate the time is not yet set.

Once a user has decided a criteria is correct - they simply need hit “Filter” and the report will populate. The below snapshot shows a report that has criteria matching (and not matching) on user id - as well as Client Activity. The user simply selected the field to query upon - then the match criteria - entered the data in the text field that says “Click to enter new value” and hit return. The criteria is then added to the list of query items for that data element.



3.6.2.1.3 GUI size

Not Applicable

3.6.2.1.4 GUI fields

The following table lists fields for GUI:

Table 2 GUI field descriptions

Field	New or Changed	Entry	Explanation and action	Associated MIB entry
SessionID	New	String	This is the id that uniquely identifies a client activity session.	Table CSM_TS.Activity.SessionId
UserID	new	String - 8 char length	This is the login id of the user who initiated the session.	Table CSM_TS.Activity.UserId
Activity	new	String	Designates the type of activity - ex. Authentication or Client Session	Table CSM_TS.Activity.ActivityType
Client Application Name	new	String	The name of the client application that session denotes. (not applicable to authentication).	Table CSM_TS.Activity.AppName
Start Date	New	Date (YYYY-MM-DD HH:MM:SS)	This is the time the activity started.	Table CSM_TS.Activity.StartDate
End Date	New	Date (YYYY-MM-DD HH:MM:SS)	This is the time the activity ended. (Not applicable to authentication).	Table CSM_TS.Activity.EndDate
Source Ip	New	String [xxx.xxx.xxx.xxx]	This is the Ip Address of the machine from which the user launched the session. (Not applicable Authentication)	Table CSM_TS.Activity.SourceIp
Destination Ip	New	String [xxx.xxx.xxx.xxx]	This is the Ip of the machine from which the client application is loaded. (ex. MG9kEM Midtier)	Table CSM_TS.Activity.DestinationIp
End Reason	New	String	This is the reason the session ended. Reasons can be User Exited, Inactivity, etc.	Table CSM_TS.Activity.EndReason

3.6.2.1.5 Usage example

The Client Session Monitor will be initially displayed to the user populated with the entries indicating current active client sessions. The user has the ability to modify the report criteria by selecting new criteria and then hitting "Filter". Once "Filter" is hit the data list will repopulate with the results of the new query. The Query that the current data list applies to is displayed in the middle section of the form under "Filter String" and is timestamped with the last time the query was run.

In the case where a client session appears to still be active via the report - but the security user knows the session to no longer be active - the security user can mark that session as completed. The ability to mark a client session as ended will only be accessible to those users of the group SECADM. Marking a session as completed will not cause any actions outside the realm of this report. It will simply update the session activity in the database - it will not force a user off - end their session - etc. If a user is still active and their session is marked completed, when the user truly ends the session - the row will be updated with that actions end time.

The displayed report has the ability to sort by clicking on the column the user wishes to key the sort.

3.6.2.1.6 Context sensitive launching information

There are two methods of launching this client. The first will be from the IEMS security layer via a menu item.

The second will be via a url to the authentication machine. This url will be something along the lines of:

http://<ip>/ClientSessionManager.jnlp

If the user has already authenticated and that authentication session is still active, the CSM GUI will be immediately displayed. If there is not an authentication session currently active - the user will be prompted for their user name and password via the common login utility.

3.7 Security

3.7.1 Network configuration

None

3.7.2 Key management

None

3.7.3 Protocol

This CMS GUI will be a java client which is launched using the JavaWebStart client support software.

The messaging between the CMS GUI and the CMS Server will be via https.

3.7.4 Authentication

Access to the Client Session Monitor is for this feature will require the user to login and authenticate via the common login panel. The user must be a member of the sec* group.

3.8 Configuration Walkthrough

The CSMonitor Audit functionality keeps the session database from growing too large. All client monitor sessions, even after they are closed, are kept in the Client Session Monitor database to provide historical data of logins and logouts. The CSMonitor Audit functionality allows the user to configure when to poll the database for sessions to clean up and allows the criteria for clean up to be specified.The selection of sessions is strictly based on start time and may delete session which have not ended. Therefore, care must be taken to specify criteria so as not to delete any active sessions.

In order to configure the CSMonitor Audit and start the cleanup of sessions from the Client Session Monitor database, the following steps are performed:

1 - login to the IEMS security server as root

2 - enter the cli command

3 - select the Configuration option

4 - select the Succession Element Configuration option

5 - select the CSMCLEANUP Application Configuration option

6 - select the setCleanupTime option

7 - enter the amount of time for the CSMonitor Audit to poll the database for removal of sessions based on the criteria below, sessions are only removed when the CSMonitor wakes up after the time period specified. For example, if 24 hours is specified the CSMonitor Audit wakes up 24 hours from the time CSMonitor Audit is started and queries the database for sessions needing to be removed.

8 - select the setCleanupCriteria option

9 - select criteria for removal from the database. Max sessions per user criteria keeps the sessions based on start time for each user id. Time based criteria keeps sessions based on start time.

10 - if max criteria select above, skip to step 14

for time based criteria, enter the number of hours to keep sessions. For example, it 1 hour then any session started one hour prior to the audit polling are kept. If user x has two session one started at 10:00 and another started at 13:00 and the current time is 13:20 only the session started at 13:00 is maintained in the database. If user y has three sessions, first started at 12:21 and ended at 12:30. Second session started at 13:05 and the third session stared at 13:19. All three session for user y are kept. It is advisable to keep session at least 24 hours. Suggested is 7 days or 168 hours. Maximum is 30 days or 720 hours.

11 - select exit option, until no longer in CLI.

12 - restart CSMonitor_Audit for the changes to take affect (servrestart CSMonitor_Audit)

13 - done with configuration

14 - for max session per user based criteria, enter the maximum number of session to keep for each user. Go to step 11.

Product = CS 2000

A00009839 -- Ability to apply patches during ESUP upgrade

Functional Description

1: Applicable Solution(s)

PT-AAL1

1.1 Description

To equip ESUP with patching capabilities. There are three requirements for this feature. They are as follows:

- ESUP should be able to read and apply ".patch" files.
- ESUP should support patching along with regular upgrades.
- ESUP should also have an option of "patch only" upgrade, wherein user should be able to apply only patches (and not any other files).

Format for patch files has changed from SDM20. Prior to SDM20, the patch files used to be in IBM "bff" format with ".tape" as extension. From SDM20, after creating the patches they are tarred and zipped (gzip). The resulting patch files has an extension of ".patch".

1.2 Hardware Requirements or Dependencies

No new hardware dependencies has been introduced by this feature.

1.3 Software Requirements or Dependencies

With this feature ESUP will use the NTSimTool package to convert ".patch" files to ".tape" files.

1.4 Limitations and restrictions

None

1.5 Interactions

This feature brings some changes in user interactions. Please see the configuration section of this document.

1.6 Glossary

Term	Description
SDM	SuperNode Data Manager
ESUP	Enhanced SDM UPgrade

2: Configuration for A00009839

2.1 Hardware and Software Requirements

No new hardware dependencies has been introduced by this feature.

With this feature ESUP will use the NTSimTool package to convert ".patch" files to ".tape" files.

2.2 Initial Configuration

N/A

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

2.4 Upgrade Considerations

N/A

2.5 Data schema (DS) (CM, MIBS, RDB)

N/A

2.6 Service Orders (SO) (CM & SESM)

N/A

2.7 Software optionality control (SOC)

N/A

2.8 Element Management

N/A

2.9 User interface changes

This feature brings some changes in user interactions. This feature will intoduce a new screen at the begining just **before** the existing screen where ESUP asks for media type. This new screen will prompt user to enter “upgrade type”. The options will be:

1) Upgrade to higher release

2) Patch only upgrade

Following figure shows the new screen:

Figure 1 :New screen prompting user to enter upgrade type

```
=============================================================
=
===              Enhanced SDM Upgrade Procedure
===
=============================================================
=
===
===  Please select the upgrade type
===     1) Upgrade to higher release
===     2) Patch only upgrade
===
===     type ‘abort’ to abort the upgrade
=============================================================
=

Upgrade Type >
```

If user selects option 1, then the “select media” screen comes next. If user selects option 2, then “select media” is bypassed as patches will always be taken from DISK-media only.

During an upgrade to higher release, ESUP gives user another prompt asking - whether he wants to install patches or not? If the user enters ‘yes’, ESUP

prompts the user to enter the location of the patch filesets. These prompts comes **after** the “select media” screen. Following figure explains this scenario:

Figure 2 : New prompt asking for patches location

```
================================================================
===              Enhanced SDM Upgrade Procedure
===
===
================================================================
===
=== The following device has been selected to perform the
upgrade
===
===            Media Type: DISK
===
================================================================
Continue (yes/no) >yes

Please enter the directory location for [CS2E0090 NCL Load]
Enter 'go' to accept the default or 'abort' to abort the
upgrade.
   Directory (default:/swd/sdm/esd/) >go

[01:45:44] Examining load content of /swd/sdm/esd/ .... Com-
pleted.
[01:46:38] Verifying load content of /swd/sdm/esd/ .... Com-
pleted.
Do you want to install patches (yes/no/abort)? yes

Please enter the directory location for [CS2E0090 PATCHES]
Enter 'go' to accept the default or 'abort' to abort the
upgrade.
   Directory (default:/swd/sdm/esd/) >
```

During a patch-only upgrade, ESUP will bypass the “select media” screen. It will directly prompt the user to enter the location of patches. Following screen shows that:

Figure 3 :New prompt asking for patches location in patch-only upgrade

```
============================================================
=
===              Enhanced SDM Upgrade Procedure
===
============================================================
=
===
===  Please select the upgrade type
===     1) Upgrade to higher release
===     2) Patch only upgrade
===
===     type 'abort' to abort the upgrade
============================================================
=

Upgrade Type >2

Please enter the directory location for [CS2E0090 PATCHES]
Enter 'go' to accept the default or 'abort' to abort the
upgrade.
   Directory (default:/swd/sdm/esd/) >
```

2.10 OSSGate Interface Changes

N/A

2.11 Security

N/A

2.12 Configuration Walkthrough

N/A

Product = CS 2000

A00009840 -- CBM IPSec Northbound Interface

Functional Description

1: Applicable Solution(s)

PT-AAL1

1.1 Description

This activity provides an easy-to-use IPSec configuration interface on the CBM for configuring IPSec/IKE parameters. This would be bundled as part of CLI tool of SSPFS for all SSPFS profiles.

This interface can be accessed only by the root user. No other users will be allowed to use this IPSec/IKE configuration interface.

This interface would accept user input values for various parameters related to the IPSec and IKE configurations. This interface will only support IPSec with IKE in preshared mode. No manual keying or certificate-based authentication will be supported by this CLI.

Following are the capabilities provided by the IPSec/IKE configuration interface

- Supports the option to save or edit changes
- Supports capability to abort configuration interface at any point of time
- All the configuration information would be automatically synchronized over to the mate system.
- This interface would generate configuration information for configuring IPSec on the downstream (for Solaris box). This information would be made available on the CBM in the /etc/inet/remotesystem/solaris directory as static file. The downstream would require to be manually modified to reflect this configuration information.[2] A sample downstream configuration file which would be generated by this interface is documented in the Appendix section of this document.

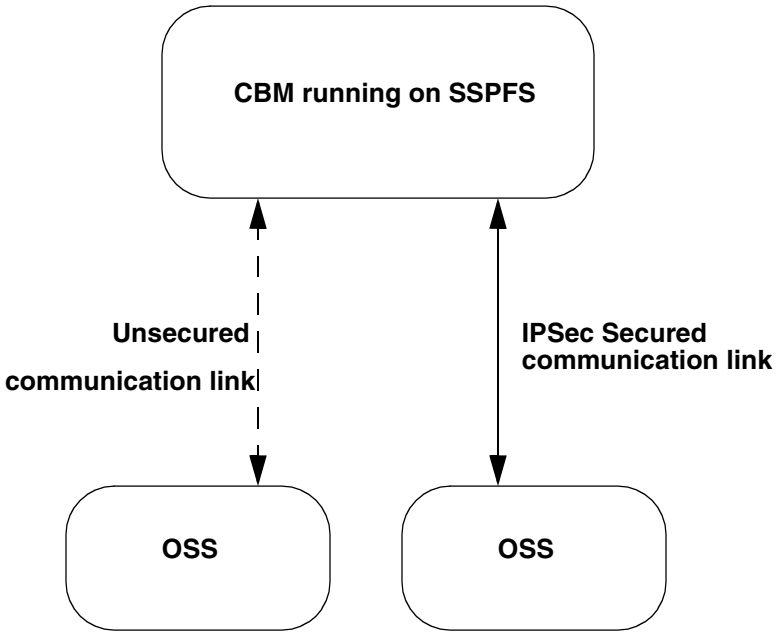
Details about the different parameters, valid options which would be accepted by each of these parameters and the configuration interfaces (snapshots) with examples have been documented in the CN section of this activity.

Figure 1 indicates a broad picture on the secure and unsecured communication between the CBM and the OSS. If IPSec communication is enabled between the OSS and the CBM, then the communication channel would be secure.

[2] **Warning :** This static file contains confidential information (related to the preshared key) and should be removed from the machine once its no longer needed.

Note: IPSec is used to provide additional security between OSS and CBM and is not meant to replace the use of standard secure protocols such as SSH, SFTP or HTTPS.

Figure 1 : Functional Layout



1.2 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced by this feature

1.3 Software Requirements or Dependencies

SN09 or later SSPFS load (with NTIpSec package) for the CBM.

The OSS should support IPSec for secure communication.

1.4 Limitations and restrictions

This activity only supports IPSec in Transport Mode.

IPSec Tunnel mode configuration would not be supported as part of this activity.

1.4.1 Security

For secure communication, all security parameters provisioned on the OSS must match with security parameters provisioned on the CBM.

1.4.2 IP Addresses

Only IPv4 (32 bit) addresses will be supported

1.4.3 Keys

Only Preshared keys would be used for IKE communication.

1.4.4 Test Strategy

- The OSS which would be tested in this activity would be a solaris 9 machine.

1.4.5 HA system key negotiation

IPSec or IKE SA's will not be replicated on HA CBM's. There would be loss of communication for inbound connections (from OSS to CBM) post CBM fail-over, until the existing IPSec SA's expire and IPSec SA's get re-negotiated.

This issue could become prevelant again if the OSS is an HA platform and it fails over.

1.5 IPSec Precedence Order

When there are numerous IPSec policy entries in the IPSec configuration file, the system could resort to reordering of the policy entries or attach precedence to some rules defined in the IPSec configuration files. This can happen in the following conditions.

If the new policy entry has been defined with action bypass ("action" attribute can take in values drop, ipsec and bypass), then this entry would be attached the highest precedence. If there are more than one bypass entries, the system would match all the bypass entries before matching any other entries.

If there are IPSec configuration entries with matching entries for the input and output datagrams, then the first such kind of a match would be taken.

In case of matching entries for input and output datagrams, the policy entries would be reordered (adding the new entry before the old entry) if the new policy entry has a higher level of protection strength than the old entry.

The strength of the policy entries would be defined as

AH and ESP > ESP > AH

Entries with both the AH and ESP present in the policy entry would be ordered before entries with AH-only and ESP-only entries.

For other entries, the order specified by the user would not be modified, newer entries are added at the end of all the old entries.

A new entry is considered duplicate of the old entry if an old entry matches the same traffic pattern as the new entry.

1.6 Interactions

None

1.7 Glossary

Term	Description
AH	Authentication Header
CBM	Core and Billing Manager
CLI	Command Line Interface (config tool on SSPFS)
ESP	Encapsulated Security Payload
IP	Internet Protocol
IPSec	Internet Protocol Security
IKE	Internet Key Exchange
IPv4	Internet Protocol Version 4
OSS	Operations Support System
SA	Security Association
SSPFS	Succession Server Platform Foundation Software
SSH	Secure Shell
SFTP	Secure File Transfer Protocol

1.8 Appendix A for A00009840

This interface would generate configuration information for configuring IPSec on the downstream (for Solaris box). This information would be made available on the CBM in the /etc/inet/remotesystem/solaris directory as static file. The downstream would require to be manually modified to reflect this configuration information. Following section provides snippets of downstream configuration files.

1.8.1 Sample IPSec downstream configuration file (downstream.ipsec)

The following new rule should be added into the ipsecinit.conf file on the downstream in the similar format. This file is available in the directory /etc/inet and this instruction is applicable only for a solaris (sspfs) box

{ laddr 47.135.214.62 raddr 47.135.214.130 dir both } ipsec { encr_auth_algs sha1 encr_algs 3des auth_algs sha1 }

1.8.2 Sample IKE downstream configuration file (downstream.ike)

The following rule below needs to be added into IKE config file on the downstream in the similar format. This file is available in the directory /etc/inet/ike and the file to be updated with the below changes is config. This instruction is applicable only for a solaris (sspfs) box.

{

label Newrule

remote_addr 47.135.214.130

local_addr 47.135.214.62

p2_pfs 2

p2_lifetime_secs 400

p1_xform { oakley_group 2 auth_method preshared encr_alg 3des auth_alg sha1 p1_lifetime_secs 400 }

}

The following key information should be updated on the file ike.preshared in the directory /etc/inet/secret on the downstream. This instruction is applicable only for a solaris (sspfs) box. This key information should be matching with the above added IKE rule

{

localidtype IP

localid 47.135.214.62

remoteidtype IP

remoteid 47.135.214.130

key 12333895734895abc23489237489723

}

2: Configuration for A00009840

2.1 Hardware and Software Requirements

SN09 or later SSFPS load (with NTIpSec package) for the CBM.

OSS supporting IPSec communication.

2.2 Initial Configuration

2.2.1 Security

Following are the high-level steps to enable security between OSS and the CBM.

- Load the CBM with SN09 or later version of SSPFS
- After logging into the CBM, the craftsperson will then invoke the CLI tool available as part of SSPFS and proceed to the option of configuring the IPSec/IKE parameters with the OSS details.
  - The user should not log from the target OSS machine onto the CBM to perform the IPSec/IKE configuration.
- Enable security on the OSS to secure the connection from OSS to the CBM

2.2.2 OSS

IPSec and IKE configuration parameters which are provisioned on the OSS must match the corresponding parameters on the CBM provisioned through the configuration interface bundled under the CLI tool.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable

2.4 Upgrade Considerations

Not Applicable

2.5 Data schema (DS) (CM, MIBS, RDB)

Not Applicable

2.6 Service Orders (SO) (CM & SESM)

Not Applicable

2.7 Software optionality control (SOC)

Not Applicable

2.8 Element Management

2.8.1 New/modified GUI

Not Applicable

2.8.2 GUI information

Not Applicable

2.8.3 CLUI Interface

This interface is bundled into CLI tool available as part of SSFPS.

This interface will be accessible from “IP configuration” menu entry available in the list of Configuration options. The following figure (Figure 1) indicates the sequence of menu options navigated in reaching the IPSec/IKE configuration interface.

Figure 1 : CLI Menu Options

```
Command Line Interface
 1 - View
 2 - Configuration
 3 - Other

 X - exit

select - 2

Configuration
 1 - NTP Configuration
 2 - Apache Proxy Configuration
 3 - DCE Configuration
 4 - OAMP Application Configuration
 5 - CORBA Configuration
 6 - IP Configuration
 7 - DNS Configuration
 8 - Syslog Configuration
 9 - Database Configuration
10 - NFS Configuration
11 - Bootp Configuration
12 - Restricted Shell Configuration
13 - Security Services Configuration
14 - Login Session
15 - Location Configuration
16 - Cluster Configuration
17 - Succession Element Configuration
18 - snmp_poller (SNMP Poller Configuration)
19 - backup_config (Backup Configuration)

select - 6

IP Configuration
 1 - config_router (Configure Default Router and Netmask)
 2 - config_data (Configure System Data IP Addresses)
 3 - ipsecike_config (Configure IPSec/IKE Rules)

 X - exit

select - 3

 X - exit
```

2.8.3.1 Functional Description

Figure 2 indicates the screen snapshot when the IPSec/IKE configuration interface menu option is exercised from the list of options displayed in the IP Configuration menu (option 3 as indicated in Figure 1).

Figure 2 : IPSec/IKE Configuration Interface

```
IPSec/IKE Configuration Menu
 1 - IPSec Configuration
 2 - IKE Configuration

 X - Exit

 Select -
```

2.8.3.2 CLUI usage and implications

This activity provides an easy to use IPSec configuration interface on the CBM for configuring IPSec/IKE parameters.

Initially, IPSec entries are created by entering the necessary parameters. If the craftsperson has chosen to use “ipsec” action,the next step would be to create a corresponding IKE entry using the necessary parameters.

2.8.3.3 IPSec configuration interface

The following figure (Figure 3) lists the screen snapshot when IPSec configuration option is chosen from the IPSec/IKE configuration menu initially displayed.

Figure 3 : IPSec Configuration Interface

```
IPSec Configuration Menu
 1  -  Add IPSec entry
 2  -  Delete IPSec entry
 3  -  List All IPSec entries

 X  -  Exit

Select -
```

2.8.3.3.1 IPSec fields

The following table lists the parameters which would accepted by the interface and the valid options for each of these parameters.

Table 1 : IPSec field descriptions

Field	Entry	Explanation and Action
Remote Address	A numeric internet IP address of the form : www.xxx.yyy.zzz	Source address on incoming packets and destination address on outgoing packets
Remote Port	1-65535,all	IP port of the remote system communicating with the server
Local Address[a]	A numeric internet IP address of the form : www.xxx.yyy.zzz	Destination address on incoming packets and source address on outgoing packets
Local Port	1-65535, all	IP Port of this server
Upper Layer Protocol	any, udp,tcp and icmp	Determines which protocol traffic this entry is matched against
Direction	in, out and both	Determines whether this entry is for inbound or outbound traffic
Action	bypass,drop and ipsec	Determines the action to be taken when the traffic pattern is matched
ESP Encryption	none, any, NULL, DES, 3DES	Encryption Algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”

Table 1 : IPSec field descriptions

Field	Entry	Explanation and Action
ESP Authenticaion	none,any, SHA1, MD5	Authentication Algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”
AH Authentication	none,any, SHA1, MD5	Authentication algorithm that will be used to apply the IPSec AH protocol to outbound datagrams and verify it to be present on inbound datagrams, Only valid when action is set to “ipsec”

a. The Local Address would be cluster IP address if the system is a HA configuration. If the system is having a simplex configuration, the local address would be the address of this node.

2.8.3.3.2 IPSec Add Entry Example

The following figure (Figure 4) shows screen snapshot for IPSec Add entry option.

Figure 4 : IPSec adding a new rule

```
Enter the Remote IP Address   : 47.135.214.62
Enter the Remote Port No [1-65535,all] : all
Enter the Local IP Address [47.135.214.127] :
Enter the Local Port No [1-65535,all] : all
Enter the Upper Layer Protocol [any,udp,tcp,icmp] : any
Enter the Direction [in,out,both] : both
Enter the Action [ipsec,drop,bypass] : ipsec
Enter the ESP Header
  Authentication Algorithm [md5,sha1,none,any] : sha1
  Encryption Algorithm [none,NULL,des,3des,aes,blowfish] : 3des
Enter the AH Header
  Authentication Algorithm [md5,sha1,none,any] : md5
```

The following figure (Figure 5) captures the screen snapshot of the confirmation prompt for IPSec add entry screen.

Figure 5 : IPSec add entry confirmation screen

Do you wish to add the following IPSec configuration Information

Remote IP Address : 47.135.214.62
Remote Port No. : all
Local IP Address : 47.135.214.127
Local Port No. : all
Upper Layer Protocol : any
Direction : both
Action : ipsec
ESP Encryption Algorithm : 3des
ESP Authentication Algorithm : sha1
AH Authentication Algorithm : md5

Select [save, edit, abort] -

The following figure (Figure 6) captures the screen snapshot when the values entered for a new IPSec rule through add option is being edited before committing to the database.

Figure 6 : IPSec Add entry - Edit option

```
Press ENTER to continue with the current option

Remote IP Address [47.135.214.62] :
Remote Port No. [all] :
Local IP Address [47.135.214.127] :
Local Port No. [all] :
Upper Layer Protocol [any] :
Direction [both] :
Action [ipsec] :
ESP Encryption Algorithm [3des] :
ESP Authentication Algorithm [sha1] : md5
AH Authentication Algorithm [md5] : sha1

Do you wish to add the following IPSec configuration Information

Remote IP Address              : 47.135.214.62
Remote Port No.                : all
Local IP Address               : 47.135.214.127
Local Port No.                 : all
Upper Layer Protocol           : any
Direction                      : both
Action                         : ipsec
ESP Encryption Algorithm       : 3des
ESP Authentication Algorithm : md5
AH Authentication Algorithm  : sha1

 Select [save, edit, abort] -  save

Configuration successfully completed

For downstream configuration refer to instructions placed
in downstream.ipsec file in /etc/inet/remotesystem/solaris directory
```

2.8.3.3.3 IPSec List Entry Example

The following figure (Figure 7) shows screen snapshot when the list option is exercised.

The rules will be listed in the order in which they are listed in the IPSec configuration file (ipsecinit.conf).

Figure 7 : IPSec List Entry Output

```
--------------------------------------------------------------------------------
indexID      raddr          laddr             lport    rport    dir  status
--------------------------------------------------------------------------------
 1       47.135.214.62  47.135.214.127  all      all      both  up
 2       47.135.214.63  47.135.214.127  all      all      both  down


Enter the indexID of rule to be detailed (x to exit) - 2

Remote IP Address              : 47.135.214.63
Remote Port No.                : all
Local IP Address               : 47.135.214.127
Local Port No.                 : all
Direction                      : both
Action                         : ipsec
ESP Encryption Algorithm       : 3des
ESP Authentication Algorithm : sha1
AH Authentication Algorithm  : sha1

Enter the indexID of rule to be detailed (x to exit) -
```

2.8.3.3.4 IPSec Delete Entry Example

The following figure (Figure 8) shows screen snapshot when the delete option is exercised from IPSec configuration interface.

Figure 8 : IPSec Delete Entry Output

```
-------------------------------------------------------------------------------
indexID     raddr          laddr          lport    rport    dir  status
-------------------------------------------------------------------------------
 1      47.135.214.127  47.135.214.62   all      all      both  up
 2      47.135.214.130  47.135.214.62   all      all      both  down

 Enter the indexID of rule to be deleted (x to exit) - 2

Remote IP Address              : 47.135.214.130
Remote Port No.                : all
Local IP Address               : 47.135.214.62
Local Port No.                 : all
Direction                      : both
Action                         : ipsec
ESP Encryption Algorithm       : 3des
ESP Authentication Algorithm : sha1
AH Authentication Algorithm  : sha1

Do you wish to delete the above ipsec rule
Select [Yes, No, Exit(x)] :
```

2.8.3.4 IKE Configuration Interface

The following figure (Figure 9) lists the screen snapshot when IKE configuration option is chosen from the IPSec/IKE configuration menu initially displayed.

Figure 9 : IKE Configuration Interface

```
IKE Configuration Menu
 1  -  Add IKE entry
 2  -  Delete IKE entry
 3  -  List IKE entries
 4  -  Change Preshared key for IKE entry

 X  -  Exit

Select -
```

2.8.3.4.1 IKE Fields

The following table lists the parameters which would accepted by the interface and the valid options for each of these parameters.

Table 2 IKE Field Descriptions

Field	Entry	Explanation and Action
Remote Address	A numeric internet IP address of the form : www.xxx.yyy.zzz	IP Address of the remote system cmmunicating with this server
Local Address	A numeric internet IP address of the form : www.xxx.yyy.zzz	IP Address of this server
Oakley Group	1 (768 bit), 2 (1024 bit) or 5 (1536 bit)	The Oakley Diffie-Hellman group used for IKE Security Association key derivation
Authentication Method	Preshared	Authentication method used for IKE phase 1.
Encryption	DES, 3DES	Specifies the encryption algorithm for a security association
Authentication	SHA1, MD5	Specifies the authentication algorithm for a security association
PFS Group ID	0 (do not use Perfect Forward Secrecy for IPSec SAs), 1(768 bit), 2(1024 bit),5(1536 bit)	Oakley Diffie-Hellman group used for IPSec Security Association key derivation
Preshared Key File	String (file name with full path)	Specifies the file with complete path which would contain the preshared key. This file would contain the preshared key for this Security Association.

Table 2 IKE Field Descriptions

Field	Entry	Explanation and Action
IKE Lifetime	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days	Specifies the lifetime for an IKE phase 1 Security Association
IPSec Lifetime	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days	Specifies the lifetime for an IPSec Security Association

2.8.3.4.2 IKE Add Entry Example

The following figure (Figure 10) shows screen snapshot for IKE Add entry option.

Figure 10 : IKE adding a new rule

```
Enter the Remote IP Address : 47.135.214.62
Enter the Local IP Address [47.135.214.127] :
Enter the Oakley Group [1,2,5] : 2
Enter the Authentication Method [preshared] : preshared
Enter the Encryption Algorithm [des, 3des] : 3des
Enter the Authencation Algorithm [md5, sha1] : sha1
Enter the PFS Group ID [0,1,2,5] : 0
Enter the IKE Lifetime value : 14400
Enter the IKE Lifetime unit [secs,min,hrs] : secs
Enter the IPSec Lifetime Value : 14400
Enter the IPSec Lifetime unit [secs,min,hrs] : secs
Enter the IKE Preshared Key file location (full path) : /tmp/arun1
```

The following figure (Figure 11) captures the screen snapshot of the confirmation prompt for IKE add entry screen.

Figure 11 : IKE add entry confirmation screen

Do you wish to add the following IKE configuration Information

Remote IP Address : 47.135.214.62
Local IP Address : 47.135.214.127
Oakley Group : 2
Authentication Method : preshared
Encryption Algorithm : 3des
Authentication Algorithm : sha1
PFS Group ID : 0
IKE Lifetime : 14400
IKE Lifetime unit : secs
IPSec Lifetime : 14400
IPSec Lifetime unit : secs
IKE preshared key Location : /tmp/arun1

Select [save, edit, abort] - save

Configuration successfully completed

For downstream configuration refer to instructions placed
in downstream.ike file in /etc/inet/remotesystem/solaris directory

The following figure (Figure 12) captures the screen snapshot when the values entered for a new IKE entry through add option is being edited before committing to the database.

Figure 12 : IKE Add entry - Edit option

```
Press ENTER to continue with the current option
Remote IP Address [47.135.214.63] :
Local IP Address [47.135.214.127] :
Oakley Group [2] :
Authentication Method [preshared] :
Encryption Algorithm [3des] :
Authentication Algorithm [sha1] :
PFS Group ID [0] :
IKE Lifetime value [400] :
IKE Lifetime Unit [secs] :
IPSec Lifetime Value [400] : 800
IPSec Lifetime Unit [secs] : secs
IKE Preshared key File location [/tmp/arun1] :

Do you wish to add the following IKE configuration Information

Remote IP Address            : 47.135.214.63
Local IP Address             : 47.135.214.127
Oakley Group                 : 2
Authentication Method        : preshared
Encryption Algorithm         : 3des
Authentication Algorithm     : sha1
PFS Group ID                 : 0
IKE Lifetime                 : 400
IKE Lifetime unit            : secs
IPSec Lifetime               : 800
IPSec Lifetime unit          : secs
IKE preshared key Location   : /tmp/arun1

 Select [save, edit, abort] -  save

Configuration successfully completed

For downstream configuration refer to instructions placed
in downstream.ike file in /etc/inet/remotesystem/solaris directory
```

2.8.3.4.3 IKE List Entry Example

The following figure (Figure 13) shows screen snapshot when the list option is exercised from the IKE configuration interface menu.

Figure 13 : IKE List Entry Output

```
-------------------------------------------------------
 indexID       raddr            laddr
-------------------------------------------------------
  1         47.135.214.62      47.135.214.127
  2         47.135.214.63      47.135.214.127


 Enter the indexID of rule to be detailed (x to exit) - 2

Remote IP Address          : 47.135.214.63
Local IP Address           : 47.135.214.127
Oakley Group               : 2
Authentication Method      : preshared
Encryption Algorithm       : 3des
Authentication Algorithm   : sha1
PFS Group ID               : 0
IKE Lifetime               : 400
IPSec Lifetime             : 800
IKE preshared key          : ********

 Enter the indexID of rule to be detailed (x to exit) -
```

2.8.3.4.4 IKE Delete Entry Example

The following figure (Figure 14) shows screen snapshot when the delete option is exercised from the IKE configuration interface menu.

Figure 14 : IKE Delete Entry Output

```
-------------------------------------------------------
indexID       raddr            laddr
-------------------------------------------------------
 1         47.135.214.62      47.135.214.127
 2         47.135.214.63      47.135.214.127


 Enter the indexID of rule to be deleted (x to exit) - 2

Remote IP Address          : 47.135.214.63
Local IP Address           : 47.135.214.127
Oakley Group               : 2
Authentication Method      : preshared
Encryption Algorithm       : 3des
Authentication Algorithm   : sha1
PFS Group ID               : 0
IKE Lifetime               : 400
IPSec Lifetime             : 800
IKE preshared key          : ********

Do you wish to delete the above ike rule
Select [Yes, No, Exit(x)] :
```

2.8.3.4.5 IKE Change Key Entry Example

The following figure (Figure 15) shows screen snapshot when the change key option is exercised from the IKE configuration interface menu.

Figure 15 : IKE Change Key Output

```
-------------------------------------------------------
indexID       raddr            laddr
-------------------------------------------------------
 1        47.135.214.62      47.135.214.127
 2        47.135.214.63      47.135.214.127

 Enter the indexID of rule whose key is to be changed (x to exit) - 2

Remote IP Address          : 47.135.214.63
Local IP Address           : 47.135.214.127
Oakley Group               : 2
Authentication Method      : preshared
Encryption Algorithm       : 3des
Authentication Algorithm   : sha1
PFS Group ID               : 0
IKE Lifetime               : 400
IPSec Lifetime             : 800
IKE preshared key          : ********
Do you wish to change key for above IKE rule
Select [Yes, No, Exit (x)] - yes


 Enter the preshared key file location (full path) : /tmp/arun2


Do you with to change key to the above
Select [Yes, No, Exit(x)] - yes

Configuration successfully completed

 Enter the indexID of rule whose key is to be changed (x to exit) -
```

2.8.3.5 OSS parameter settings

- The IPSec and IKE specific entries which needs to be configured at the downstream would be put into files (downstream.ipsec & downstream.ike) on the SSPFS box in /etc/inet/remotesystem/solaris directory
- Appropriate instructions would be provided as part of the interface to read from the static files so created, for configuring IPSec on the downstream

- The configuration information for the downstream machine would be limited to Solaris in this release.

Note : This static file contains confidential information (related to preshared key) and should be removed from the machine once its no longer needed.

2.8.3.6 CLUI release history update

Initial Availability

2.8.3.7 Supplementary Information

None

2.9 User interface changes

Not Applicable

2.10 OSSGate Interface Changes

Not Applicable

2.11 Security

2.11.1 Network configuration

None

2.11.2 Key management

Preshared keys would be used for IKE communication.

The IKE preshared key would be entered by the user as part of the IPSec/IKE configuration interface. Solaris stores all keys in a hidden system file not accessible by common users but is available to the root user.

2.11.3 Protocol

IPsec is being used on the solaris machine.

2.11.4 Authentication

Not Applicable

2.12 Configuration Walkthrough

2.12.1 CBM

Following lists the steps which needs to be carried out on the CBM.

The user should not log from target OSS machine onto the CBM to perform the IPSec/IKE configuration.

- Load the CBM with SN09 or later version of SSPFS
- Login as root into the CBM.

- Launch the CLI tool
- Select the IPSec/IKE Configuration option from the list of options listed by the CLI tool (available only as root user).
- In the IPSec/IKE Configuration menu, select the IPSec configuration option to add IPSec rules.
- Using the IKE configuration option in IPSec/IKE Configuration menu, add IKE rules.
- Exit the CLI tool.

2.12.2 OSS

- Make appropriate modifications to the configuration files on the downstream for enabling IPSec communication.

Note : This interface would generate configuration information for configuring IPSec on the downstream (for Sun and Linux boxes). This information would be make available on the CBM in the /tmp directory as static file. The downstream would require to be manually modified to reflect this configuration information.

2.13 Glossary

Term	Description
AH	Authentication Header
CBM	Core and Billing Manager
CLI	Command Line Interface (config tool of SSPFS)
IP	Internet Protocol
IPSec	Internet Protocol Security
ICMP	Internet Control Message Protocol
IKE	Internet Key Exchange
OSS	Operations Support System
PFS	Perfect Forward Secrecy
SA	Security Association
SSPFS	Succession Server Platform Foundation Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Product = CS 2000

A00009893 -- Session Server Call Processing Overload

Functional Description

1: Applicable Solution(s)

PT-IP, PT-AAL2

1.1 Description

This feature provides enhancements to the Session Server SIP Gateway Application overload functionality that was introduced by the SN08 feature A00007270, Session Server Call Processing Overload.

A00007270 used an overload detection scheme that was based solely on the depth of two call processing messaging queues - the Generic Control Protocol (GCP) queue used for CS2K-originated calls and the Session Initiation Protocol (SIP) queue used for remote SIP server- originated calls. If either queue was determined to be above its threshold at the end of a sampling period (defined as the collection of five samples from each queue, one every two seconds), the application was put into an overload state.

Once the application was in overload, all new incoming calls received from a remote SIP server were rejected. This call rejection continued until the results of a subsequent sample period indicated the queue sizes had decreased below the overload threshold.

A few areas of note regarding SN08 application overload detection:

- The amount of work being done by the CPU (the CPU occupancy) was not a factor in determining whether the application was in overload.
- When the application was in overload, all new remote SIP server calls were rejected. There was no throttling mechanism that would have allowed some new SIP calls to continue to be processed while the application attempted to come out of overload.
- Since only new remote calls were rejected, a server that handled a higher proportion of local originations (i.e., calls from a CS2K) got little or possibly no overload relief using the SN08 overload handling mechanism.

An overview of the new functionality provided by this feature for SN09:

- For **Overload Detection**, CPU occupancy is now a factor in the algorithm for determining overload.
- For **Flow Control**, instead of blocking all new SIP originations during overload, new calls - both CS2K-originated and remote SIP

server-originated - will be throttled to allow a certain percentage of both call types to complete.

- **Babbling Node Detection** - Provides the ability to detect and limit the impact of a remote SIP server that is sending an excessive number of bad messages to the Session Server.
- **Overload Monitoring and Fault Management** - New OMs, logs and alarms are created for the purpose of providing information regarding CPU occupancy, queue sizes and percentage of calls that are being rejected.

1.1.1 Overload Detection

For SN09, the overload sampling period remains unchanged. In addition to getting samples of each of the call processing queue sizes every two seconds, the CPU occupancy is also checked at the same time. After five samples of each have been collected, the SIP Gateway Application is considered to be in overload if at least **one** of the following conditions exists:

- CPU occupancy value is 90% or greater
- GCP queue length exceeds its overload threshold
- SIP queue length exceeds its overload threshold

If the application is found to be in overload, a major alarm is generated along with a SIPC310 log (SN08 functionality).

The application can also be in a pending overload state, meaning it is either approaching overload or possibly receding from an earlier overload condition. Parameters for the pending state are:

- CPU occupancy value is 85% or greater
- GCP queue length exceeds its pending threshold
- SIP queue length exceeds its pending threshold

There are no changes to call processing while in the pending state, unless the application is in the early stages of recovering from overload. In the latter case, some calls may still be getting rejected. This is discussed in more detail in the Flow Control section.

As in SN08, when the application is in pending overload, a minor alarm is generated, along with a SIPC310 log.

1.1.2 Flow control

Once the application has entered the overload state, new call originations are throttled as a means of easing the load on the CPU. The level of throttling is determined by the Flow Control Rate (FCR). FCR is analogous to the percentage of new calls allowed to complete while the application is in this condition. This percentage is applied to both local (CS2K-originated) and

remote (SIP-originated) calls. In other words, if the FCR is 90, 90% of new local calls and 90% of new remote calls are allowed, or every 10th call of each type is rejected. Calls in progress are not affected in any way.

When the system enters overload, an initial FCR of 90 is applied. It can fluctuate between 0 (all calls blocked) and 100 (no calls blocked), increasing or decreasing in increments of 10, based on the current overload state.

For each sample period that the application remains in overload, the FCR is decreased by 10, causing additional calls to be blocked (down to 0% - all calls blocked).

If conditions improve and a sampling period indicates the application is no longer in overload, the FCR is not immediately returned to 100%. Instead, a gradual increase of 10% each period is done to ensure the system does not bounce back into overload.

For call rejection, a Local Release with Cause Value of 42 is sent for GCP originations and a 503 Service Unavailable is sent for SIP originations.

In SN08, when the SIP Gateway application was in overload it responded to a SIP OPTIONS request with a 503 Service Unavailable response. The purpose of this was to indicate to the remote server that the Session Server was no longer accepting any new calls. If the far end reacted appropriately to this response, it would stop sending new calls to the overloaded Session Server.

With the changes in this feature that now allows for a certain percentage of calls to complete during overload, the 503 response will no longer be sent in response to an OPTIONS request when the application is in overload.

1.1.3 Babbling Node Detection and Isolation

This component provides the ability to detect and limit the impact of a remote SIP server IP address that is flooding the Session Server with an excessive number of bad syntax messages. Once an IP address is labeled as a babbling node, lower level software intercepts all messages from the node before they reach the application, thereby freeing the application from the time it would have to spend processing each message.

Babbling node detection involves keeping a count of the number of SIP messages with bad syntax received from an IP address. Every 5 seconds, this counter is scanned for each IP address. If 20 new bad messages have been received from an IP since the last check, the address is removed from service in such a way that no further messages from this IP are processed by the application.

Note that in order to determine the source (the remote SIP server) of a bad syntax message, the Session Server must at a minimum be able to parse the SIP

via header. If the via header is too corrupted for parsing, the message will not be uncounted as a bad syntax message.

Babbling node isolation is implemented by using the Linux iptables functionality. When a node is determined to be babbling it is marked in iptables in such a way that all messages from the IP will be discarded. No responses are sent to the remote node. In the session server, the connection status of the remote SIP server is marked inactive and all access links mapped to the server are removed from service. Corresponding trunks in the CS2K are put into a SYS state. This effectively disables all incoming and outgoing calls from the server.

After the IP has been disabled for 5 minutes, its status in the iptables is changed so that its messages are no longer dropped and the associated access links/trunks are brought back into service. The same criteria are again used to detect and isolate the IP if it continues to send an excessive amount of SIP messages with syntax errors.

1.1.4 Overload Monitoring and Fault Management

As a means of providing the ability to monitor overload-related events and statistics, new Operational Measurements, logs and alarms are created by this activity.

A new OM group, SIPGW_OVERLOAD, contains information related to the level of usage for each of the monitored resources (CPU, GCP queue, SIP queue). The following types of registers are in the group:

- CPU occupancy calculation from the latest sampling period
- GCP queue size from the latest sampling period
- Radvision queue size from the latest sampling period
- High water marks for each resource over a 30 minute period. Reset to 0 every 30 minutes.

Below is a sample output of the new OM group SIPGW_OVERLOAD:

```
Active Register Counts
START Thu Feb 10 10:30:00 2005   STOP Thu Feb 10 10:31:44 2005

OMGROUP: SIPGW_OVERLOAD
*************************************************************

TUPLE KEY: 0            TUPLE KEY NAME:

Register Name                          Value
-------------------------------       ----------
CPU_OCCUPANCY                              45
CPU_OCCUPANCY_HWM                          67
GCP_QUEUE_SIZE                             15
GCP_QUEUE_SIZE_HWM                         29
SIP_QUEUE_SIZE                             25
```

```
SIP_QUEUE_SIZE_HWM                              30
*****************************************************************
```

In addition to the OMs, two new STGW700 logs are added to cover various scenarios:

- Changes in the Flow Control Rate. Note that this log can be generated when the application is not in overload, such as when it is still recovering from an earlier overload state.
- When an IP address is either removed from or re-added to the Access Control List as a result of babbling node isolation.

Per existing functionality, a minor alarm is raised when the application is in a pending overload state and a major alarm when in overload. These remain unchanged. This feature adds three new alarms and associated STGW700 logs to indicate that certain CPU occupancy levels have been reached:

- minor = 80% CPU occupancy
- major = 85% CPU occupancy
- critical = 90% CPU occupancy

Note the minor and major CPU alarms can be activated even if the application is not in overload.

Here are examples of the new logs:

```
Mar 16 12:46:20 pnc1y0jp sipgwyappln: STGW700 NONE INFO SIPOVLD FCR Change OLD
FCR: 90 NEW FCR: 80

Mar 16 22:58:02 pnc1y0jp sipgwyappln: STGW700 NONE INFO SIPOVLD Babbling node
timeout, RTPFMGC 47.142.123.48 IP enabled

Mar 16 22:58:37 pnc1y0jp sipgwyappln: STGW700 NONE INFO SIPOVLD Babbling node
detected, RTPFMGC 172.16.80.24 IP disabled

Mar 16 22:59:33 pnc1y0jp sipgwyappln: STGW700 NONE INFO SIPOVLD All babbling node
IPs re-enabled due to initialization

Mar 16 12:46:10 pnc1y0jp alarmd: STGW700 CRIT TBL  SIPOVLD NCGL=pnc1y0jp;SIPC CPU
occupancy critical alarm

Mar 16 12:17:42 pnc1y0jp alarmd: STGW700 NONE TBL  SIPOVLD NCGL=pnc1y0jp;SIPC CPU
occupancy major alarm cleared
```

1.2 Hardware Requirements or Dependencies

No new hardware requirements or dependencies.

1.3 Software Requirements or Dependencies

No new software requirements of dependencies.

1.4 Limitations and restrictions

In addition to the normal, 5 minute timeout, disabled babbling nodes are re-enabled in the following situations:

- When Remote SIP Server configuration data is changed in the Session Server.
- When the Session Server is suspended. Upon unsuspension the IP will be enabled.
- When the Session Server switches activity to the other unit.

In order to count the number of bad syntax messages received from a remote SIP server, the Session Server must be able to parse the SIP via header in the offending message to determine the sender of the message. Without the source IP address, the bad message cannot be counted against a server.

1.5 Interactions

In SN09, the 503 response will no longer be sent in response to an OPTIONS request when the application is in overload.

When Access Control List (ACL) functionality is activated, babbling node message discarding using iptables takes precedence over the ACL iptables setting. In other words, if the ACL iptables setting allows messages from an IP to be received, but the node was found to be babbling, all messages from the IP will be discarded until the babbling node timeout. At that point, the ACL setting determines what to do with messages from the IP.

1.6 Glossary

Term	Description
ACL	**Access Control List** - the list of allowable IP addresses from which the Session Server can receive messages.
FCR	**Flow Control Rate** - the percentage of new call originations allowed while in overload or during the recovery period when the application is coming out of overload.
GCP	**Generic Control Protocol** - call control protocol used between the gateway controller and the session Server.
SIP	**Session Initiation Protocol** - an application-layer protocol for creating, modifying and terminating sessions with one or more participants.

2: Fault Management for A00009893

2.1 Fault management strategy

To provide notification of SIP Gateway application overload-related events on the Session Server, new logs and alarms are created by this activity.

2.2 Fault management tools and utilities

2.2.1 Faults, Alarms and Logs

New STGW700 logs are added to cover various scenarios:

- Generated when the Flow Control Rate changes. Note that this log can be generated when the application is not in overload, such as when it is still recovering from an earlier overload state.
- Generated when an IP address is either removed from or re-added to the Access Control List as a result of babbling node isolation.

This feature also adds three new alarms and associated STGW700 logs to indicate that certain CPU occupancy levels have been reached:

- minor = 80% CPU occupancy
- major = 85% CPU occupancy
- critical = 90% CPU occupancy

2.3 STGW700 SIP Gateway Application FCR Change Log

2.3.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	NONE
Event Type	INFO
Label	SIPOVLD
Component ID	SIPC
Description	FCR Change OLD FCR: <0-100> NEW FCR: <0-100>

2.3.2 Action

None.

2.3.3 Associated Operational Measurements or Performance Measurements

OM group SIPGW_OVERLOAD

2.3.4 Additional information

2.4 STGW700 Babbling node detected log

2.4.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	NONE
Event Type	INFO
Label	SIPOVLD
Component ID	SIPC
Description	Babbling node detected, <server name> <IP addresss> IP disabled

2.4.2 Action

None

2.4.3 Associated Operational Measurements or Performance Measurements

None

2.4.4 Additional information

2.5 STGW700 Babbling node timeout Log

2.5.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	NONE
Event Type	INFO
Label	SIPOVLD
Component ID	SIPC
Description	Babbling node timeout, <server name> <IP addresss> IP enabled

2.5.2 Action

None

2.5.3 Associated Operational Measurements or Performance Measurements

None

2.5.4 Additional information

2.6 STGW700 Babbling node initialization Log

2.6.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	NONE
Event Type	INFO
Label	SIPOVLD
Component ID	SIPC
Description	All babbling node IPs re-enabled due to initialization

2.6.2 Action

None

2.6.3 Associated Operational Measurements or Performance Measurements

None

2.6.4 Additional information

2.7 STGW700 CPU occupancy critical alarm Log

2.7.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	CRITICAL
Event Type	TBL
Label	SIPOVLD
Component ID	SIPC
Description	CPU occupancy critical alarm

2.7.2 Action

None

2.7.3 Associated Operational Measurements or Performance Measurements

OM group SIPGW_OVERLOAD

2.7.4 Additional information

2.8 STGW700 CPU occupancy major alarm Log

2.8.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	MAJOR
Event Type	TBL
Label	SIPOVLD
Component ID	SIPC
Description	CPU occupancy major alarm

2.8.2 Action

None

2.8.3 Associated Operational Measurements or Performance Measurements

OM group SIPGW_OVERLOAD

2.8.4 Additional information

2.9 STGW700 CPU occupancy minor alarm Log

2.9.1 Formats

Report Name	STGW
Report Number	700
Alarm Level	MINOR
Event Type	TBL
Label	SIPOVLD
Component ID	SIPC
Description	CPU occupancy minor alarm

2.9.2 Action

None

2.9.3 Associated Operational Measurements or Performance Measurements

OM group SIPGW_OVERLOAD

2.9.4 Additional information

2.10 Alarms

2.10.1 CPU Occupancy Critical

This alarm is generated when the CPU occupancy reaches 90%.

Table 3: NGSS Alarm GUI Field descriptions

Field	Value
Severity	Critical
Category	Quality of Service Alarm
Description	CPU Occupancy 90% or above
LogName	STGW
LogNumber	700
EventType	TBL
EventLabel	SIPOVLD

Table 3: NGSS Alarm GUI Field descriptions

Field	Value
ProbableCause	No Probable Cause

2.10.2 CPU Occupancy Major

This alarm is generated when the CPU occupancy reaches 85%

Table 4: NGSS Alarm GUI Field descriptions

Field	Value
Severity	Major
Category	Quality of Service Alarm
Description	CPU Occupancy at 85%
LogName	STGW
LogNumber	700
EventType	TBL
EventLabel	SIPOVLD
ProbableCause	No Probable Cause

2.10.3 CPU Occupancy Minor

This alarm is generated when the CPU occupancy reaches 80%.

Table 5: NGSS Alarm GUI Field descriptions

Field	Value
Severity	Minor
Category	Quality of Service Alarm
Description	CPU Occupancy at 80%
LogName	STGW
LogNumber	700
EventType	TBL
EventLabel	SIPOVLD
ProbableCause	No Probable Cause

2.11 Related documentation

3: Performance Management for A00009893

3.1 Performance management strategy

OM group SIPGW_OVERLOAD is added to the Session Server to provide statistics related to the resources that are monitored to determine whether the SIP Gateway application is in overload.

3.2 Performance Measurements (PM), Operational Measurements (OM), and stats

3.2.1 PM, OM, and stats format

Component: SIPGW_OVERLOAD

Performance measurement name: CPU_OCCUPANCY

Performance measurement description: The value calculated for the amount of time the CPU spent performing work as a percentage to its total running time over the last sampling period (10 seconds).

History: created in SN09

Performance Value Range: 0 - 100

Collection Interval: 10 seconds

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 Bytes

Component: SIPGW_OVERLOAD

Performance measurement name: CPU_OCCUPANCY_HWM

Performance measurement description: The maximum value calculated for the amount of time the CPU spent performing work as a percentage to its total running time over a 30 minute period. Reset to 0 every 30 minutes.

History: created in SN09

Performance Value Range: 0 - 100

Collection Interval: 10 seconds

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

Component: SIPGW_OVERLOAD

Performance measurement name: GCP_QUEUE_SIZE

Performance measurement description: The size of the GCP queue at the time the last sample was collected.

History: created in SN09

Performance Value Range: 0 - 4,294,967,296

Collection Interval: 10 seconds

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

Component: SIPGW_OVERLOAD

Performance measurement name: GCP_QUEUE_SIZE_HWM

Performance measurement description: The maximum sampled size of the GCP queue over a 30 minute period. Reset to 0 every 30 minutes.

History: created in SN09

Performance Value Range: 0 - 4,294,967,296

Collection Interval: 10 seconds

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

Component: SIPGW_OVERLOAD

Performance measurement name: SIP_QUEUE_SIZE

Performance measurement description: The size of the SIP queue at the time the last sample was collected.

History: created in SN09

Performance Value Range: 0 - 4,294,967,296

Collection Interval: 10 seconds

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

Component: SIPGW_OVERLOAD

Performance measurement name: SIP_QUEUE_SIZE_HWM

Performance measurement description: The maximum sampled size of the SIP queue over a 30 minute period. Reset to 0 every 30 minutes.

History: created in SN09

Performance Value Range: 0 - 4,294,967,296

Collection Interval: 10 seconds

OSS delivery (and interface) or Local only: Local

OSS Collection Interval: N/A

Element Manager Screen Name: N/A

File Name: /opt/apps/ngsspm/stdhist/NGSS.STD_OMs.QoS.<year>.<month>.<day>_<time>_EDT.csv

Memory Usage: 4 bytes

3.2.2 Performance File (CSV, SSV, XML) Format

```
Table=Begin
TableId,MeasurementKind,IntervalDuration,CaptureTime,Realiability
SIPGW_OVERLOAD,PeriodBased,15,unknown,Valid
Labels=Begin
TupleKey,KeyName
Key,KeyName
Reg1Name,Reg2Name,Reg3Name,Reg4Name
CPU_OCCUPANCY,CPU_OCCUPANCY_HWM,GCP_QUEUE_SIZE,GCP_QUEUE_SIZE_HWM
Reg5Name,Reg6Name
SIP_QUEUE_SIZE,SIP_QUEUE_SIZE_HWM
Labels=End
RowOfValues=Begin
RowOfValues=End
Table=End
```

Product = CS 2000

A00010303 -- Map Level Service Control Application Programming Interface

Functional Description

1: Applicable Solution(s)

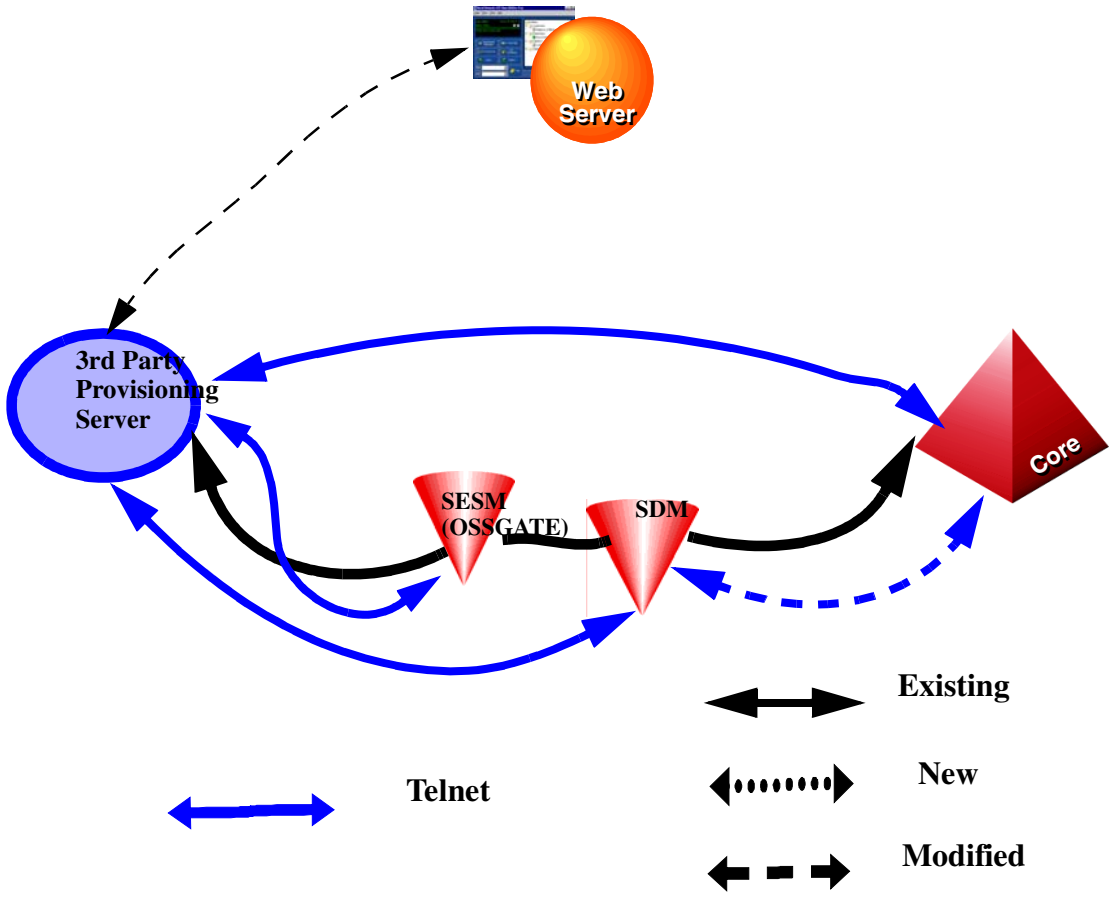
DMS, PT-AAL2

1.1 Description

This activity addresses the development associated with enabling in DMS and CS2000, the update and/or query capabilities for the switch based services. With the addition of this set of capabilities, subscribers will have the ability to both query the status and/or programmed information as well as activate/deactivate and update their corresponding service. Based on the service provider's interface for the end user, it takes out the complexity faced by the user to activate, deactivate, add, delete, change or edit specific data. The command performance will be in the range of 1 to 3 seconds.

1.1.1 Functional Behavior:

For CS2K, the commands issued by the end user will be sent via a 3rd party provisioning server to the OSSGATE via telnet. This is then sent to the SDM (Supernode Data Manager or CS2K Manager) which is the interface to the core for processing. The output will then be sent back and displayed to the end user via the web server. For TDM lines, there is a direct telnet connection between the 3rd party provisioning server and the SDM. This architecture can be used both for DMS and CS2K.



1.2 The Query command

Depending on the feature, the Query command can be used to query different fields such as the status, the list (if present), the delay interval and so on. When issued at the CI prompt, the query command will take the input parameters and call the query procedure for that feature. Depending on whether the feature is present or not, the corresponding return code is output.

1.2.1 QueryRequest

For a query request, the following are the input parameters:

- The DN of the subscriber associated with the given request would be a 10 digit DN.
- The corresponding feature/service would be simple enumerated type similar to the one defined in SERVORD and representing all supported services.

- The list of service attributes being queried would be simple set or enumerated type representing all possible attributes.

1.2.2 QueryResponse

The response will include the following:

Values corresponding to the service attributes queried.

- Only attributes for a single service per query will be supported in SN09.
- For list queries, the privacy indicator should be checked prior to displaying the corresponding DN.

1.2.3 List of supported Query Attributes

Table 1 List of supported Query Attributes

Enumeration	Return Value	Description
status	active or inactive	Query the status of the corresponding service
list	list of DNs 10 digits in length with/ without priv. ind.	Query all entries in the corresponding service's screening list.
listSize	positive integer less than 255	Query the number of entries in the corresponding service's screening list.
forwardDN	DN up to 30 digits in length	Query the forwarding DN of the corresponding call diversion service.
delayInterval	Positive integer between 1 and 10	Query the delay Interval of the corresponding service.This represents the number of rings.
scList	List of DNs variable in length up to 30 digits	Query all entries in the corresponding Speed Call list
all	Some aggregate of the above	Query all attributes of the corresponding service.

1.2.4 Service to Query attribute matrix

Each service belongs to a group from group1 to group9. These groups are based on the attributes of each service. The matrices below show the attributes present for each service.

Table 2 Service to Query Attribute matrix

Service	Status	Delay Interval	List	List Size	Forward DN	Speed Call List
MWI	X					
VMWI	X					
AMWI	X					
ACRJ	X					
ACB	X					
AR	X					
CSMI	X					
CWT	X					
LDSA	X					
SUPPPRESS	X					
MSB	X					
DRCW	X		X	X		
SCRJ	X		X	X		
SIMRING	X		X	X		
CFU	X				X	
CFDA	X				X	
CFB	X				X	
SCA	X		X	X		
SCF	X		X	X	X	
CFDVT		X				
CNDB						
CNAB						
COT						
CCW						
SCS						X
SCL						X
SCU						X

1.2.5 Error codes for the Query command

Table 3 Error codes for the Query Command

Return Code	Description
Failure - Invalid_Dn	DN entered is not valid.
Failure - Unavailable_Resources	The service is not subscribed on the DN.
	The feature SOC is idle.
	SLE SOC is idle.
Failure - SOC_Idle	The svcntrl SOC is idle.

1.2.6 Query Examples

Syntax to query the status of SCRJ for 6136631001

>svcntrl query 6136631001 scrj status

Status - Service_Active

Syntax to query the SCRJ list for 6136631001

>svcntrl query 6136631001 scrj list

List_Dn -

6136634567; 6136638901; 6136671001

6136671023; 6136789021; 6136779001

6136772021;

Syntax to query SCRJ for 6136631001

>svcntrl query 6136631001 scrj all

Status - Service_Active

List_Dn -

6136634567; 6136638901; 6136671001

6136671023; 6136789021; 6136779001

6136772021;

List_Size - 7

Syntax to query the Speed Call List of 6136771052

>svcntrl query 6136771052 scl all

Speed Call Code: 12 Dn: 6631021

Speed Call Code: 13 Dn: 6631022

Speed Call Code: 29 Dn: 6136671021

>svcntrl query 6136771052 scl sclist

Speed Call Code: 12 Dn: 6631021

Speed Call Code: 13 Dn: 6631022

Speed Call Code: 29 Dn: 6136671021

For a DN with any of the Call Forwarding features like CFB, CFD, SCF, if the feature is subscribed on the DN, but there is no forward DN present, then the return code for a Query command will be “ForwardDn - Not_Available”

>svcntrl query 6136671021 cfb forwarddn

ForwardDn - Not_Available

If the DN is not provisioned with the service, then the following error message displayed:

>Syntax to query status of CSMI on 6136671021

>svcntrl query 6136671021 CSMI status

Failure - Unavailable_Resources

1.2.7 The Query All Command

This command queries all the features and prints the response for each feature that is present on the User Dn. The feature name is not specified in the command. The syntax of the Query All command is:

> SVCNTRL QUERY <User DN> ALL

This command queries for all the features on a User DN and if any Service Management feature is subscribed on the User Dn, prints out the response. If a feature is not subscribed on the User DN, then no response for that feature is printed out. Only if the User Dn has no feature subscribed on it, the response of ‘Failure - Unavailable_Resources’ is printed.

There are certain conditions when the feature is subscribed on the User DN but returns ‘Failure - Unavailable_Resources’. For these conditions, only if no other feature is subscribed on the User DN, will this error message be printed. Else, it will be ignored and the other feature responses are printed. The following are the conditions:

- For the SLE features, the feature is subscribed on the User DN, but the required datafills in Table CUSTSTN are missing.
- For certain features like CFDVT, if the feature specific SOC is idle.
- Features belonging to Group 7(CNAB & CNDB) and Group 8(COT & CCW) are not supported for the Query command. So even if these features are present on the User Dn, the Query All command will not consider these features.

Some examples of the Query All command:

>svcntrl query 9097502513 all

MSB

Status - Service_Inactive

SCRJ

Status - Service_Active

List_Dn -

6136211025; 6136631022;

List_Size - 2

SCA

Status - Service_Active

List_Dn -

6136218001; 6136671001;

List_Size - 2

If no Service Management feature is present on the User Dn, a response of ‘Failure - Unavailable_Resources’ is returned.

>svcntrl query 9097502514 all

Failure - Unavailable_Resources

The Dn 6136218001 has COT, CNAB and CNDB subscribed on it. The response will be Unavailable_Resources since these features are not supported by the Query Command.

>svcntrl query 6136218001 all

Failure - Unavailable_Resources

1.3 The Update command

Depending on the feature, the Update command can be used to update different attributes such as the status, the delay interval, the forward DN and so on. When issued at the CI prompt, the Update command will take the input parameters and call the Update procedure for that feature. Depending on whether the feature is updated or not, the corresponding return code is output.

1.3.1 Update Request

For an Update request, the following are the input parameters

- The DN of the subscriber associated with the given request will be a 10 digit DN.
- The corresponding service will be represented as a simple enumerated type similar to the one defined in SERVORD and representing all supported services.
- The action to be taken will be represented as a simple enumerated type representing all supported actions.

1.3.2 Update Response

Will include the following:

Return codes indicating non availability of the API (i.e. is the CI SOC idle)

- The return code will be in the form of readable text.

Return codes indicating the confirmation or denial of the Update request.

- Simple enumerated type representing all supported Update return codes.
- The return code will be displayed as readable text.

  For example, confirmation from an Update request to activate CSMI would be represented as “Success - Service_Activated”.

1.3.3 List of supported Update Actions

The following table gives the list of actions that is supported for each service.

Table 4 List of supported Update Actions

Enumeration	Description
activate	Activate corresponding service.
deactivate	Deactivate corresponding service.
delayInterval	Set delay interval for corresponding service.This is the number of rings.
adddn	Add specified DN to corresponding service's screening list.
deletedn	Delete specified DN from corresponding service's screening list.
deleteAlldn	Delete all DNs from corresponding service's screening list.
deleteAllPrivdn	Delete all private DNs from corresponding service's screening list.
setfwdDN	Set forwarding DN for corresponding call diversion service.
clearFwdDN	Clear forwarding DN for corresponding call diversion service.
toggle	Toggle status of the corresponding services.
invoke	Invoke the corresponding service.
changeList	Change a specified speed call cell entry.

1.3.4 Service to Update Action matrix

Each service belongs to a group from group1 to group9. These groups are based on the attributes of each service. The matrices below show the attributes present for each service.

Table 5 Service to Update Action matrix

Service	Activate	Deactivate	DelayInterval	Adddn	Deletedn	DeleteAlldn	Delete All Privated n	Set Fwd Dn	Clear Fwd DN	Toggle	Invoke	Change List
MWI	X	X										
VMWI	X	X										
AMWI	X	X										
ACRJ	X	X										
ACB	X	X										
AR	X	X										
CSMI	X	X										
CWT	X	X										

Service	Activate	Deactivate	DelayInterval	Addn	Deletedn	DeleteAlldn	Delete All Privatedn	Set Fwd Dn	Clear Fwd DN	Toggle	Invoke	Change List
LDSA	X	X										
MSB	X	X										
SUPPRESS	X	X										
DRCW	X	X		X	X	X	X					
SCRJ	X	X		X	X	X	X					
SIMRING	X	X		X	X	X	X					
CFU	X	X						X	X			
CFDA	X	X						X	X			
CFB	X	X						X	X			
SCA	X	X		X	X	X	X					
SCF	X	X		X	X	X	X	X	X			
CFDVT			X									
CNDB										X		
CNAB										X		
COT											X	
CCW											X	
SCS												X
SCL												X
SCU												X

Update Examples
Syntax to activate Call Forward BusyLine on 4164731051

>svcntrl update 4164731051 cfb activate

Success - Service_Activated

Syntax to clear the forward DN on 4164731051

>svcntrl update 4164731051 cfb clearFwdDn

Success - ForwardingDn_Cleared

Syntax to set the forward DN on 4164731051

>svcntrl update 4164731051 cfb setFwdDn dn 4164631001

Success - ForwardingDn_Set

Syntax to add a DN to the Speed Call List of 6136771052

>svcntrl update 6136771052 scl changelist 12 6631021

Success - Service_Activated

Error conditions:

If we try to activate an already activated service

>svcntrl update 4164731051 cfb activate

Failure - Service_Already_Active

If the user tries deleting a list which is empty, the response would be

>svcntrl update 4164731051 simring deleteallDN

Failure - List_Is_Empty

If the SOC for SPRING (call forward ringing) is not turned on, the response would be

>svcntrl update 4164731051 cfdvt delayInterval 4

Failure - Unavailable_Resources

Ex6: If the parameters entered are insufficient

>svcntrl update

The response would be:

Failure - Missing_Parameter

1.3.5 List of supported Update responses

Table 6 List of supported Update responses

Response	Meaning
Success - Service_Activated	Successful activation of the service.
Success - Service_Deactivated_or_Cancelled	Successful deactivation of the service.
Success - AnonymousEntry_Added	Successful addition of a private no. to the list of a DN.
Success - PublicEntry_Added	Successful addition of a DN to the list of another DN.
Success - AnonymousEntry_Removed	Successful deletion of a private number from a DNs list.
Success - PublicEntry_Removed	Successful deletion of a DN from a DNs list.
Success - All_Anonymous_Entries_Removed	Successful deletion of all private DNs from the list.
Success - All_Entries_Removed	Successful deletion of all DNs from the list.
Success - ForwardingDn_Set	Successful setting of a FwdDN to another DN.
Success - ForwardingDn_Cleared	Successful clearing of a FwdDN from another DN.
Success - DelayInterval_Updated	Successful updating of delay interval of a DN.
Failure - Service_Already_Active	Not updated because the service is already active on the DN.
Failure - Service_Not_Activated	Gives this response because the service might be inactive and the user is trying to deactivate or in the case of ACB/AR if the feature queue is not present.
Failure -Invalid_Forwarding_Dn	FwdDN not set because the FwdDN did not pass validation.
Failure - List_Is_Empty	When trying to delete a DN from the list of another DN and if the list is empty.
Failure -List_Is_Full	When trying to add a DN to the list of another DN and if the list is full and cannot accommodate more DNs.
Failure - Public_Dn_Already_On_List	If the DN you are trying to add to the list of another DN is already present.
Failure - Anonymous_Dn_Already_On_List	If the private DN you are trying to add to the list of another DN is already present.
Failure - Dn_Not_On_List	If the DN you are trying to delete is not on the list.
Failure - No_Match	When trying to update the delay interval, if the ring control is not programmable ring type.
	For the SLE features, when trying to delete a private DN from the list of the subscriber DN, if no private DN is present on the list.

Response	Meaning
Failure - Unsuccessful_Update	This message comes when the update is not successful and for different features and actions, are different.
	For ACB/AR, activation of the feature is not supported.
	For CFB, if Fixed or Programmable version is not provisioned.
	For CFBL & CFDA, with control N type.
	FOR CFDA if IECFD is provisioned or if CFD Normal is provisioned.
	For Speed Call, if SCU is provisioned.

1.3.6 Error codes for the update command

Table 7 Error codes for the Update Command

Return Code	Description
Failure - Invalid_Dn	DN entered is not valid.
Failure - MSRID_Does_Not_Match_User_Profile	For all types of MWT an Msr Id has to be input.This will be validated against Table MSRTAB.If there is a mismatch, then it returns this code.
Failure - Unavailable_Resources	The service is not subscribed on the DN.
	The feature SOC is idle.
	For ACB and AR, checks the validity of the feature and if the feature is not allowed gives this response.
	For ACRJ, COT if universal access is not permitted.
	For CFB, if IECFB is provisioned.
	For CFD, if IECFD is provisioned.
	For CFU, if CFU/CFI/CFF is not provisioned.
	For CNAB & CNDB, if the call is not up.
	FOR MWI, if EMW or CALLOG is assigned to the line.
	The SLE SOC is idle.
	Deactivate MWT when MWT is not active
	For services that use SLE, if SLE datafills are missing in Table CUSTSTN.
Failure - SOC_Idle	The SVCNTRLI SOC is idle.

1.3.7 SIMRING Virtual DN

A SIMRING Virtual DN can be provisioned using the NEWDN command in SERVORD. It is the only feature in Service Management that can be provisioned on a Virtual DN. On issuing an Update/Query command for a SIMRING Virtual DN, the DN is validated and then the query is sent to the Service Management framework. The following is the response received for a SIMRING Virtual DN:

>svcntrl query 6136672000 simring all

Status - Service_Inactive

List_Dn -

6136634567; 6136638901; 6136671001

List_Size - 3

> svcntrl update 6136672000 simring activate

Success - Service_Activated

When the Query/Update command for a SIMRING Virtual DN is given with other features, the response will be Failure - Unavailable_Resources.

>svcntrl query 6136672000 msb all

Failure - Unavailable_Resources

>svcntrl query 6136672000 scf all

Failure - Unavailable_Resources

> svcntrl update 6136672000 msb activate

Failure - Unavailable_Resources

> svcntrl update 6136672000 scf adddn dn 6631022

Failure - Unavailable_Resources

When the User DN is a Virtual DN of a type other than SIMRING like ACD, AIN etc, then the comand will be blocked at the CI level with a response of Failure - Invalid_Dn.

>svcntrl query 6136671000 simring all

Failure - Invalid_Dn

>svcntrl query 6136671000 msb all

Failure - Invalid_Dn

>svcntrl update 6136671000 simring activate

Failure - Invalid_Dn

> svcntrl update 6136671000 drcw adddn dn 6671001

Failure - Invalid_Dn

1.4 Error responses for Invalid Entries

Table 8 Error responses for invalid entries

Return Value	Description
Failure - Invalid_Action	When any other value other than update or query is entered after svcntrl.
Failure - Invalid_DNformat	When the DN entered has alpha numeric values or if the DN is not of 10 digit form.
Failure - Unrecognized_Service	When the service entered is invalid.
Failure - Invalid_Attribute	When the attribute entered for that service is invalid.
Failure - Invalid_Attribute_Parameter	When the parameters for the attributes are specified incorrectly. For e.g., if the value of delay interval to be updated is greater than 10.
Failure - Missing_Parameter	When an incomplete command is issued, i.e. if the service, attribute, or any of the parameters are missing.

Ex 1: When the action given is not update/query

>svcntrl updation 6136631001 acrj activate

The response would be:

Failure - Invalid_Action

Ex2: If the DN is invalid

>svcntrl query abc6790123 drcw list

The response would be:

Failure - Invalid_DNformat

Ex3: If the DN entered is not 10 digit

>svcntrl query 6631001 cfb ForwardDN

The response would be:

Failure - Invalid_DNformat

Ex4: If the service is not valid

>svcntrl update 6136671021 cssi activate

The response would be:

Failure - Unrecognized_Service

Ex5: If the attribute is not valid for that service

>svcntrl update 4164671021 cndb FwdDn

The response would be:

Failure - Invalid_Attribute

EX7: If the attribute parameters are invalid

>svcntrl update 4164671001 cfdvt delayInterval 65

The response would be:

Failure - Invalid_Attribute_Parameter

Ex6: If the parameters entered are insufficient

>svcntrl update

The response would be:

Failure - Missing_Parameter

>svcntrl query scs

Failure - Missing_Parameter

1.5 Hardware Requirements or Dependencies

In order to enable this capability for affected subscribers, the following must be present in the provider's network

- Some Provider Network Server designed to support service queries/updates via some Web or PC Client based interface.
- SESM/OSSGATE - An application that is used for the provisioning and maintenance of lines, trunks etc. The OSSGATE passes on the command information to the SDM.
- SDM /CS2K Core Manager - The SDM is an interface to the core. It takes in the commands given by the SESM and passes them onto the core and also takes the responses from the core and gives it to the SESM.

1.6 Software Requirements or Dependencies

The new SOC SMGT0001 will control the CI interface to Service Management. This SOC will be independent of the AIN TCAP Service Management SOC control. The following table gives the possible supported state of both the SOCs:

Table 9 Supported SOC States

AIN SOC	Service Management SOC	Implication
ON	ON	Both interfaces will be active at the same time.
IDLE	IDLE	Both interfaces will be inactive at the same time.
ON	IDLE	AIN interface to be active and SVCNTRL to be inactive.
IDLE	ON	AIN interfaces to be inactive and SVCNTRL to be active.
ON for some	ON	Some combination of AIN interfaces active and SVCNTRL active.
ON for some	IDLE	Some combination of AIN interfaces active and SVCNTRL inactive.

1.7 Limitations and restrictions

This capability will be applicable only to North American loads. If some invalid characters are entered after a valid command, then the command will not be rejected. The command will be processed with the valid input. Refer to A00004036 FN for the limitations and restrictions of each service.

1.7.1 List of supported services/features

The following table gives the list of supported services/features the market that they are valid for.

Table 10 Supported Services/Features

Service	Servord Acronym
Message Waiting Indicator [a]	MWI
Visual Message Waiting Indicator <Superscript1>a.	VMWI
Audio Message Waiting Indicator <Superscript1>a.	AMWI
Anonymous Call Rejection	ACRJ
Automatic Callback	ACB
Automatic Recall	AR
Call Screening<Superscript1>a.	CSMI
Outside Calling Area Alerting<Superscript1>a.	LDS
Calling ID delivery & Suppression	SUPPRESS
Call Waiting (requires CWTACT)	CWT
Make Set Busy	MSB
Distinctive Ringing Call Waiting [b]	DRCW
Selective Call Rejection<Superscript1>b.	SCRJ
Simultaneous Ringing	SIMRING
Call Forward Don't Answer [c]	CFDA
Call Forwarding Variable	CFU
Call Forward Busy Line[d]	CFB
Selective Call Acceptance <Superscript1>a.	SCA
Selective Call Forwarding<Superscript1>a.	SCF
Call Forwarding Ringing Control<Superscript1>b.	CFDVT
Calling Number Delivery Blocking	CNDB
Calling Name Delivery Blocking	CNAB
Customer Originated Trace	COT
Cancel Call Waiting	CCW
Speed Calling Short	SCS
Speed Calling Long	SCL

Service	Servord Acronym
Speed Calling User	SCU

a.North American Market Only
b.North American Dialplan Only

c.This service will include both CFDA and CFD.
d.This service will include both CFBL and CFB.

1.7.2 List of supported DN specifiers

Table 11 Supported DN Specifiers

Enumeration	Description
user	DN being added or deleted provided explicitly by the subscriber.
speed call	Add/Delete the DN in the subscriber's corresponding speed call entry
icm	Add/Delete the DN in the subscriber's Incoming Call Memory.

1.8 Applicable customer facing sections

Fault Management

Logs ___N/A

Alarms ___N/A

Configuration

Data Schema ___N/A

User Interface ___N/A

Element Management ___X

Security ___N/A

Service Order ___N/A

Office Parameters ___N/A

Accounting (includes AMA billing) _____X

Performance (includes operational measurements) _____X

1.9 Glossary

Term	Description
SDM	Supernode Data Manager or CS2K Manager
SESM	Succession Element Sub element Manager

1.10 References

A00004036 - Off Board Service Control

2: Configuration for A00010303

2.1 Hardware and Software Requirements

2.1.1 Hardware requirements

In order to enable this capability for affected subscribers, the following must be present in the provider's network:

- Some Provider Network Server designed to support service queries/updates via some Web or PC Client based interface.
- SESM/OSSGATE - An application that is used for the provisioning and maintenance of lines, trunks etc. The OSSGATE passes on the command information to the SDM.
- SDM - The SDM is an interface to the core. It takes in the commands given by the SESM and passes them onto the core and also takes the responses from the core and gives it to the SESM.

2.1.2 Software requirements

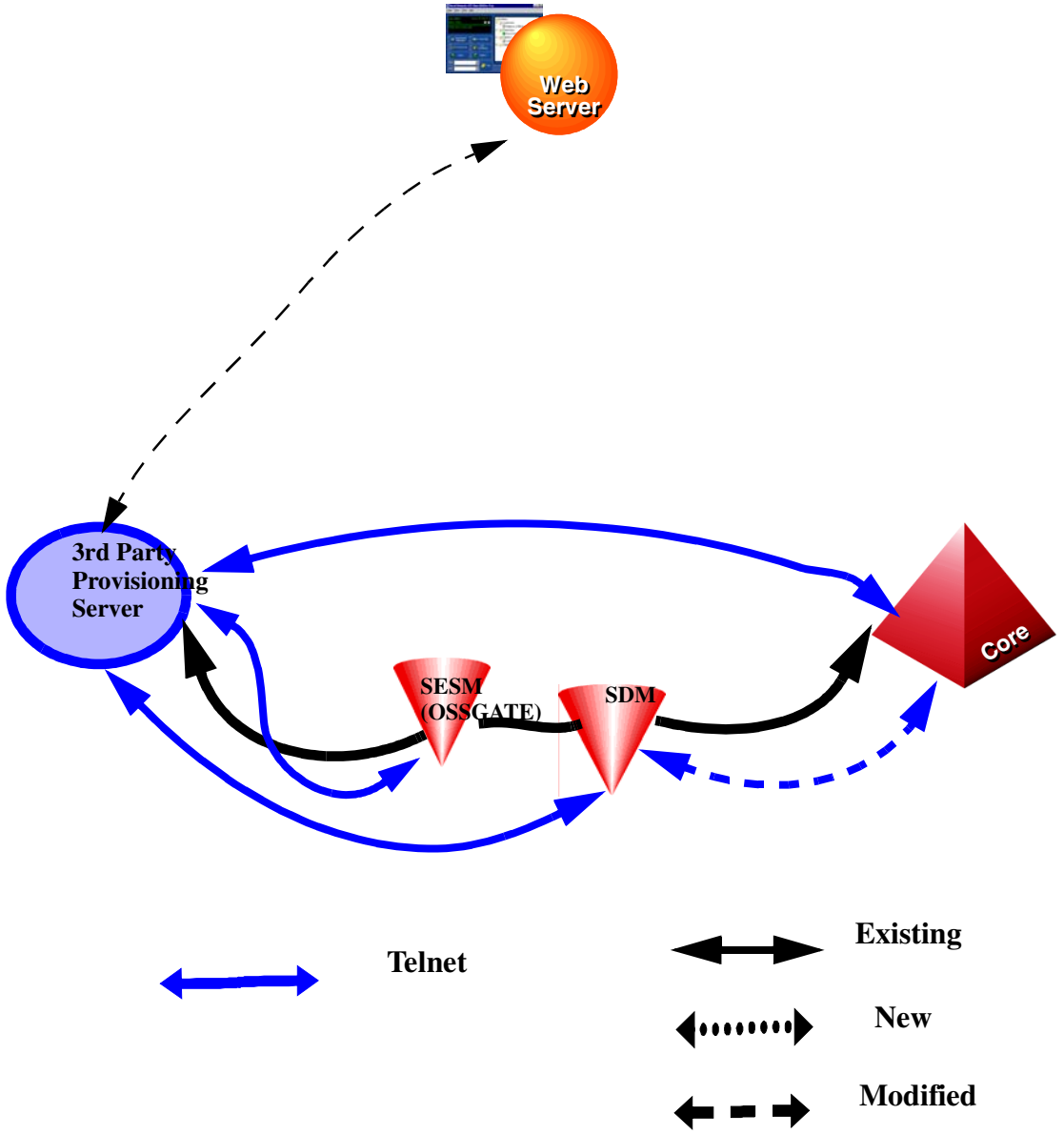
The new SOC SMGT0001 will control the CI interface to Service Management. This SOC will be independent of the AIN TCAP Service Management SOC control. The following table gives the possible supported state of both the SOCs:

Table 1 Supported SOC states

AIN SOC	Service Management SOC	Implication
ON	ON	Both interfaces will be active at the same time.
IDLE	IDLE	Both interfaces will be inactive at the same time.
ON	IDLE	AIN interface to be active and SVCNTRL to be inactive.

AIN SOC	Service Management SOC	Implication
IDLE	ON	AIN interfaces to be inactive and SVCNTRL to be active.
ON for some	ON	Some combination of AIN interfaces active and SVCNTRL active.
ON for some	IDLE	Some combination of AIN interfaces active and SVCNTRL inactive.

2.2 Initial Configuration



In the case of CS2K, the commands issued by the end user will be sent via a 3rd party provisioning server to the OSSGATE via telnet. This is then sent to the SDM (Supernode Data Manager or CS2K Manager) which is the interface to the core for processing. The output will then be sent back and displayed to the end user via the web server. In the case of TDM lines, there is a direct connection between the provisioning server and the core. This architecture can be used both for DMS and CS2K.

2.3 Software optionality control (SOC)

Table 2 SOC

SOC option name:	Service Mgmt-DMSCS2K
SOC option title:	Map Based Service Control
SOC option control type:	State
New SOC option?	Yes
SOC option order code	SMGT0001
Option defined in DRU:	CCM
Affected products:	SNNCSH09

2.4 Command interface changes

2.4.1 Directory: SVCNTRL

The command to enter into this CI tool is

> svcntrl <query/update> <DN> <feature/service> <attribute><attribute parameter>

2.4.1.1 Directory description

On entering command SVCNTRL, the user should enter one of the two options i.e. either query a service or update a service. For Query, the further options will be the DN, the feature/service and the attribute to be queried. For Update, the further options will be the DN, the feature/service and the attribute, and the attribute parameter to be updated.

2.4.1.2 Accessing directory: SVCNTRL

The directory will be a single level directory. The user will be able to enter the commands on a single line.

2.4.1.2.1 Access to directory or MAP level and return to CI

Access to the directory from CI prompt will be available on entering SVCNTRL at the CI level. Enter a Carriage Return to return to the CI prompt.

CI:

>svcntrl <query/update> <DN> <feature> <attribute><attribute parameter>

2.4.2 Command: SVCNTRL

2.4.2.1 Command type: NON- MENU

2.4.2.2 Command target: All

2.4.2.3 Command availability: RES

2.4.2.4 Command description

SVCNTRL is the command issued at CI prompt that is used to both query the status and/or programmed information as well as activate/deactivate and update their corresponding service.

2.4.2.4.1 The Query command

The Query command is used to query the following attributes depending on what the service is:

Table 3 List of supported Query attributes

Enumeration	Return Value	Description
status	active or inactive	Query the status of the corresponding service.
list	list of DNs 10 digits in length with /without priv. ind.	Query all entries in the corresponding service's screening list.
listSize	Positive integer less than 255	Query the number of entries in the corresponding service's screening list.
forwardDN	DN up to 30 digits in length	Query the forwarding DN of the corresponding call diversion service.
delayInterval	Positive integer between 1 and 10	Query the delay Interval (number of rings) of the corresponding service.
scList	List of DNs variable in length up to 30 digits	Query all entries in the corresponding Speed Call list.
all	Some aggregate o f the above	Query all attributes of the corresponding service.

The following table gives the structure of the SVCNTRL query command and how a valid command is to be issued. It also gives the valid option for each of the services. Only one attribute can be queried at a time.

Table 4 Query Command Syntax

Command	Action	DN	Feature	Attribute

SVCNTRL	Query	<10 digit DN>	MWI	Status All
			VMWI	
			AMWI	
			ACRJ	
			ACB	
			AR	
			CSMI	
			CWT	
			LDSA	
			MSB	
			SUPPRESS	
SVCNTRL	Query	<10 digit DN>	DRCW	Status List List Size All
			SCRJ	
			SIMRING	
SVCNTRL	Query	<10 digit DN>	CFU	Status Forward DN All
			CFDA	
			CFB	
SVCNTRL	Query	<10 digit DN>	SCA	Status List List Count All
			SCF	Status List List Count Forward DN All
SVCNTRL	Query	<10 digit DN>	CFDVT	Delay Interval All
SVCNTRL	Query	<10 digit DN>	SCS	Speed Call List All

Some examples of the Query command are:

Syntax to query the status of SCRJ for 6136631001

>svcntrl query 6136631001 scrj status

Status - Service_Active

Syntax to query the SCRJ list for 6136631001

>svcntrl query 6136631001 scrj list

List_Dn -

6136634567;6136678901;61366710021

6136631021; 6136789021;6136779001;

6136772021

Syntax to query SCRJ for 6136631001

>svcntrl query 6136631001 scrj all

Status - Service_Active

List_Dn -

6136634567; 6136678901; 61366710021

6136631021; 6136789021; 6136779001

6136772021;

List_Size - 7

Syntax to query the Speed Call List of 6136771052

>svcntrl query 6136771052 scl all

Speed Call Code: 12 Dn: 6631021

Speed Call Code: 13 Dn: 6631022

Speed Call Code: 29 Dn: 6136671021

>svcntrl query 6136771052 scl sclist

Speed Call Code: 12 Dn: 6631021

Speed Call Code: 13 Dn: 6631022

Speed Call Code: 29 Dn: 6136671021

For a DN with any of the Call Forwarding features like CFB, CFD, SCF, if the feature is subscribed on the DN, but there is no forward DN present, then the return code for a Query command will be “ForwardDn - Not_Available”

>svcntrl query 6136671021 cfb forwarddn

ForwardDn - Not_Available

If the DN is not provisioned with the service, then the following error message is displayed:

Syntax to query status of CSMI on 6136671021

>svcntrl query 6136671021 CSMI status

Failure - Unavailable_Resources

2.4.2.4.2 The Query All Command

This command queries all the features and prints the response for each feature that is present on the User Dn. The feature name is not specified in the command. The syntax of the Query All command is:

> SVCNTRL QUERY <User DN> ALL

This command queries for all the features on a User DN and if any Service Management feature is subscribed on the User Dn, prints out the response. If a feature is not subscribed on the User DN, then no response for that feature is printed out. Only if the User Dn has no feature subscribed on it, the response of ‘Failure - Unavailable_Resources’ is printed.

There are certain conditions when the feature is subscribed on the User DN but returns ‘Failure - Unavailable_Resources’. For these conditions, only if no other feature is subscribed on the User DN, will this error message be printed. Else, it will be ignored and the other feature responses are printed. The following are the conditions:

- For the SLE features, the feature is subscribed on the User DN, but the required datafills in Table CUSTSTN are missing.
- For certain features like CFDVT, if the feature specific SOC is idle.
- Features belonging to Group 7(CNAB & CNDB) and Group 8(COT & CCW) are not supported for the Query command. So even if these features are present on the User Dn, the Query All command will not consider these features.

Some examples of the Query All command:

>svcntrl query 9097502513 all

MSB

Status - Service_Inactive

SCRJ

Status - Service_Active

List_Dn -

6136211025; 6136631022;

List_Size - 2

SCA

Status - Service_Active

List_Dn -

6136218001; 6136671001;

List_Size - 2

If no Service Management feature is present on the User Dn, a response of 'Failure - Unavailable_Resources' is returned.

>svcntrl query 9097502514 all

Failure - Unavailable_Resources

The Dn 6136218001 has COT, CNAB and CNDB subscribed on it. The response will be Unavailable_Resources since these features are not supported by the Query Command.

>svcntrl query 6136218001 all

Failure - Unavailable_Resources

2.4.2.4.3 The Update Command

The Update command is used to update the following attributes depending on what the service is:

Table 5 List of supported Update Actions

Enumeration	Description
activate	Activate corresponding service.

Enumeration	Description
deactivate	Deactivate corresponding service.
delayInterval	Set delay interval for corresponding service.This is an integer value between 1 and 10 and represents the no. of rings.
adddn	Add specified DN to corresponding service's screening list.
deletedn	Delete specified DN from corresponding service's screening list.
deleteAlldn	Delete all DNs from corresponding service's screening list.
deleteAllPrivdn	Delete all private DNs from corresponding service's screening list.
setfwdDN	Set forwarding DN for corresponding call diversion service.
clearFwdDN	Clear forwarding DN for corresponding call diversion service.
toggle	Toggle status of the corresponding services.
invoke	Invoke the corresponding service.
changeList	Change a specified speed call cell entry.

The following table gives the structure of the SVCNTRL Update command and how a valid command is to be issued. It gives the valid option for each of the services. Only one attribute can be updated at a time.

Table 6 Update Command Syntax

Command	Action	DN	Feature	Attribute	Attribute parameters

SVCNTRL	Update	<10 digit DN>	MWI	Activate Deactivate	
			VMWI		
			AMWI		
			ACRJ		
			ACB		
			AR		
			CSMI		
			CWT		
			LDSA		
			MSB		
			SUPPRESS		
SVCNTRL	Update	<10 digit DN>	DRCW	Activate Deactivate Adddn Deletedn DeleteAlldn DeleteAllprivdn	
			SCRJ		DN <Dn> SpeedCallCode <SCC> ICM
			SIMRING		
SVCNTRL	Update	<10 digit DN>	CFU	Activate Deactivate Setfwddn ClearFwddn	
			CFDA		dn <DN> SpeedCallCode <SCC>
			CFB		
SVCNTRL	Update	<10 digit DN>	SCA	Activate Deactivate Adddn Deletedn DeleteAlldn DeleteAllprivdn	dn <DN> SpeedCallCode <SCC> ICM
			SCF	Activate Deactivate Adddn Deletedn DeleteAlldn DeleteAllprivdn SetFwdDN ClearFwdDN	dn <DN> SpeedCallCode <SCC> ICM
SVCNTRL	Update	<10 digit DN>	CFDVT	Set Delay Interval < 1 to 10>(number of rings)	< 1 to 10> (number of rings)
SVCNTRL	Update	<10 digit DN>	CNDB	Toggle	
			CNAB		

SVCNTRL	Update	<10 digit DN>	COT	Invoke	
			CCW		
SVCNTRL	Update	<10 digit DN>	SCS	Change List	SpeedCallCode <SCC> dn <DN>
			SCL		
			SCU		

NOTE: For SIMRING, deleteallprivdn and ICM is invalid.

Some examples of the Update command are:

Syntax to activate Call Forward BusyLine on 4164731051

>svcntrl update 4164731051 cfb activate

Success - Service_Activated

Syntax to clear the forward DN on 4164731051

>svcntrl update 4164731051 cfb clearFwdDn

Success - ForwardingDn_Cleared

Syntax to set the forward DN on 4164731051

>svcntrl update 4164731051 cfb setFwdDn dn 4164631001

Success - ForwardingDn_Set

Syntax to add a DN to the Speed Call List of 6136771052

>svcntrl update 6136771052 scl changelist 12 6631021

Success - Service_Activated

Error conditions:

If we try to activate an already activated service

>svcntrl update 4164731051 cfb activate

Failure - Service_Already_Active

If the user tries deleting a list which is empty, the response would be

>svcntrl update 4164731051 simring deleteallDN

Failure - List_Is_Empty

If the SOC for SPRING (call forward ringing) is not turned on, the response would be

>svcntrl update 4164731051 cfdvt delayInterval 4

Failure - Unavailable_Resources

2.4.2.5 Command syntax

Table 7 Command Syntax

Command	Parameters and variables
SVCNTRL	**input parameters** <query/update> <DN> <feature/service> <attribute> <attribute parameters> **output parameters** A readable sentence depending upon what the return code is

2.4.2.6 Qualifications and warnings

2.4.2.7 Responses

2.4.2.7.1 Error codes for the Query Command

Table 8 Error codes for the Query Command

Return Code	Description
Failure - Invalid_Dn	DN entered is not valid.
Failure - Unavailable_Resources	The service is not subscribed on the DN.
	The feature SOC is idle.
	SLE SOC is idle.
Failure - SOC_Idle	The SVCNTRL SOC is idle.

2.4.2.7.2 Responses for the update command

The following table gives the valid responses for the update command

Table 9 Responses for the Update Command

Response	Meaning
Success - Service_Activated	Successful activation/deactivation of the service.
Success - Service_Deactivated_or_Cancelled	Successful deactivation of the service.
Success - AnonymousEntry_Added	Successful addition of a private no to the list of a DN.
Success - PublicEntry_Added	Successful addition of a DN to the list of another DN.
Success - AnonymousEntry_Removed	Successful deletion of a private number from a DNs list.
Success - PublicEntry_Removed	Successful deletion of a DN from a DNs list.
Success - All_Anonymous_Entries_Removed	Successful deletion of all private DNs from the list.
Success - All_Entries_Removed	Successful deletion of all DNs from the list.
Success - ForwardingDn_Set	Successful setting of a FwdDN to another DN.
Success - ForwardingDn_Cleared	Successful clearing of a FwdDN from another DN.
Success - DelayInterval_Updated	Successful updating of delay interval of a DN.
Failure - Service_Already_Active	Not updated because the service is already active on the DN.
Failure - Service_Not_Activated	Gives this response because the service might be inactive and the user is trying to deactivate or in the case of ACB/AR if the feature queue is not present.
Failure -Invalid_Forwarding_Dn	FwdDN not set because the FwdDN did not pass validation.
Failure - List_Is_Empty	When trying to delete a DN from the list of another DN and if the list is empty.
Failure -List_Is_Full	When trying to add a DN to the list of another DN and if the list is full and cannot accommodate more DN's.
Failure - Public_Dn_Already_On_List	If the DN you are trying to add to the list of another DN is already present.
Failure - Anonymous_Dn_Already_On_List	If the private DN you are trying to add to the list of another DN is already present.
Failure - Dn_Not_On_List	If the DN you are trying to delete is not on the list.
Failure - No_Match	When trying to update the delay interval, if the ring control is not programmable ring type.

Response	Meaning
	For the SLE features, when trying to delete a private DN from the list of the subscriber DN, if no private DN is present on the list.
Failure - Unsuccessful_Update	When the update is not successful and for different features and actions, its meaning is different.
	For ACB/AR, activation of the feature is not supported.
	For CFB, if Fixed or Programmable version is not provisioned.
	For CFBL & CFDA, with control N type.
	FOR CFDA if IECFD is provisioned or if CFD Normal is provisioned.
	For Speed Call, if SCU is provisioned.

2.4.2.7.3 Error codes for the update command

Table 10 Error codes for the Update Command

Return Code	Description
Failure - Invalid_Dn	DN entered is not valid.
Failure - MSRID_Does_Not_Match_User_Profile	For all types of MWT an Msr Id has to be input.This will be validated against Table MSRTAB.If there is a mismatch, then it returns this code.
Failure - Unavailable_Resources	The service is not subscribed on the DN.
	The feature SOC is idle.
	For ACB and AR, checks the validity of the feature and if the feature is not allowed gives this response.
	For ACRJ, COT if universal access is not permitted.
	For CFB, if IECFB is provisioned.
	For CFD, if IECFD is provisioned.
	For CFU, if CFU/CFI/CFF is not provisioned.
	For CNAB & CNDB, if the call is not up.
	FOR MWI, if EMW or CALLOG is assigned to the line.
	The SLE SOC is idle.
	Deactivate MWT when MWT is not active

Return Code	Description
	For services that use SLE, if SLE datafills are missing in Table CUSTSTN.
Failure - SOC_Idle	The SVCNTRLCI SOC is idle.

Table 11 Map outputs with associated meanings and actions

Command
Ex1: If the user tries to update the delay interval of a DN with CFW ring control **>svcntrl** update 4164731051 cfdvt delayInterval 4 **RESPONSE**:>Failure - Unavailable_Resources **Meaning:** Each feature is controlled by a SOC and this SOC needs to be turned on. The above response means that the SOC for SPRING is not turned on. **System or user actions:** For the delay Interval attribute to be update the SOC for SPRING should be turned on. **Ex2:**If the user tries deleting the list of a DN with the SIMRING feature **>svcntrl update 4164731051 simring deleteallDN** **RESPONSE:> Failure - List_Is_Empty** **Meaning: This means that there is no DN present in the list of 4164731051** **System or user actions:** This is not an error scenario, so no action need be taken but the user can query the DN for the list before trying to delete the list.

2.4.2.7.4 Error responses when invalid entries are given

Table 12 Error responses for invalid entries

Return Value	Description
Failure - Invalid_Action	When any other value other than update or query is entered after SVCNTRL.
Failure - Invalid_DNformat	When the DN entered has alpha numeric values or if the DN is not of 10 digit form.
Failure - Unrecognized_Service	When the service entered is invalid.
Failure - Invalid_Attribute	When the attribute entered for that service is invalid.

Return Value	Description
Failure - Invalid_Attribute_Parameter	When the parameters for the attributes are specified incorrectly. For e.g., if the value of delay interval to be updated is greater than 10.
Failure - Missing_Parameter	When an incomplete command is issued, i.e. if the service, attribute, or any of the parameters are missing.

If the user enters an invalid option then the tool will throw an exception. Rather than prompting the user, the appropriate message will be given and the user will have to re-enter the command with valid options. The following are the responses for invalid entries.

Ex 1: When the action given is not update/query

>svcntrl updation 6136631001 acrj activate

The response would be:

Failure - Invalid_Action

Ex2: If the DN is invalid

>svcntrl query abc6790123 drcw list

The response would be:

Failure - Invalid_DNformat

Ex3: If the DN entered is not 10 digit

>svcntrl query 6631001 cfb ForwardDN

The response would be:

Failure - Invalid_DNformat

Ex4: If the service is not valid

>svcntrl update 6136671021 cssi activate

The response would be:

Failure - Unrecognized_Service

Ex5: If the attribute is not valid for that service

>svcntrl update 4164671021 cndb FwdDn

The response would be:

Failure - Invalid_Attribute

EX7: If the attribute parameters are invalid

>svcntrl update 4164671001 cfdvt delayInterval 65

The response would be:

Failure - Invalid_Attribute_Parameter

Ex6: If the parameters entered are insufficient

>svcntrl update

The response would be:

Failure - Missing_Parameter

>svcntrl query scs

Failure - Missing_Parameter

2.4.2.8 SIMRING Virtual DN

A SIMRING Virtual DN can be provisioned using the NEWDN command in SERVORD. It is the only feature in Service Management that can be provisioned on a Virtual DN. On issuing an Update/Query command for a SIMRING Virtual DN, the DN is validated and then the query is sent to the Service Management framework. The following is the response received for a SIMRING Virtual DN:

>svcntrl query 6136672000 simring all

Status - Service_Inactive

List_Dn -

6136634567; 6136638901; 6136671001

List_Size - 3

> svcntrl update 6136672000 simring activate

Success - Service_Activated

When the Query/Update command for a SIMRING Virtual DN is given with other features, the response will be Failure - Unavailable_Resources.

>svcntrl query 6136672000 msb all

Failure - Unavailable_Resources

>svcntrl query 6136672000 scf all

Failure - Unavailable_Resources

> svcntrl update 6136672000 msb activate

Failure - Unavailable_Resources

> svcntrl update 6136672000 scf adddn dn 6631022

Failure - Unavailable_Resources

When the User DN is a Virtual DN of a type other than SIMRING like ACD, AIN etc, then the comand will be blocked at the CI level with a response of Failure - Invalid_Dn.

>svcntrl query 6136671000 simring all

Failure - Invalid_Dn

>svcntrl query 6136671000 msb all

Failure - Invalid_Dn

>svcntrl update 6136671000 simring activate

Failure - Invalid_Dn

> svcntrl update 6136671000 drcw adddn dn 6671001

Failure - Invalid_Dn

2.4.2.9 Example

Table 13 Examples of SVCNTRLCI command

Description of task:	To query the delay Interval on DN 613 663 1001 with CFW ring control.
Command: MAP response:	>**svcntrl query 6136631001 CFDVT delayInterval** **Delay_Interval - 2**
Description of Task:	To set the forward DN for 6136631001 with cfb option

Command: MAP response:	>**svcntrl update 6136631001 cfb setFwdDN dn 6136671001** **Success - ForwardingDN_Set**
Description of Task:	To query the status of CSMI on 6136671021
Command: Map Response:	>**svcntrl query 6136671021 csmi status** **Failure - Unavailable_Resources** (This response is when the service CSMI is not subscribed on the DN)

2.5 OSSGate Interface Changes

2.5.1 XML Command Changes

N/A

2.5.1.1 Command XML

N/A

2.5.1.2 Response XML

N/A

2.5.2 Additional OSSGate Changes

Through this feature, the CI command, SVCNTRL is made accessible through OSSGate. For more information about SVCNTRL, see the section "Command: SVCNTRL."

2.6 Security

2.6.1 Network configuration

2.6.2 Key management

2.6.3 Protocol

2.6.4 Authentication

2.7 Configuration Walkthrough

The following are the configuration steps for CS2K:

a. Enable CI SOC on the core. The SOC needs to be turned on for the query and update commands to function.

b. Enable the SDM telnet session. This is necessary in order to make the interface to the core active.

c. For CS2K, enable the OSSGATE telnet session to enable provisioning.

d. For TDM, there should be a direct telnet connection from the 3rd party provisioning server to the core.

Ensure that telnet is enabled throughout the session.

Product = CS 2000

A00012001 -- IEMS Call Server 2000 SIP Integration

Functional Description

Note: All screen shots captured in this version are draft documents, and this document will be updated when the official versions are complete.

1: Applicable Solution(s)

UA-IP

1.1 SN07/SN08 Background

In SN07&8, IEMS manages the Multimedia Communication Server Manager (MCS Manager). The MCS Manager when added can have as its managing type either an MCS/CSE MX NE or Media Proxy NE. When an MCS Manager is added to they IEMS, the MCS/CSE MX NE or Media Proxy NE is added as a map symbol under the Network Elements. The MCS System Manager is added as an element in the Element Managers map.

Along with the configuration of the MCS device was the ability to associate Fault Performance Managers, FPM's, to an MCS device which would be another input for faults and performance data for IEMS.

There were provisions for fault, performance, and configuration management of MCS and FPM devices.

The current existing MCS device functionality along with the RTP Media Proxy and FPM will continue to be supported in SN09.

To see more information concerning the addition of the MCS device in SN08, please see document SN08 A00007346 - Backward Compatibility Functional Specification.

1.2 Main work Items

One of the first items is branding name changes for both the NGSS and MCS. The existing NGSS managed object to align with the Call Server 2000 Session Server. The Trunks version is relabelled to SSTrunks. The MCS SIP lines which is now deployed on a Linux platform will be relabelled SSLines.

The MCS configuration and management remains the same from SN08 to SN09. The Icon for the MCS on the Solaris platform for the NE will be modified to MC52 and the tree name will be changed from MCS/CSE to MCS5200. Also, a change is made in the configuration of the MCS Mgr as an EM with a type from Media *Proxy* to Media *Portal.*

Integrating the management of the fault and performance interfaces of the new SSLines platform, Langley hardware running Linux OS. The SSLines system will also have the ability to configure the Session Manager platforms associated with the System Manager EM. There will also need to be configuration of the Provisioning Client servers. The configuration of the Session Managers will allow SSH launch to each Session Manager. The configuration of the Provisioning Client servers will allow the client to launch the MCS Provisioning Client.

Another work item consists of proxying all GUI/CLUI launches through the IEMS. The GUI/CLUI's that require proxying consist of:

- MCS System Manager Console
- Provisioning GUI
- SSH to each platform associated with the SSLines deployment

The SSLines Element Manager and Network Element will provide and support all the existing functionality of the MCS/RTP Media Portal functionality pertaining to Fault Management, Performance collection, and device change management. There will however only be the option of being able to add the SSLines device as an SSLines Manager without the ability to configure the SSLines device as an RTP Media Portal. Also in SN09, the SSLines device will not be supporting FPM's.

To configure performance collection jobs, please refer to the SN08 document concerning MCS.

1.3 Existing functionality

As specified previously this activity is for rebranding and proxying the MCS GUI's through the IEMS. The functionality of handling faults and provisioning data remains unchanged.

The change and deletion of an SSLines type device has remained the same except for the type being deleted or changed.

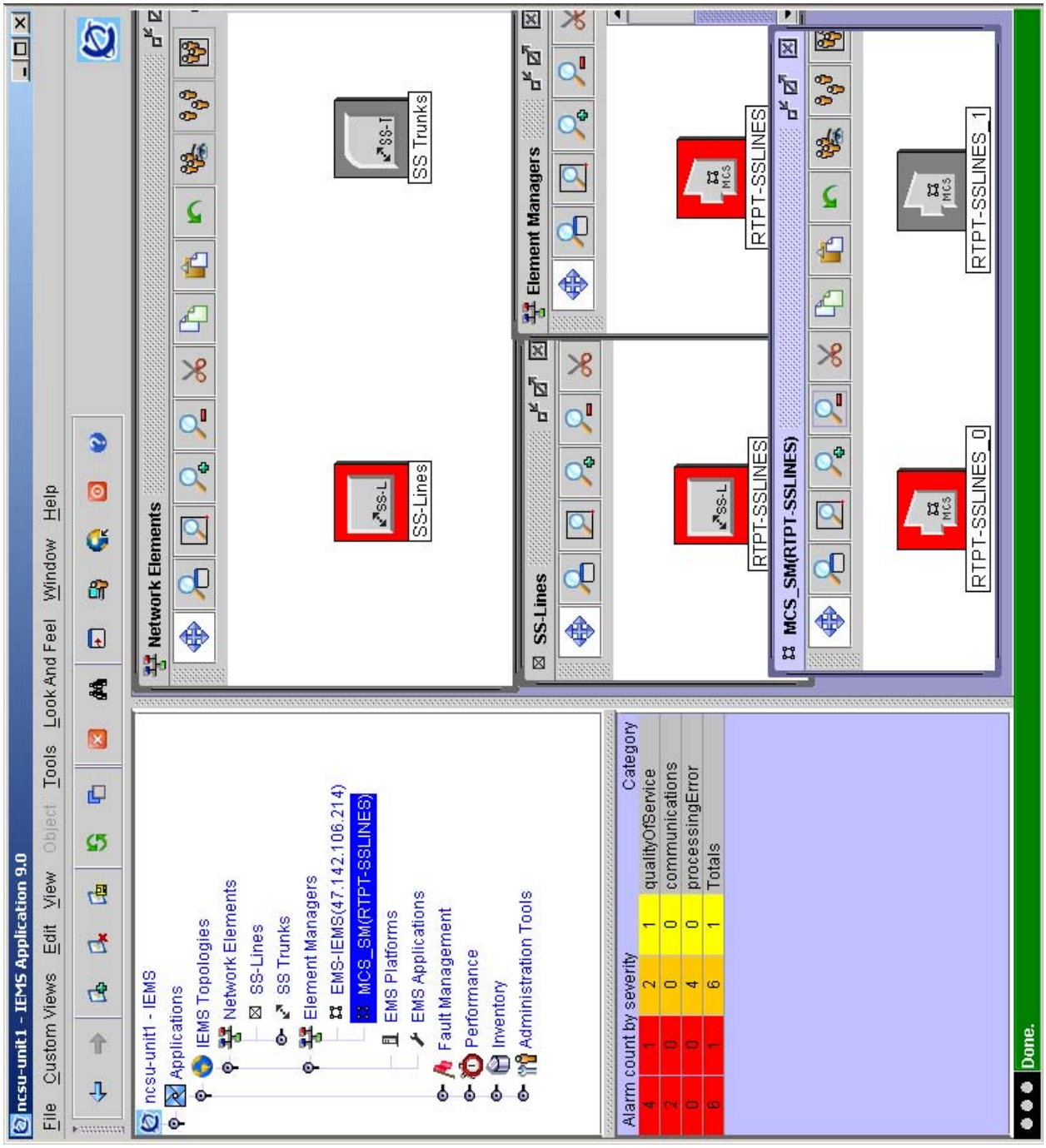
1.4 Changed Functionality

First and foremost is the branding change. When adding the SSLines device, an SSLines Mgr is added instead of an MCS Mgr or RTP Media Portal. The same information is entered concerning IP addresses, userids, SNMP information, and performance data collection.

1.4.1 Topology

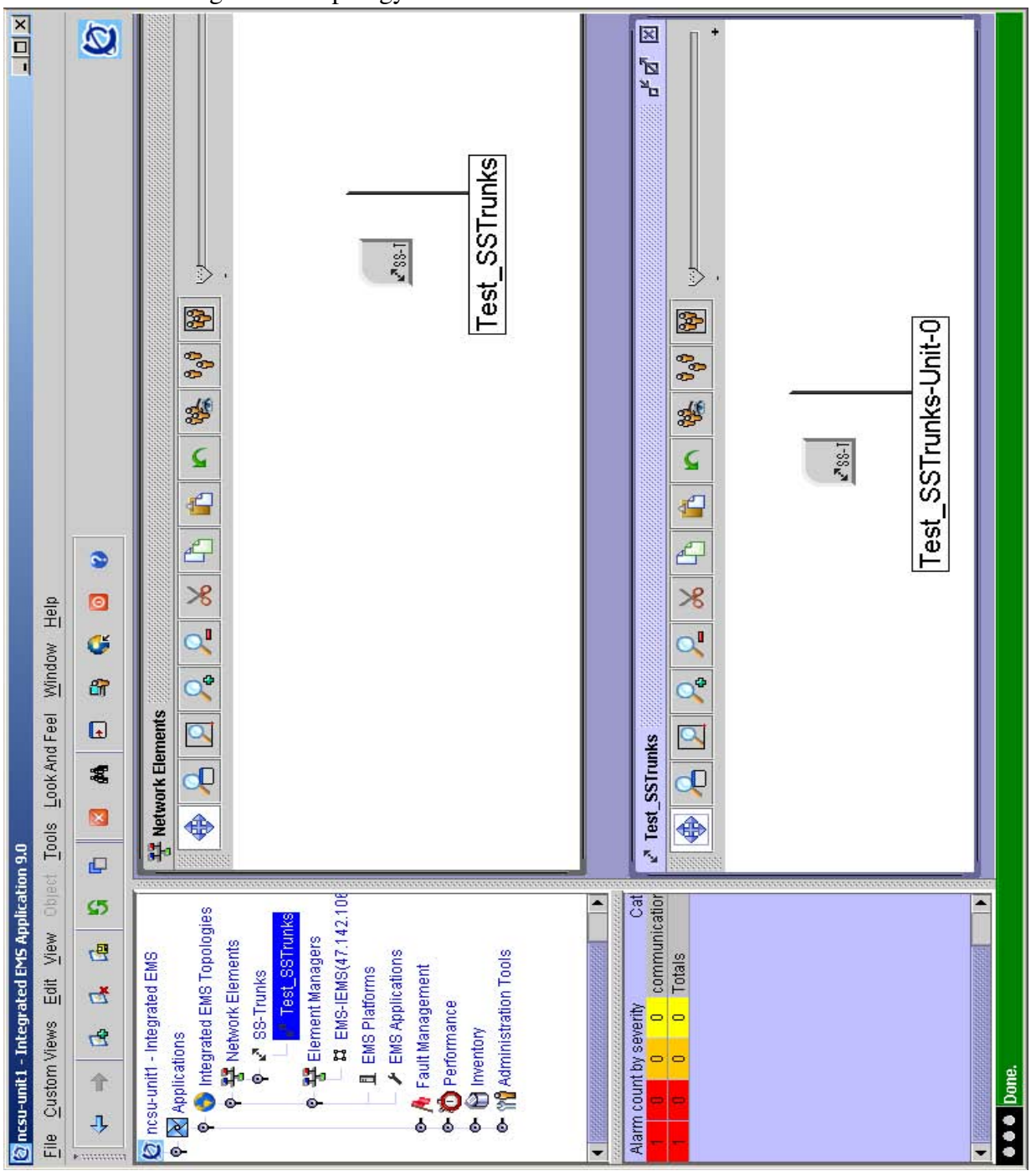
The topology of an SSLines as added into IEMS is displayed is in the same hierarchy as the existing SN08 MCS. The following screen shot shows the new branding and topology for the SN09 SSLines.

Figure 1 Topology of SSLines EM and NE



The SS Trunks topology will be similar to that of the Session Server and will be displayed as follows in SN09.

Figure 2 Topology of SS Trunks NE



1.4.2 Launch of applications

The launch of a command line has been modified in that it is now possible to launch a command line to any platform that is configured. When launch command line is selected, and new frame will be displayed which will allow the user to select the platform to launch a command line to. The launch of the command line for the System Manager and Session managers can be done from any of the maps in the GUI except from the Network Elements screen.

Figure 3 Launch of Command line From SSLines

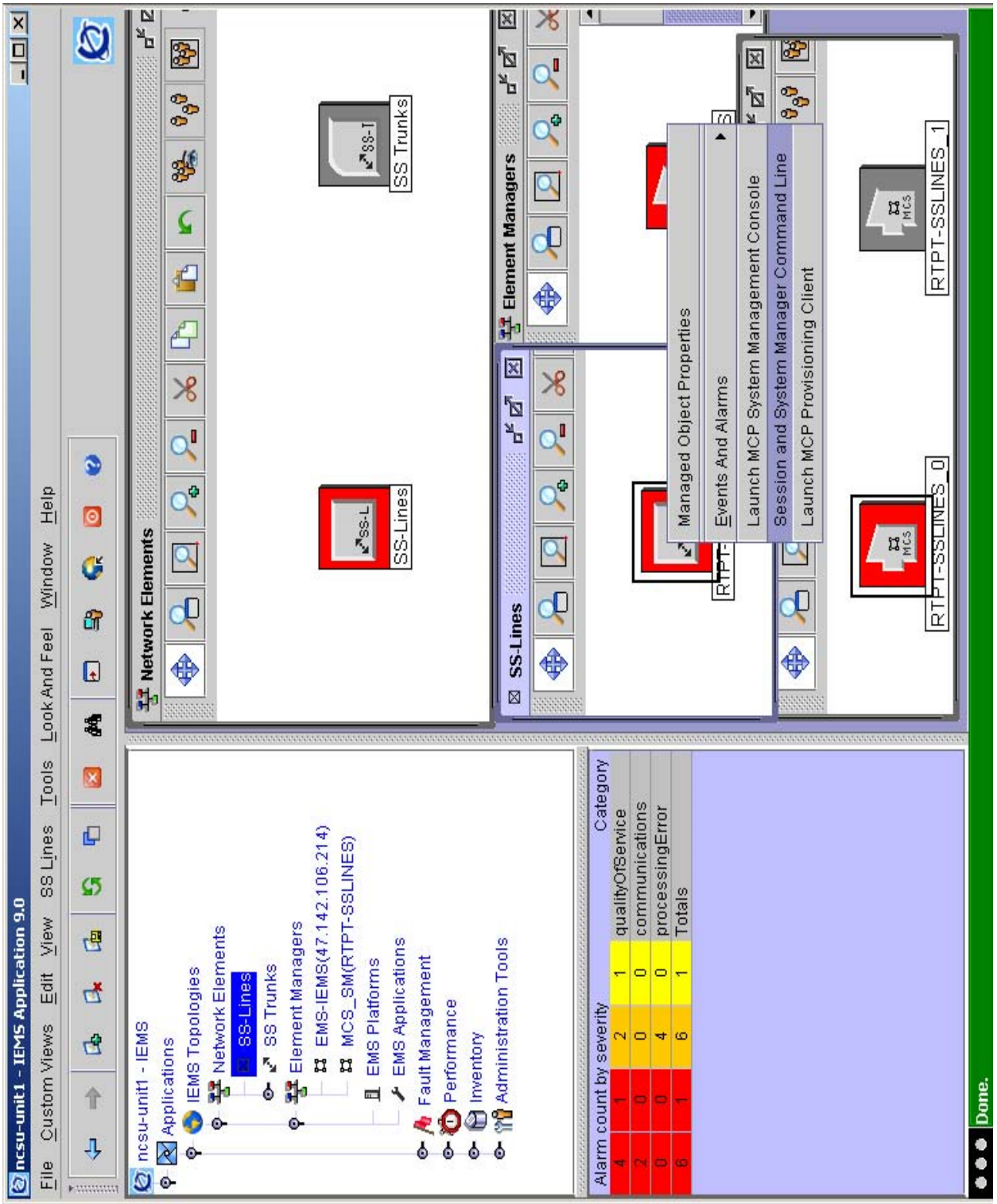


Figure 4 Launch of SSH command line to platform

The drop down box will allow the user to choose any of the platforms that SSH can be launched to. The SSH connections will be proxied via the IEMS server.There will be a new option against the EM to configure the platforms which will allow the user to configure these platforms.

1.5 New Functionality

1.5.1 GUI

For SN08, it was only possible to configure the platform(s) associated with the System Manager associated with an MCS or RTP Media Portal. In SN09, it is possible to configure all the platforms associated with an MCS/SSLines deployment including the IP addresses of

- The Provisioning Clients (two IP addresses)
- The Session Manager platform IP addresses (up to three pairs)

This configuration is done from the map reference of the SSLines EM.

From the EM or NE it is possible to launch the Provisioning client GUI.

Figure 5 Launch of Provisioning Client from EM Map

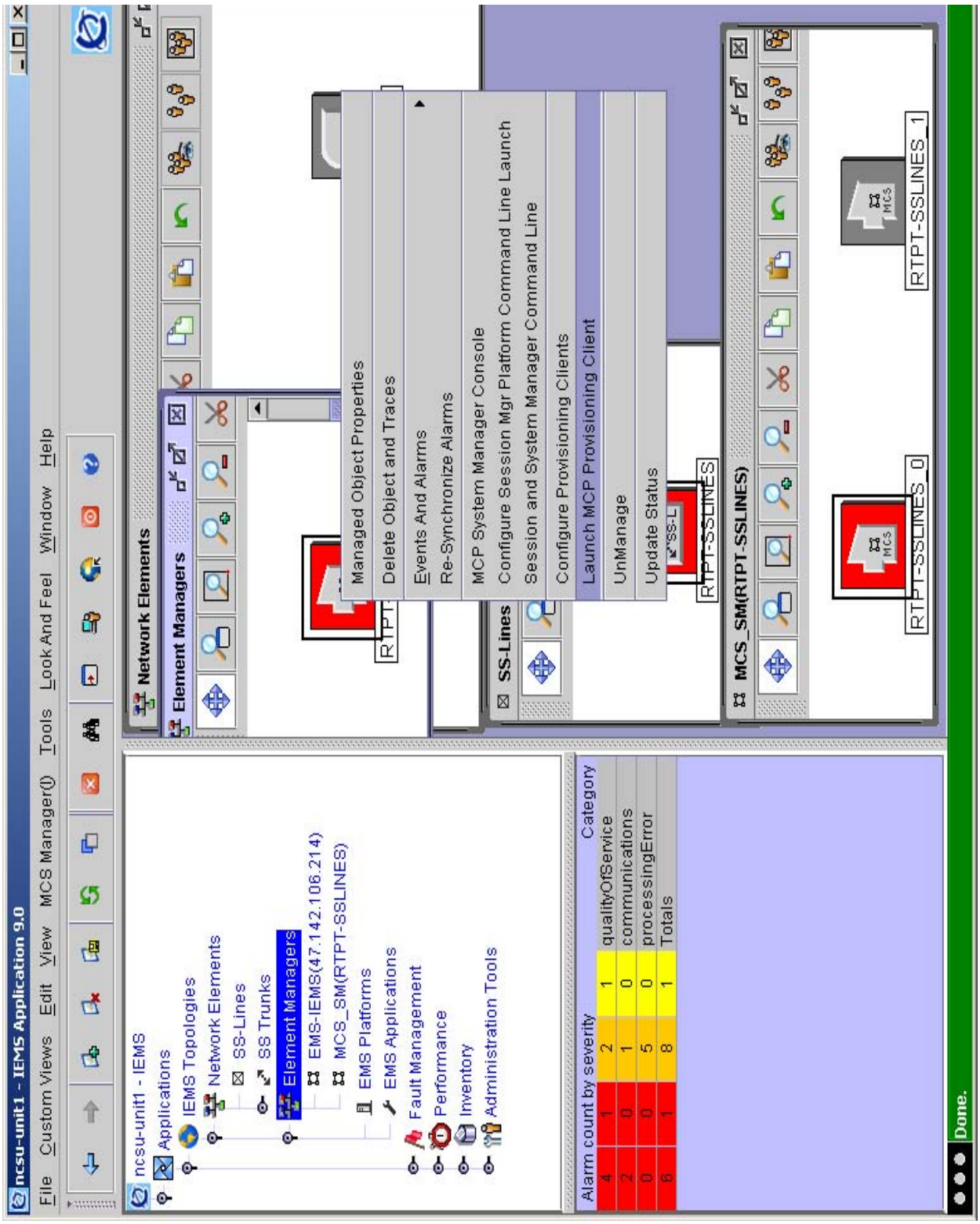


Figure 6 Launch from SSLines Element Manager Map

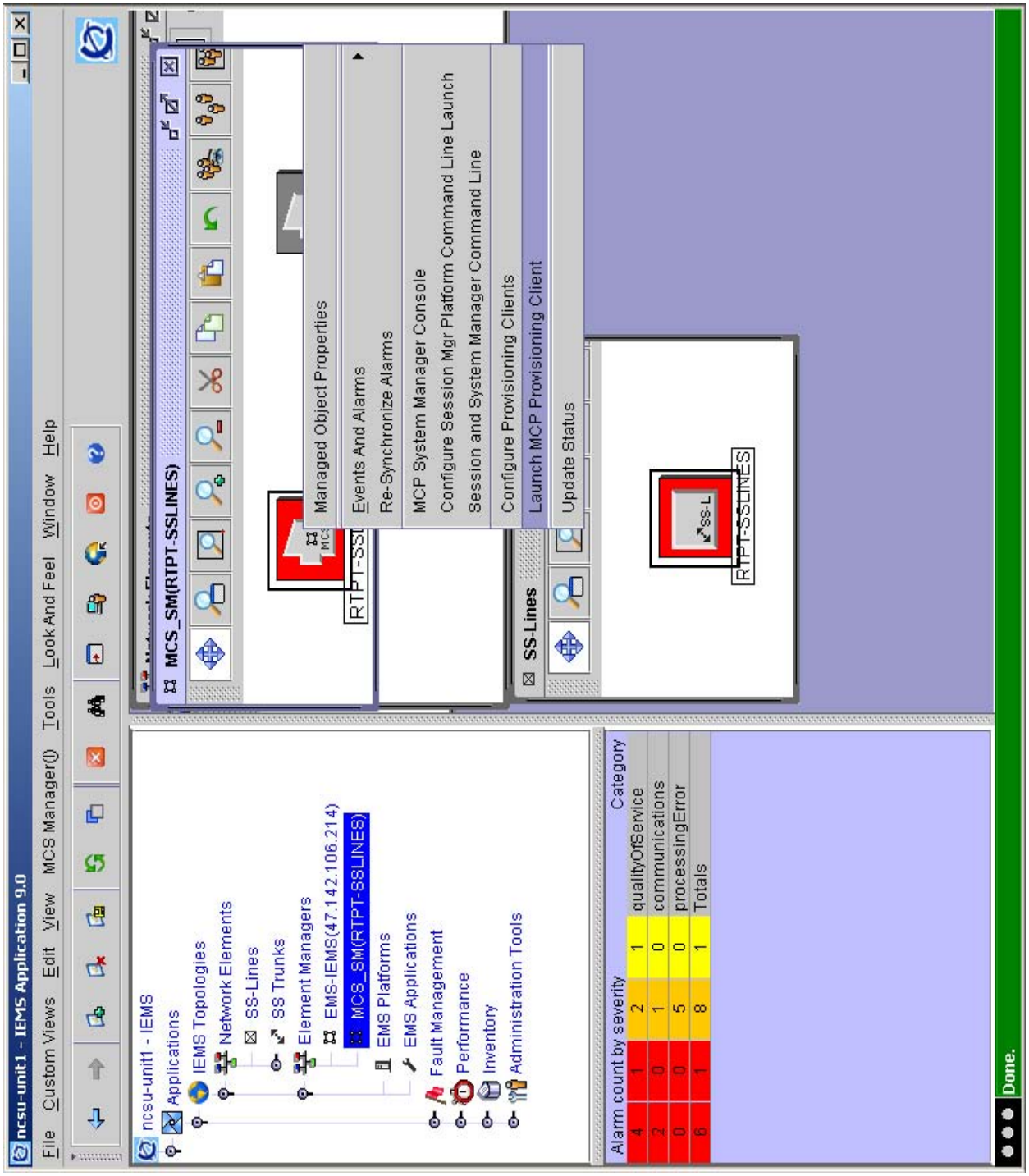
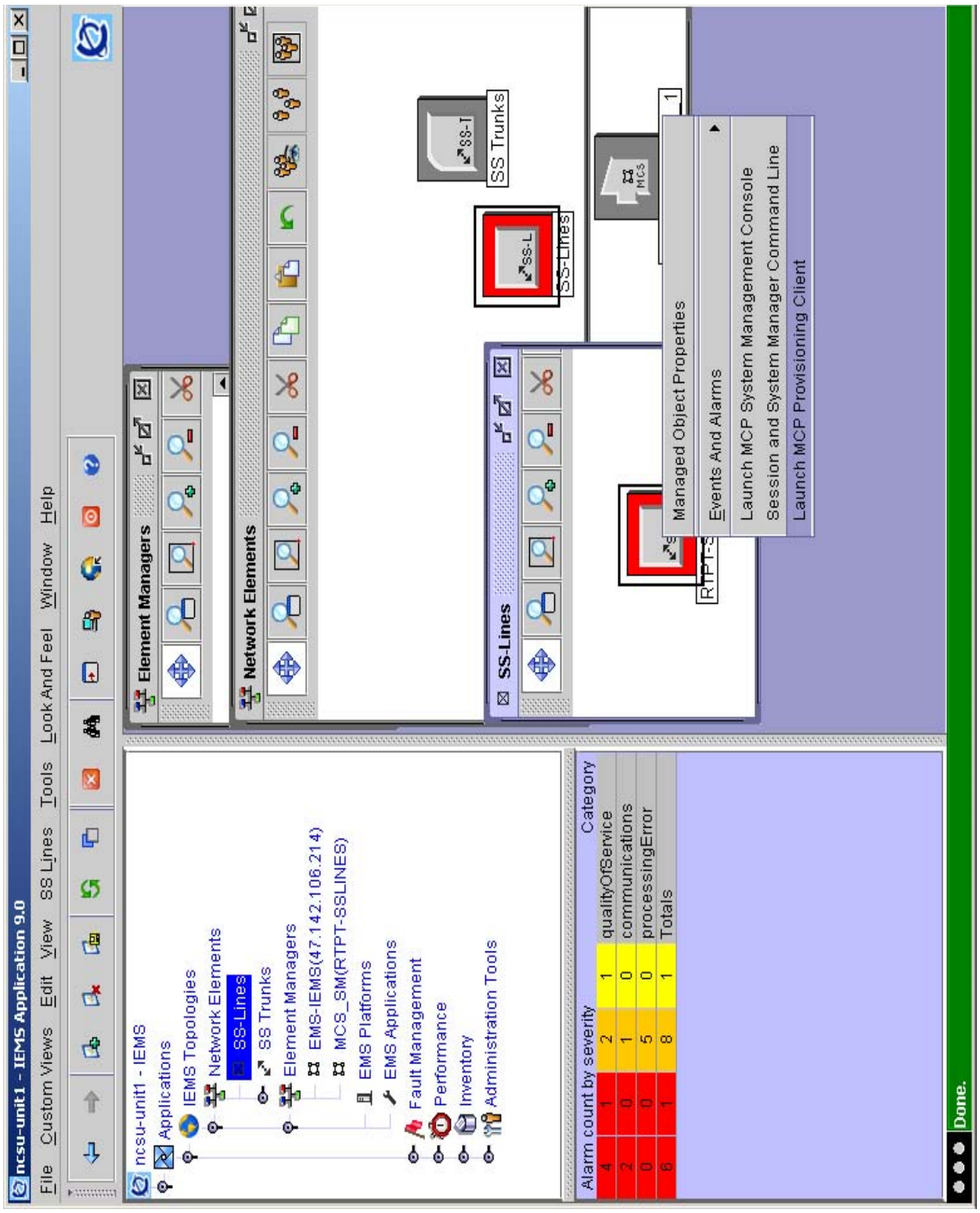
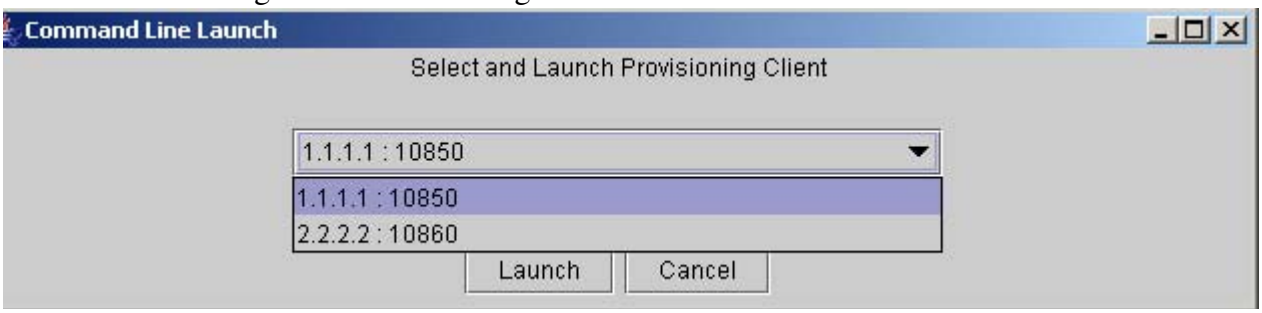


Figure 7 Launch of Provisioning Client from SSLines NE Map



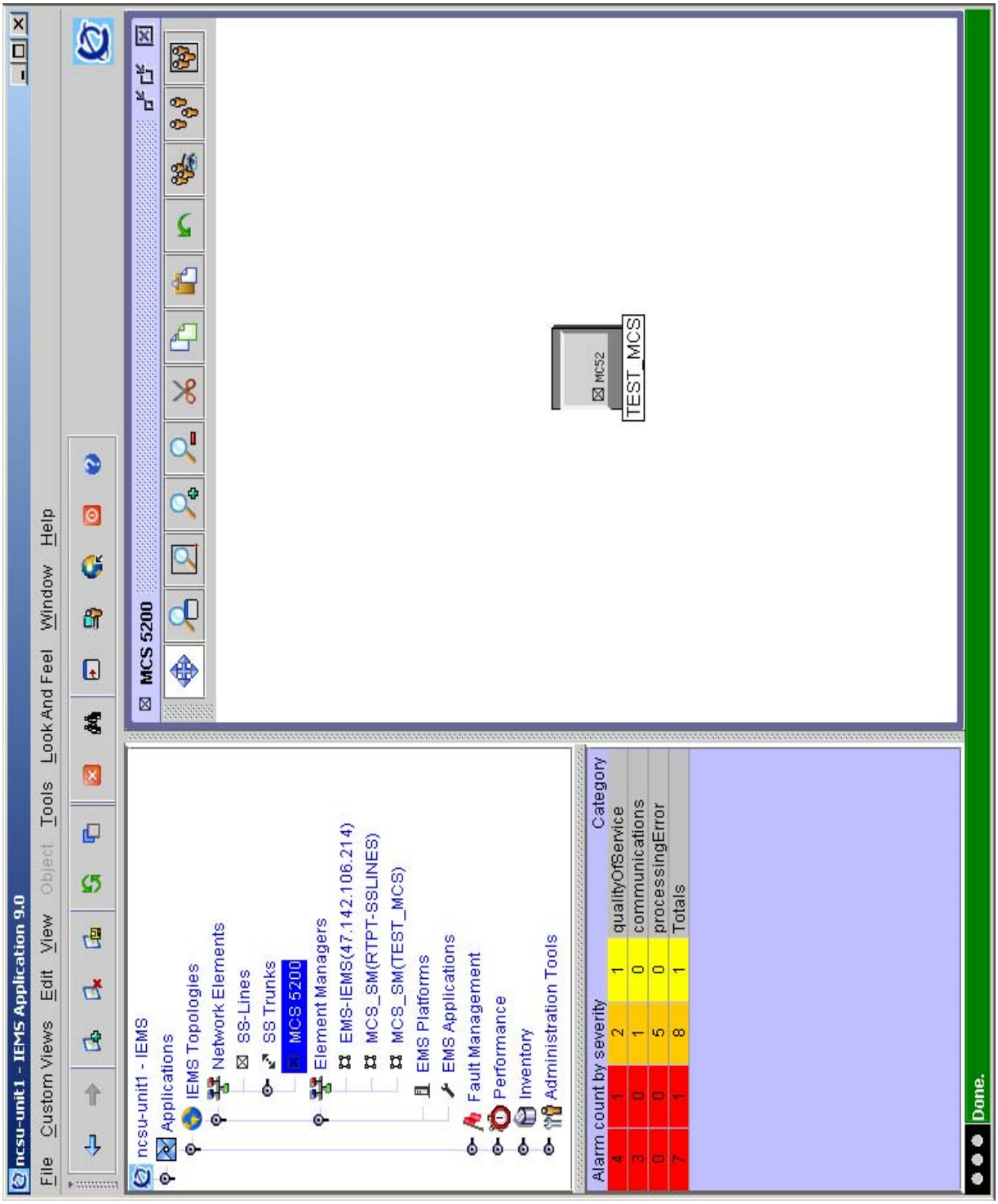
In all cases of lauching the Provisioning Client, there will be a combo dialog displayed which will have the user choose which platform to launch the Provisioning Client to as following.

Figure 8 Provisioning Client Launch



The Topology is changed somewhat for the MCS as an MCS/CSE device in the tree display to the following.

Figure 9 MCS MCS/CSE rebranded to MCS 5200



1.5.2 Proxy of MCS system manager and Provisioning client

As mentioned earlier, the MCS system manager console and provisioing client will be launched via the HTTP proxy. Both GUIs communicate with their servers via HTTPS. The apache proxy must be configured using the SSPFS CLI command. These details will be specified in the CN section.

No new ports will need to be opened on the firewall for this component.

1.6 Upgrade Considerations

1.6.1 Upgrade

For an upgrade the SSLines and SSTrunks configuration will be stored in the Oracle database as well as the faults and performance data and will be handled with the database upgrade.

1.6.2 Downgrade

For an upgrade the SSLines and SSTrunks configuration will be stored in the Oracle database as well as the faults and performance data and will be handled with the database downgrade.

1.7 Security

N/A

1.8 Hardware Requirements or Dependencies

This feature requires the SIP Lines componenets to reside on the Langley Linux platform.

1.9 Software Requirements or Dependencies

This will require an SN09 or later version of SSPFS.

1.10 Limitations and restrictions

Log streaming and bulk import and export will not be supported for the proxied system manager launch.

1.11 Interactions

N/A.

1.12 Glossary

Term	Description
IEMS	Integrated Element Management System

2: Configuration for A00012001

Note: All screen shots captured in this version are draft documents, and this document will be updated when the official versions are complete.

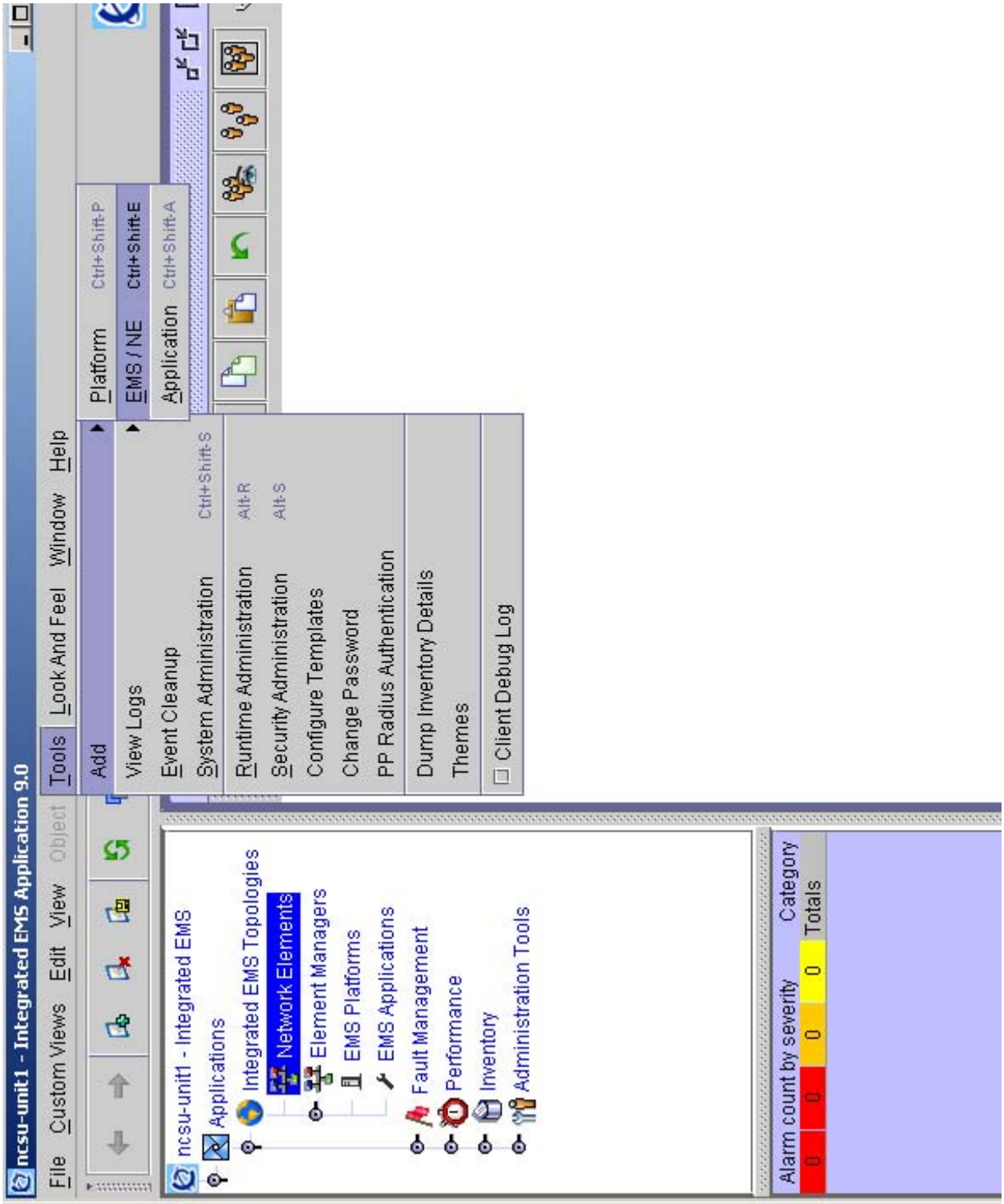
2.1 Hardware and Software Requirements

The feature requires IEMS to be installed on SN10 or later SSPFS loads.

2.2 Addition of an SSLines Mgr

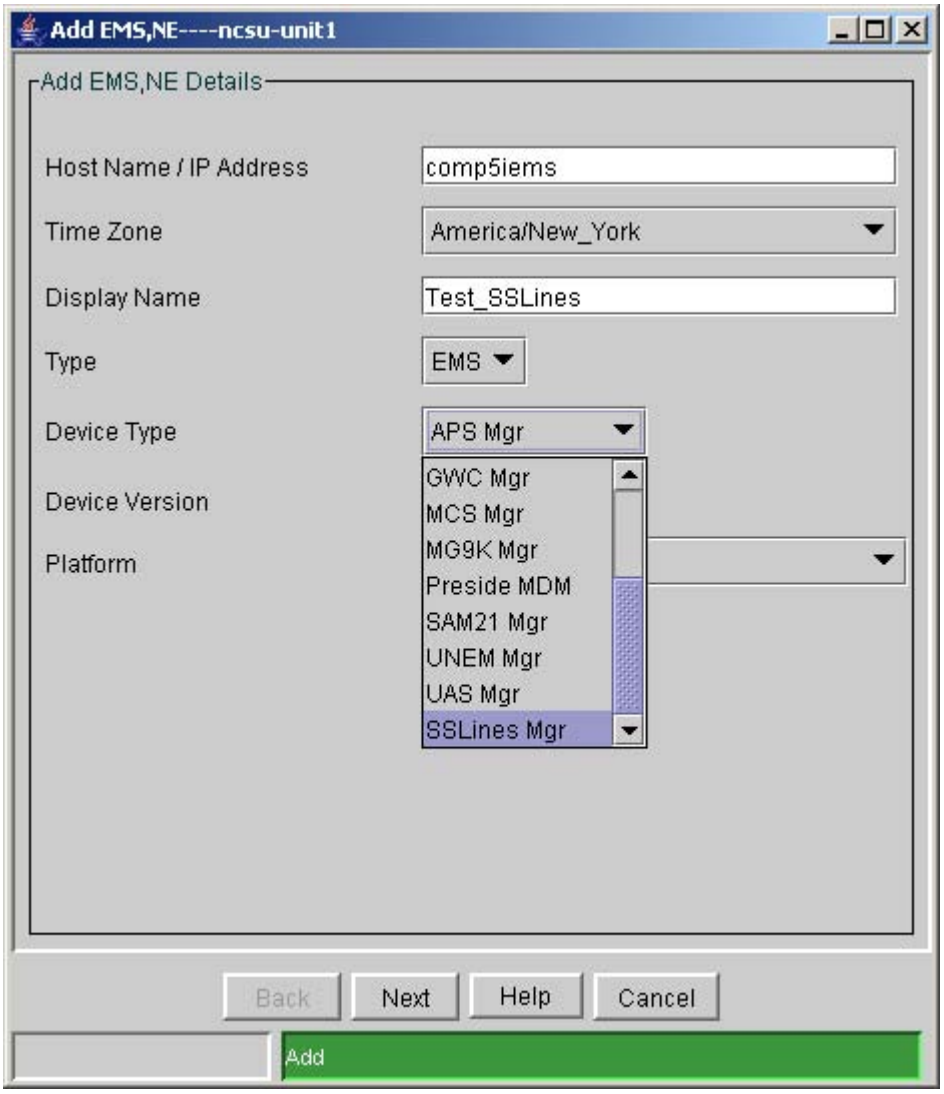
The SSLines configuration is similar to that of the MCS Mgr device in SN08, only shown here is the configuration of the first panel as all the other components are the same.

Figure 1 Getting add panel



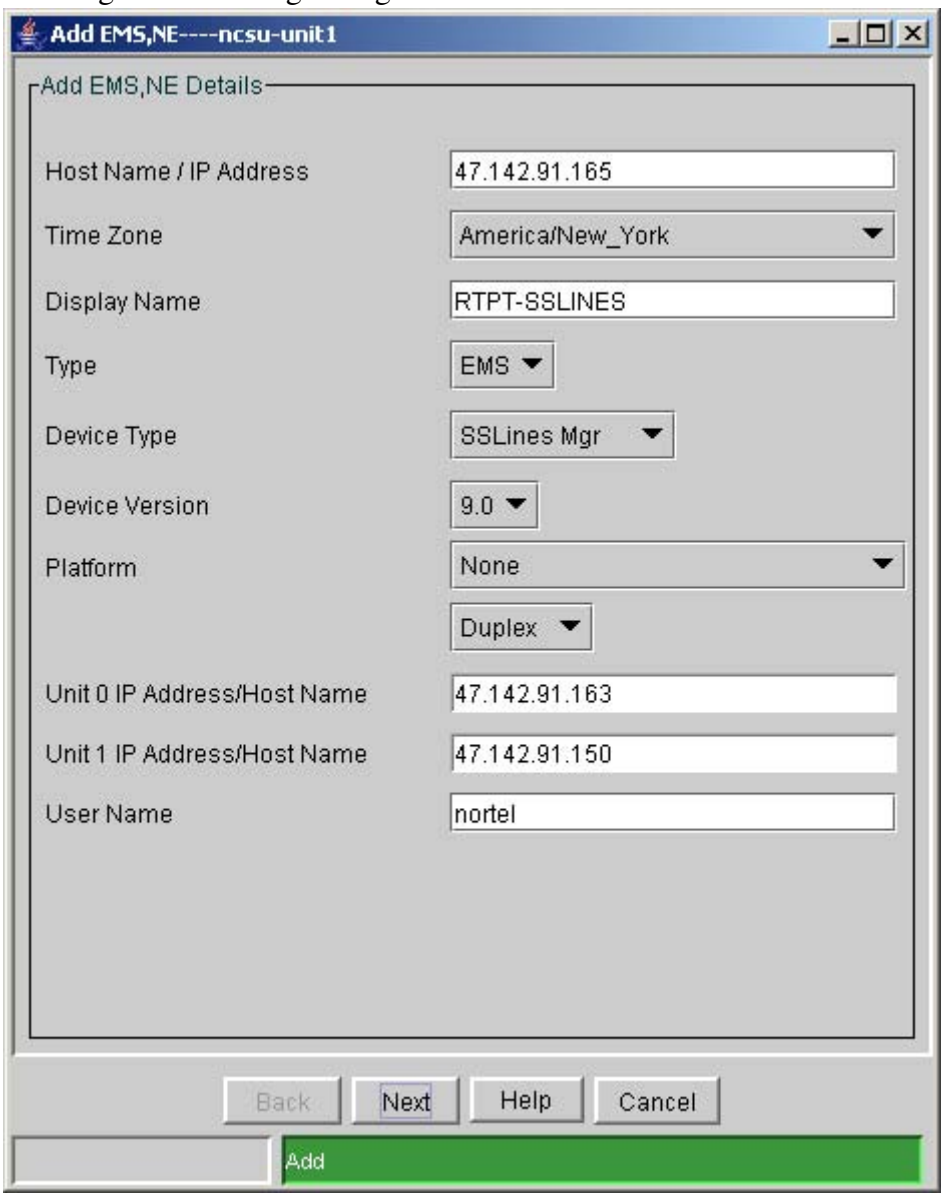
From this add panel, the SSLines option must be chosen.

Figure 2 Selecting SSLines Mgr



After this, the IP addresses for the System Manager platform and username are entered as follows. As shown below, the default is duplex for the SSLines or SIP lines on the Langley hardware.

Figure 3 Setting configuration data.



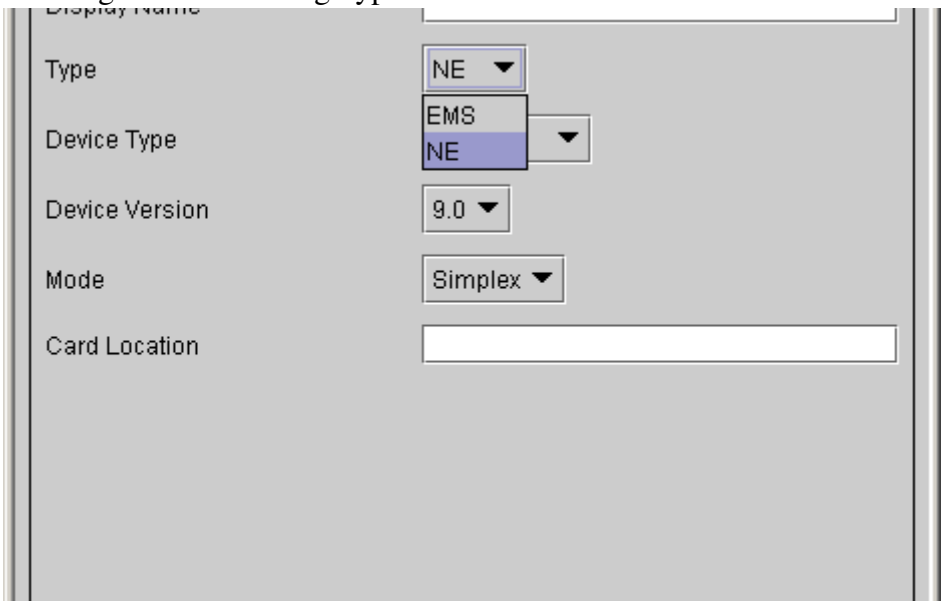
The other configuration screens are configured like the MCS Mgr configuration in SN08. Please see the SN08 documentation for those references.

2.3 Addition of an SSTrunks NE

The SSTrunks is the SN10 rebranded name of the Session Server. Following is a screen shot of the add panel. All SN08 configuration parameters are present in the SN10 version.

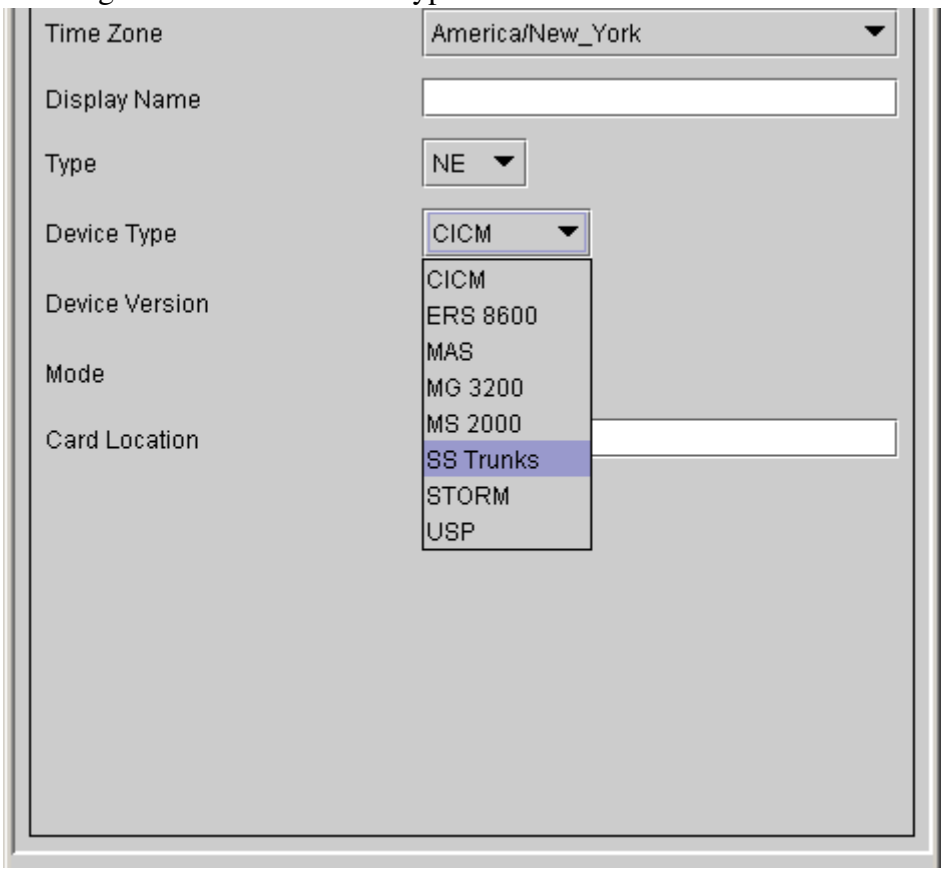
After the add node is selected, select Type as NE

Figure 4 Selecting Type as NE



Then the Device Type of SS Trunks is chosen:

Figure 5 Select Device Type of SS Trunks

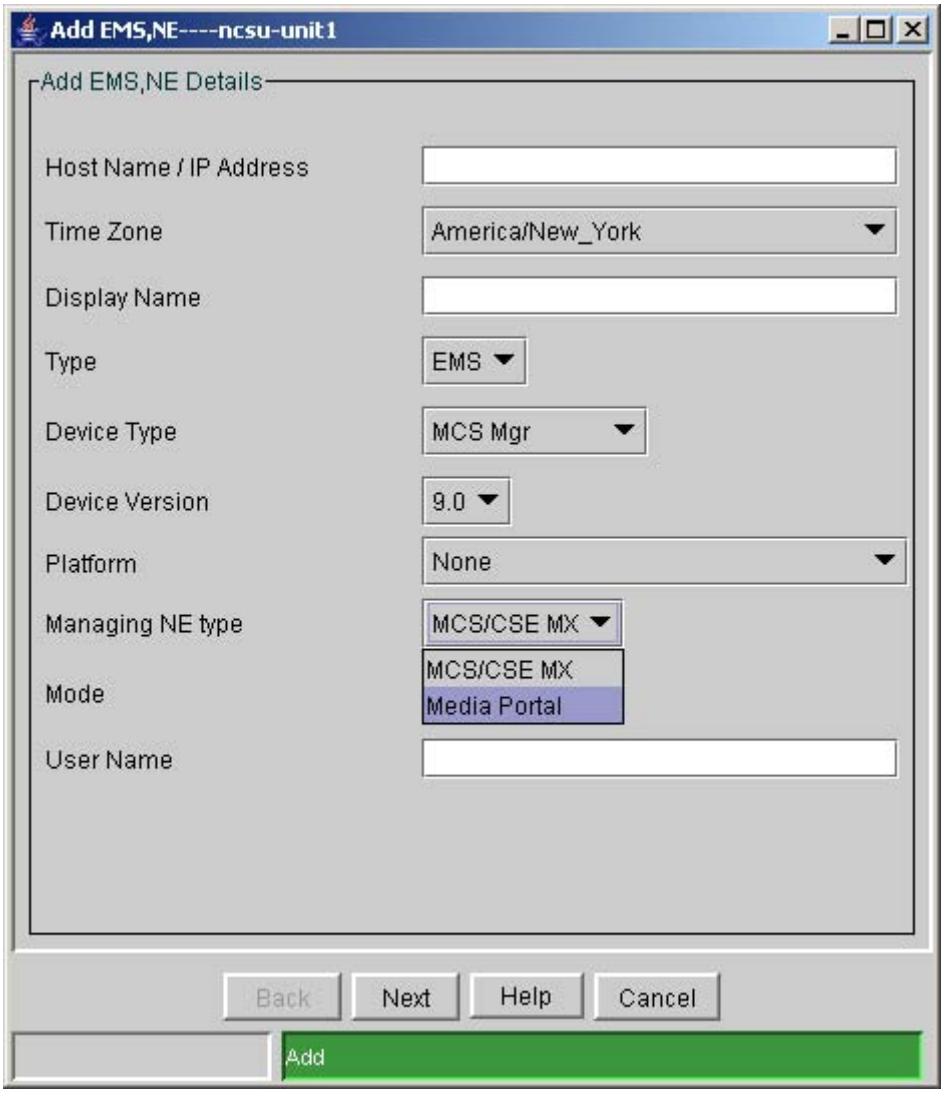


All configuration after the Device Type is chose is the same as SN08, please see the SN08 documentation for details.

2.4 Change of configuration for Media Proxy to Media Portal

The Media Proxy NE type has been changed to Media Portal as shown below.

Figure 6 Addition of MCS with Media Portal as NE



2.5 Configuring Session Managers for SSH launch

There is a requirement to be able to launch SSH directly to the Session Managers. To fulfill this requirement a new option needs to be added to allow the configuration of these Session Managers. This new option will be allowed from the EM in the MAP for SSLines.

Figure 7 Example launch of configure session manager

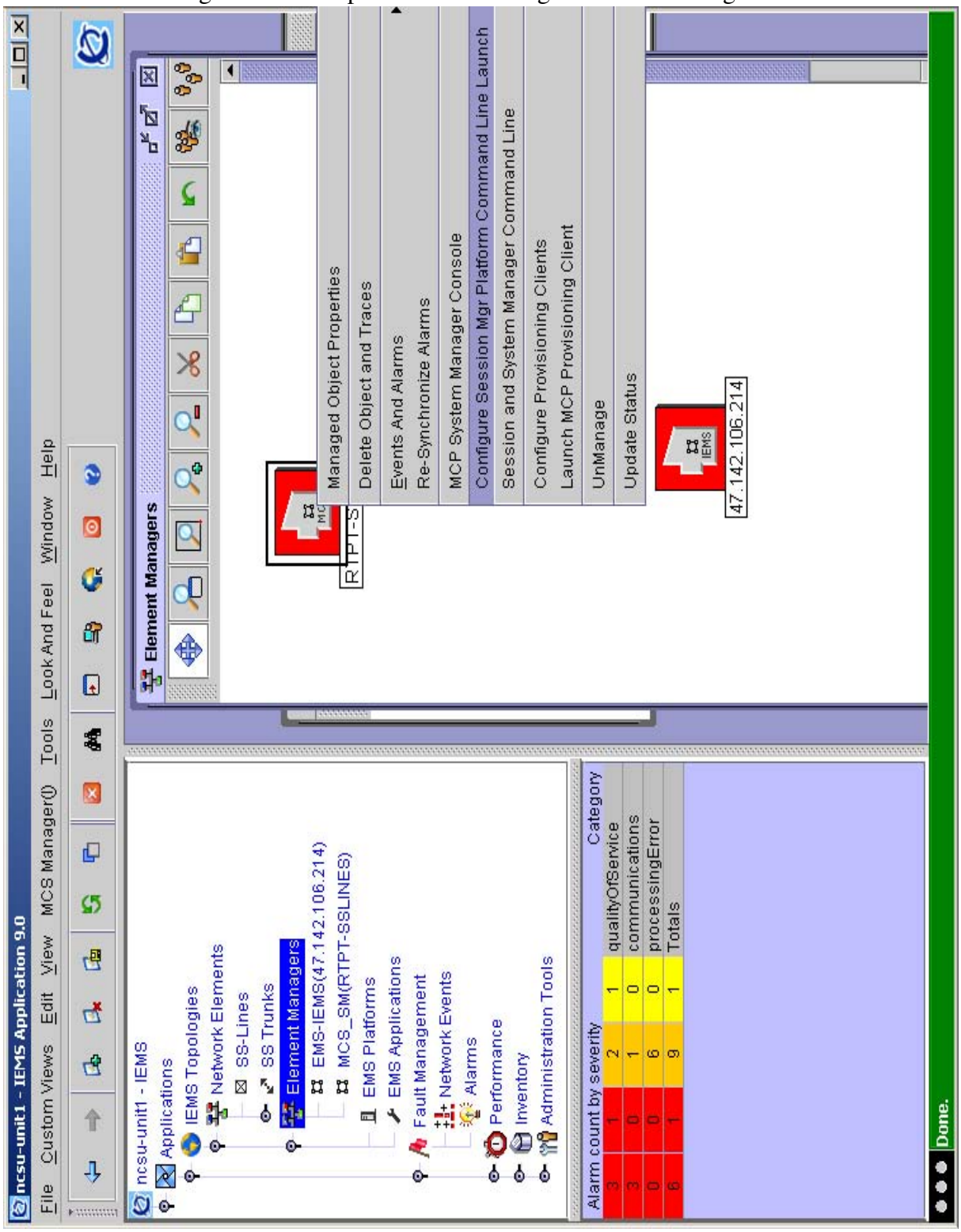


Figure 8 Or from MCS_SM map view

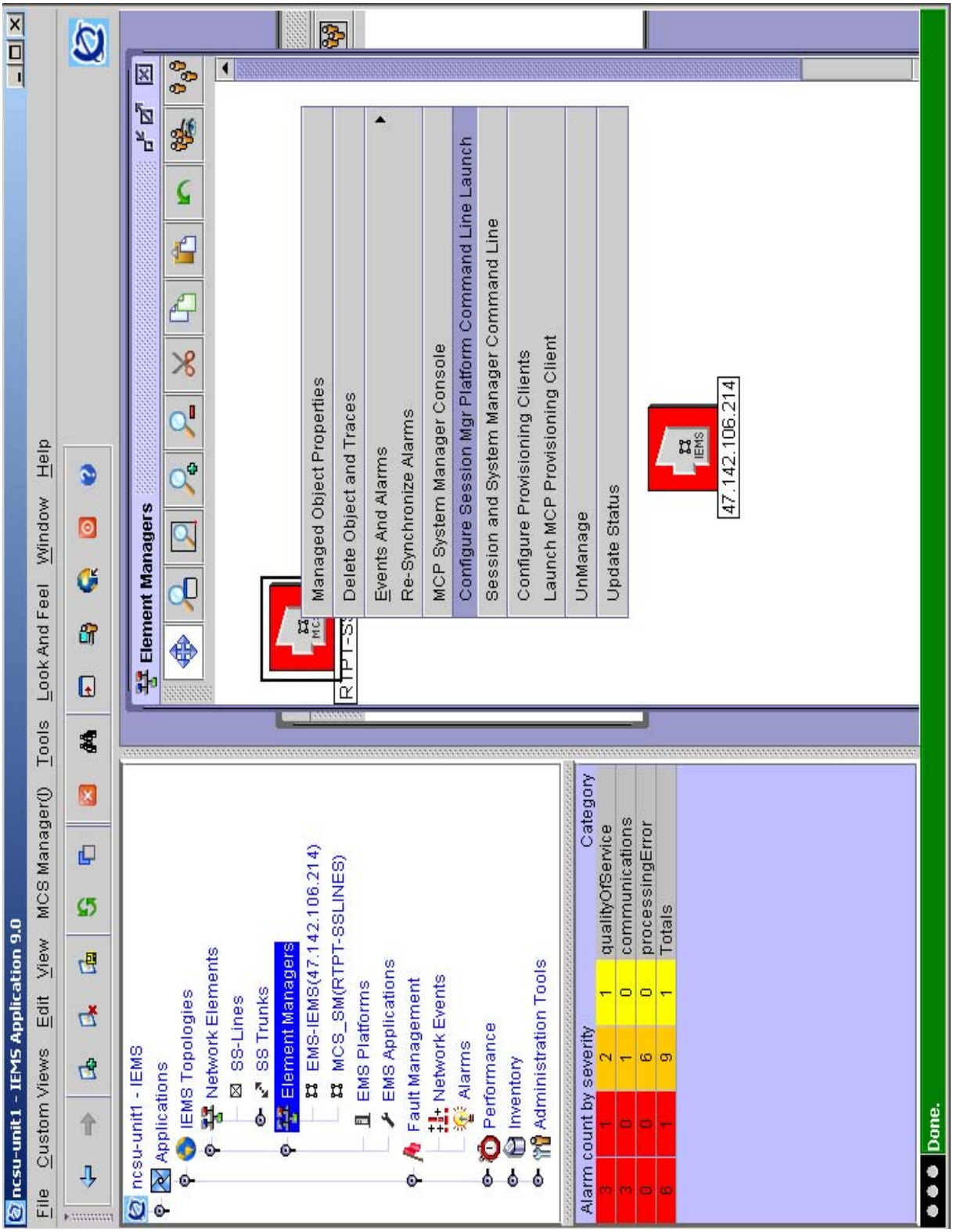
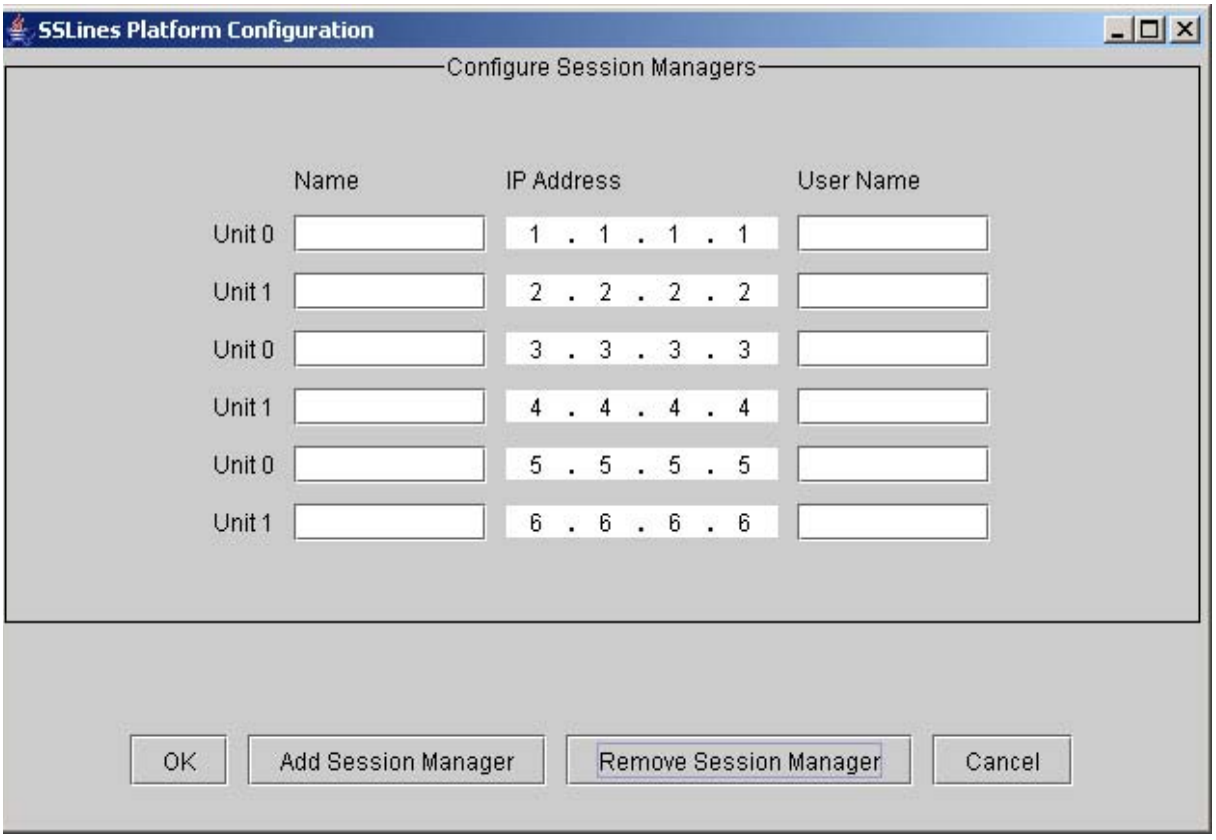


Figure 9 Configuring session managers that can have SSH launched to them



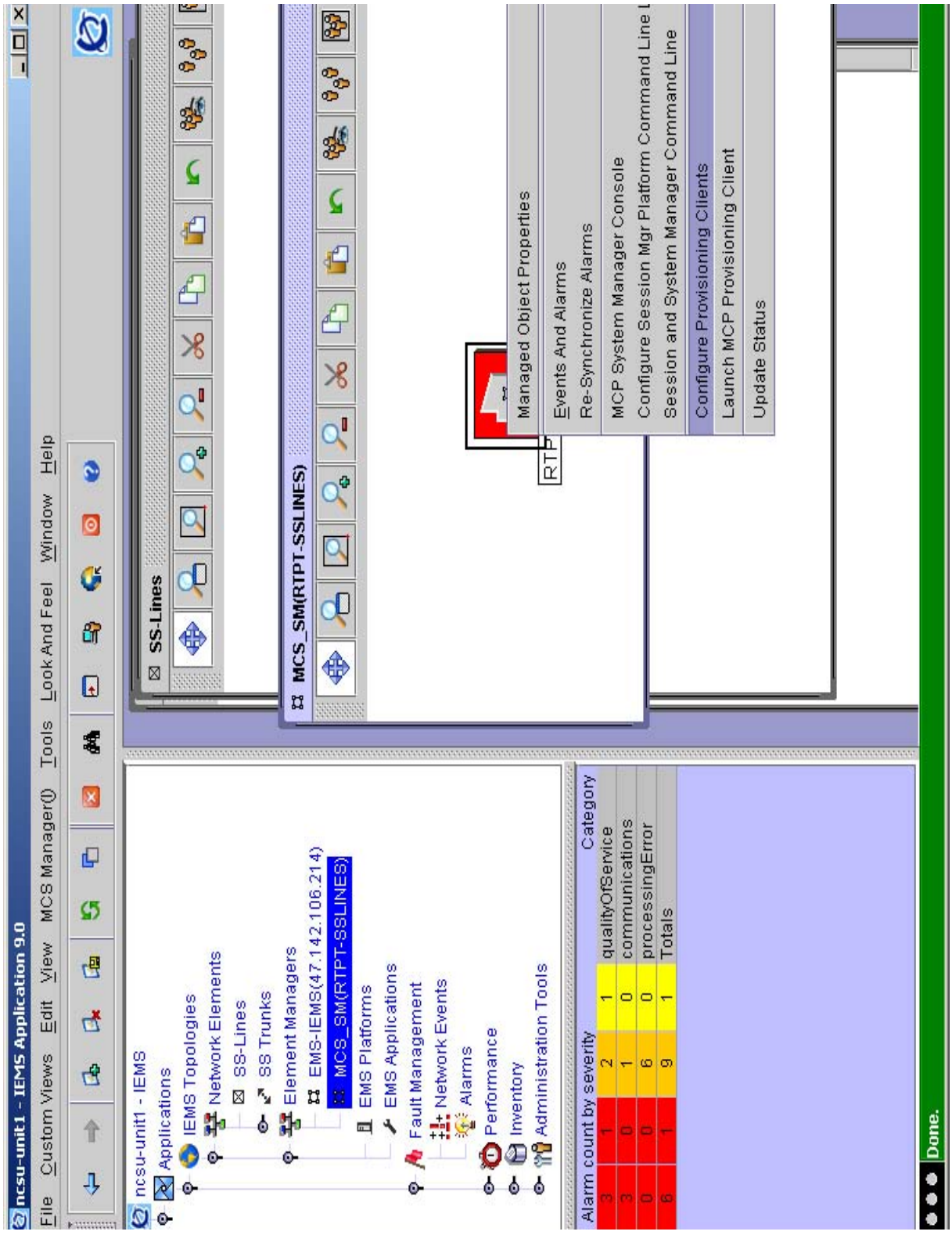
As noticed there can be 3 Session Manager pairs configured. This is a fully configured deployment.

The Add Session Manager and Remove Session Manager adds and removes a pair from the configuration screen. Only the Session Managers that are configured will be configured in the IEMS database.

2.6 Configuring Session Managers for SSH launch

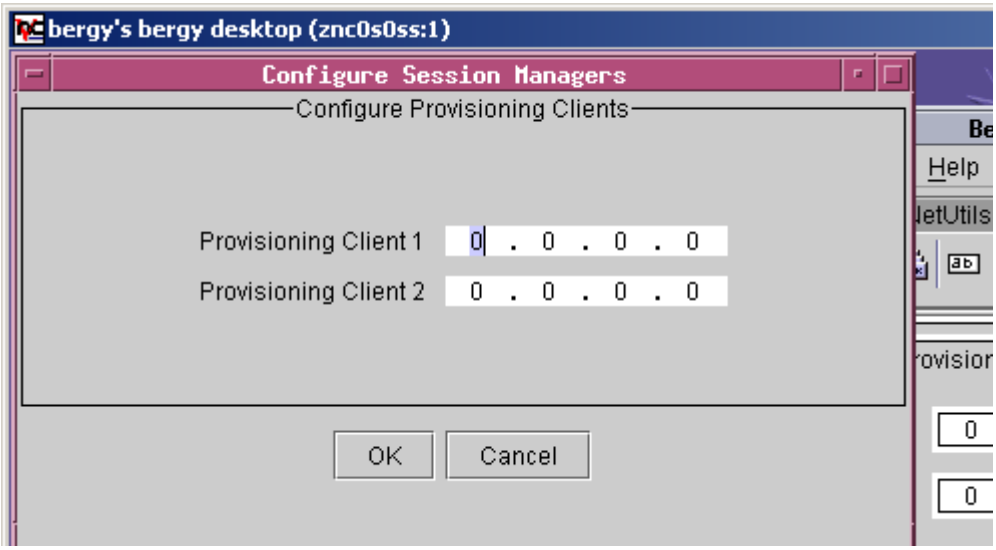
There is a requirement to be able to launch the Provisioning Client wherever they are running on the Sip lines deployment. To fulfill this requirement a new option needs to be added to allow the configuration of the IP addresses of where the provisioing servers are running. This new option will be allowed from the EM in the MAP for SSLines. These are not duplex or clustered.

Figure 10 Example launch of configuring Provisioning Client



The configuration of the provision clients can be done from either the MCS_SM map or from the Element Managers Map. Until the configuration is done, the provisioning clients cannot be launched.

Figure 11 Configuring Provisioning Clients for later launch



After the configuration the following dialog will be displayed.As the dialog indicates the WEBSERVER requires a restart prior to launching the provisioning client.The commands on the sspfs to restart the WEBSERVER is

servrestart WEBSERVER

Figure 12 Restart WEBSERVER dialog

2.7 Configuring the apache proxy using CLI

The apache webserver on the IEMS server machine must be configured to proxy https communication between the SSLines manager and its client and also between the povisioning webservers and the provisioning client. Both will be configured using the SSPFS cli tool.

The proxy configuration must be manually removed when the SSL lines platform is deprovisioned from IEMS.

Provisioning client proxy

An entry is required for each proisioning webserver IP. This the provsioning IP entered in the “SSL Lines Platform Configuration” frame in section 12.5.

Procedure (adding an entry):

1. Login into the IEMS server box as root and invoke the “cli” command:

#cli

Select option 2 (Configuration), then option 2 (Apache Proxy Configurration), then option 1 (add_proxy_conf).

2. Configure the proxy as shown below:

When prompted for the proxy IP address enter the address of the provisioning webserver.

When prompted for the “hostname/tag associated the IP” again enter the address of the provisioning web server.

When propmpted for the optional remote hostname/tag , leave blank and hit “Enter”

When prompted for the port number enter the value “8443”

Answer “Y” when prompted to restart the Apache server.

Repeat the steps above for the other provisioning client IP address.

The session below shows the proxy configuration for provisioning web server at IP address 47.142.23.24:

 # cli

Command Line Interface

1 - View

2 - Configuration

3 - Other

X - exit

select - 2

Configuration

1 - NTP Configuration

2 - Apache Proxy Configuration

3 - DCE Configuration

4 - OAMP Application Configuration

5 - CORBA Configuration

6 - IP Configuration

7 - DNS Configuration

8 - Syslog Configuration

9 - Database Configuration

10 - NFS Configuration

11 - Bootp Configuration

12 - Restricted Shell Configuration

13 - Security Services Configuration

14 - Login Session

15 - Location Configuration

16 - Cluster Configuration

17 - Succession Element Configuration

18 - snmp_poller (SNMP Poller Configuration)

19 - backup_config (Backup Configuration)

X - exit

select - 2

Apache Proxy Configuration

1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - 1

=== Executing "add_proxy_conf"

Enter proxy IP address (X to exit): 47.142.23.24
Enter hostname/tag associated with IP 47.142.23.24: 47.142.23.24
Optional, enter remote hostname/tag associated with IP 47.142.23.24:
Enter port number [443]: 8443
Accept the following values:
IP Address = 47.142.23.24
Hostname = 47.142.23.24
Remote Tag =
Port Num = 8443
!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time
Continue? [Y/N]:Y
Stopping group using servstop
Apache Web Service Stopping
WEBSERVER Stopped

Starting WEBSERVER through servstart
Updated alarm successfully.
Found valid security certificate, starting Web Services with SSL support...
Apache Web Service Starting
WEBSERVER Started

=== "add_proxy_conf" completed successfully

Apache Proxy Configuration
1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - select - (X, 1-3) X

Procedure (removing an entry):

The procedure for removing a proxy entry is virtually identical to the procedure for adding an entry:

1. Login into the IEMS server box as root and invoke the “cli” command:

#cli

Select option 2 (Configuration), then option 2 (Apache Proxy Configurration), then option 1 (del_proxy_conf).

2. Delete the proxy entry by entering the provisioning IP address and port number when prompted.

The example session snippet below shows the IP address 47.142.24.23 being removed from the configuration:

Apache Proxy Configuration:

1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - 2

=== Executing "del_proxy_conf"

Enter proxy IP address (X to exit): 47.142.23.24

Optional, enter remote hostname/tag associated with IP 47.142.23.24:

Enter port number [443]: 8443

Accept the following values:

IP Address = 47.142.23.24

Remote Tag =

Port Num = 8443

!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time

Continue Removal? [Y/N]:

Enter proxy IP address (X to exit): 47.142.23.24

Optional, enter remote hostname/tag associated with IP 47.142.23.24:

Enter port number [443]: 8443

Accept the following values:

IP Address = 47.142.23.24

Remote Tag =

Port Num = 8443

!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time

Continue Removal? [Y/N]:Y

Stopping group using servstop

Apache Web Service Stopping

WEBSERVER Stopped

Starting WEBSERVER through servstart

Alarm exists, updating alarm...

ComponentID: CLASS=SEC;CLASSTYPE=EXPIRED;SUBTYPE=HTTPSCERT;FILE=validcert.ksh

Updated alarm successfully.

Found valid security certificate, starting Web Services with SSL support...

Apache Web Service Starting

WEBSERVER Started

=== "del_proxy_conf" completed successfully

SSLines Management console proxy:

The configuration for the SSLines management console is identical to the provisioning client configuration above except for the port number and IP address used:

- When prompted for proxy IP address, use the address on which the management server resides.
- Use 12121 for the port number.

Below is an example session snippet for configuring proxy for server on IP address 47.142.200.69:

Apache Proxy Configuration

1 - add_proxy_conf (Add an IP to the Apache Proxy Module configuration)

2 - del_proxy_conf (Delete an IP from the Apache Proxy Module configuration)

3 - list_proxy_conf (List the Apache Proxy Module configuration)

X - exit

select - 1

=== Executing "add_proxy_conf"

Enter proxy IP address (X to exit): 47.142.200.69

Enter hostname/tag associated with IP 47.142.200.69: 47.142.200.69

Optional, enter remote hostname/tag associated with IP 47.142.200.69:

Enter port number [443]: 12121

Accept the following values:

IP Address = 47.142.200.69

Hostname = 47.142.200.69

Remote Tag =

Port Num = 12121

!!WARNING!! This will result in WEBSERVER going down (restarting) for a short time

Continue? [Y/N]:Y

Product = CS 2000

A00012210 -- Geo OA&M Automatic Backup and Accelerated Restore

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

This Automatic Backup and Accelerated restore feature, henceforth referred to as "remote backup", will remotely backup all data on the “target” unit. This provides a standby backup system ready to provide service should the primary system or cluster be unavailable for an extended period of time (e.g., catastrophic site loss). The remote backup can assume the identity of the target system with data and files accurate to the last sync. This feature is driven by the geographic survivability configuration where the remote backup will be at a different site from the target system. Previous backup relied on physical media which needs to be transported between the primary and backup systems. Also, the media based restore requires a multistep restore process.

This feature performs the backup via TCP/IP connection and stores an exact copy on the standby server which can be quickly and remotely activated. The data is transferred via an encrypted ssh tunnel over the CS LAN. This remote backup copies all files in each file system marked for backup. This is the same behavior as a full system backup.

If the file system layout has not changed, the backup will transfer file differences since the last backup, a practice commonly referred to as an incremental backup. This is a built in feature of the open source rsync tool. By transferring only differences there are major savings in time and bandwidth.

A remote backup configuration tool is provided to set the necessary parameters and schedule for automatic backup. These backups can be scheduled to automatically occur from once a day to four times per day. Users will be able to enter up to four times of their choice for the automatic backup to occur. For example, "02:00", "06:00", "15:00" and "21:00". This tool also provides a

facility for manually initiating a backup and monitoring its progress. Each remote backup session will provide detailed logs of that session.

The standby server has an identical copy of files from the last backup, so it can become the primary system via changing the boot pointer and rebooting. When it boots it will have the IP address and all configuration as of the last backup.

When the primary site is again available, the remote backup feature can be reused to transfer current system configuration back to the primary site and system.

Following is a high level overview for OA&M recovery using the standby server:

1. Normal state: primary site is providing service and the standby site is automatically backing up data at the scheduled times.
2. Primary site goes down. Craft person can remotely login to the standby system and activate the standby backup system.
3. The standby system boots with the configuration and data from the primary site as of the last scheduled backup. Standby site provides service.
4. Sometime later the primary site is repaired. To transfer "current" data and setting from the standby to the primary site, a craft person at the primary site installs cluster unit0 as a remote backup system.
5. Craft person at the primary site performs a remote backup of the standby site.
6. Standby site can be remotely shutdown and primary site activated
7. Primary site should clone the other cluster unit to restore normal cluster operations.
8. Craft person at standby site will need to install the standby system for automatically backing up data. Once this is complete, everything is back to the normal state.

1.2 Hardware Requirements or Dependencies

The hardware of the standby server must match the primary server. This is especially important with regard to hard disk size. This feature is supported with Sun Netra 240 servers.

1.3 Software Requirements or Dependencies

(I)SN09 or higher release.

1.4 Limitations and restrictions

Scheduled backups to the standby server will not complete if a full system backup of the primary HA server pair is in progress.

1.5 Interactions

This feature is very similar to a full system backup. The interactions are similar to the existing full system backup. Due to the exclusive use of file system snap shots, a full system backup to local media and a remote backup to a standby system can not be running at the same time. If the remote backup function detects either of these in progress, it will cleanly exit and re-try at the next scheduled backup. If a local full system backup is attempted while a remote backup is in progress it will indicate that another backup is in progress and will exit.

Remote system backup should not have any interactions with SBA file transfer via ftp or SBA backup to DVD.

1.6 Glossary

Term	Description
New term	Definition

Product = Integrated EMS

A00009289-- IEMS (Integrated Element Management System) - 10 Minute Default on User Inactivity Timer

Functional Description

1: Applicable Solution(s)

UA-IP, PT-AAL2

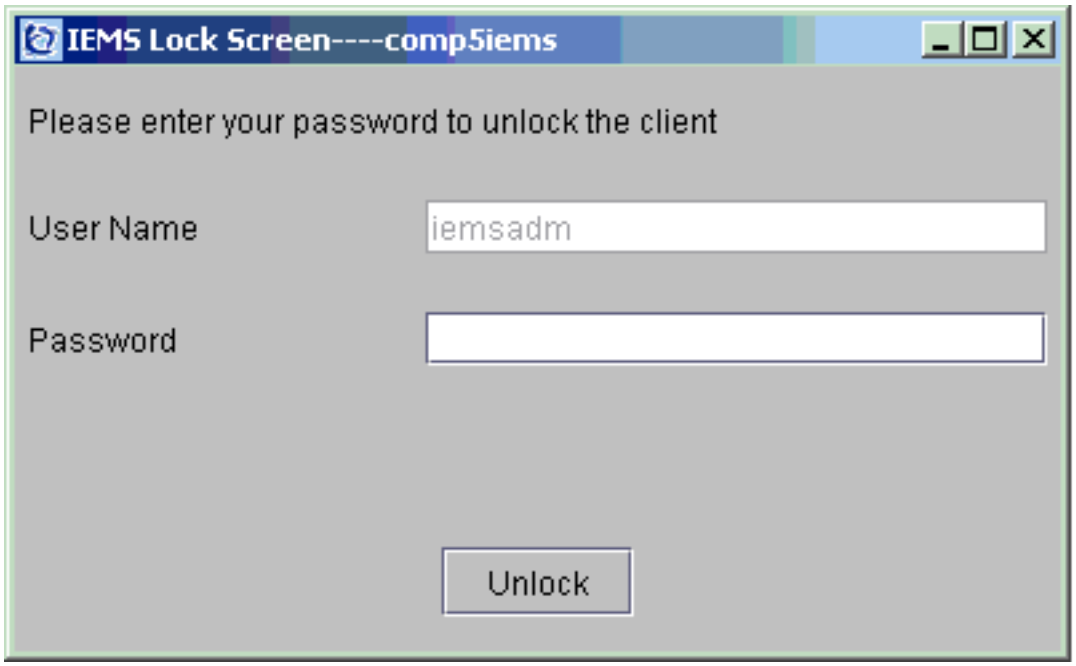
1.1 Description

In SN07, IEMS introduced a client inactivity timer that locked the client after a configurable period of time. Inactivity is defined as a lack of mouse actions - whether it be clicks or movements - on the IEMS screen. The inactivity timer functionality then locked the client until the user correctly entered his or her password. This basic security mechanism did not fully meet the customer requirements for security, so this feature further refines the existing IEMS client timeout to further meet those requirements.

With this feature, in addition to the existing locking of the IEMS client, the lockout timer will include the following:

- ability to change timeout value without requiring a restart of the server
- successive failed attempt lockout functionality to prevent multiple, rapid attempts to guess a password and unlock the client
- ability for the user to disable the client lockout will be removed

The new lock screen will look similar to the previous lock screen, without the option to disable it.



For more information on how to configure the timeout values, see the FN for A00008858 in this document.

When the user fails in 3 successive login attempts, they will be presented with a dialog box informing them that they will be unable to attempt to relogin again for a configured amount of time and the unlock button on the above window will be disabled. (Screen capture to be provided prior to IT declaration.)

The other additional functionality added this release is session termination after a specified inactivity timeout. The user will first see the GUI lock and then, if no action is taken before the user termination timer expires, the session will be terminated. This is consistent with other SSPFS based applications such as CMT and MG9KEM.

1.2 Hardware Requirements or Dependencies

No new hardware requirements or dependencies.

1.3 Software Requirements or Dependencies

This will require an SN09 or later version of SSPFS.

1.4 Limitations and restrictions

The IEMS HTML client will not timeout in this release. It will be supported in future IEMS releases.

1.5 Interactions

N/A.

1.6 Glossary

Term	Description
IEMS	Integrated Element Management System

2: Configuration for A00009289

2.1 Hardware and Software Requirements

The feature requires IEMS to be installed on SN09 or later SSPFS loads.

2.2 Initial Configuration

The configuration of the various paramaters is handled by SSPFS via the CLI. The details of the CLI are covered in the FN for A00008858. Please reference that document for additional information.

The Element Management section of this document provides links to how to change the inactivity timers - when available - for devices and element managers managed from the IEMS.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

2.4 Upgrade Considerations

2.5 Data schema (DS) (CM, MIBS, RDB)

2.6 Service Orders (SO) (CM & SESM)

2.7 Software optionality control (SOC)

2.8 Element Management

2.8.1 Setting Inactivity Timers for Managed Objects

This section provides links to the documentation for the inactivity timers for other managed objects on the IEMS.

- GWCEM, SAM21EM, UASEM, MG9KEM - these all use the same timeout values as IEMS, though inactivity on each application is calculated separately from IEMS.
- NGSS supports an inactivity timer, but it is non-configurable.
- CICM EM does not support an inactivity timer.
- USP supports an inactivity timer and details on how to set the values are provided in the USP documentation present on the USP CD image.
- STORM does not support an inactivity timer.
- SDM does not support an inactivity timer.

Table 1: Inactivity Timer Support for IEMS Managed Objects

Managed Object	Inactivity Timer Support	Configuration Documentation	Notes
GWC EM	Yes	Same timer used by IEMS	Inactivity is calculated separately from IEMS.
UAS EM	Yes	Same timer used by IEMS	Inactivity is calculated separately from IEMS.
SAM21 EM	Yes	Same timer used by IEMS	Inactivity is calculated separately from IEMS.
MG9K EM	Yes	Same timer used by IEMS	Inactivity is calculated separately from IEMS.
NGSS	Yes	Non-configurable	
CICM EM	No		
USP	Yes	Documentation provided on the USP CD image.	
STORM	No		
SDM	No		
MCS	No		

Table 1: Inactivity Timer Support for IEMS Managed Objects

Managed Object	Inactivity Timer Support	Configuration Documentation	Notes
MAS	Yes	on the MAS Server: go to Start->Programs->Administrator Tools->Terminal Services Configuration->Connections and select RDP-Tcp right click->Properties from the "Session" tab the idle session limit can be set.	The default on a standard MAS image is 30 minutes (it will automatically disconnect the client)
CEM	Yes	Same timer as IEMS	Shares inactivity calculation with the IEMS it is run from.

2.9 User interface changes

N/A

Product = IEMS

A00009292 -- IEMS: UserID-based Partitioning by NE

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Configuring rules using the Custom View Scope

Using the Custom View Scope, rules can be set such that the view can be customized as per the customer's requirement. Rules can be set at various levels which allow filtering at different levels.

The partitioning rules that can be set on user groups such that a user belonging to a particular user group has a set of predefined access as governed by the

rules. Note that Custom View Scopes cannot be added to the standard Carrier Voice over IP user groups.

The IEMS has 5 modules under which rules can be set. They are

1. Topology
2. Events
3. Alerts
4. Inventory
5. Stats Admin

Among these modules, Topology and Inventory modules are almost similar and rules set on any one of them is reflected to the user.

- Configuring Rules using the Topology / Inventory module
- Configuring Rules using the Event module
- Configuring Rules using the Alert module
- Configuring Rules using the Stats Admin module

Note: The terminology used for Maps is "**Topology**" and for Network Database is "**Inventory**".

1.2 Configuring Rules using the Topology / Inventory module

Integrated EMS administrator can add the authorized custom view scope to non-Carrier Voice over IP group using the Topology / Inventory module. This section describes Integrated EMS Security and Administration procedure to add the authorized custom view scope to a group using the Topology / Inventory module

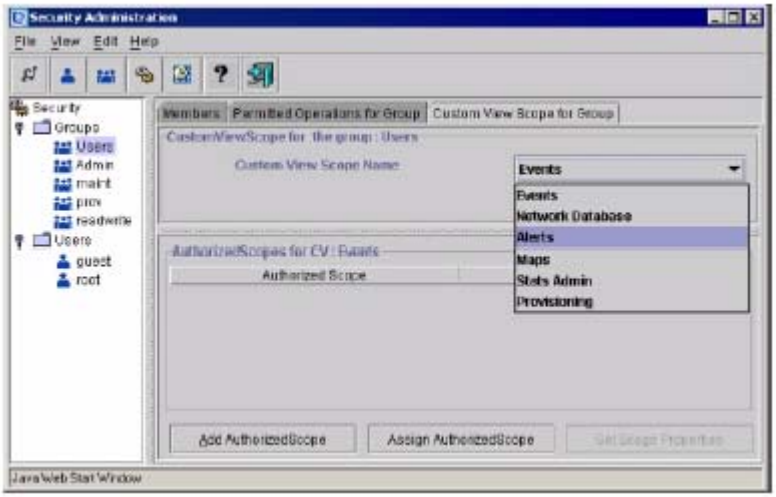
To add an authorized custom view scope to the group using the Topology/ Inventory module, follow these steps:

In the Security Administration tool of Integrated EMS

1 **1** Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

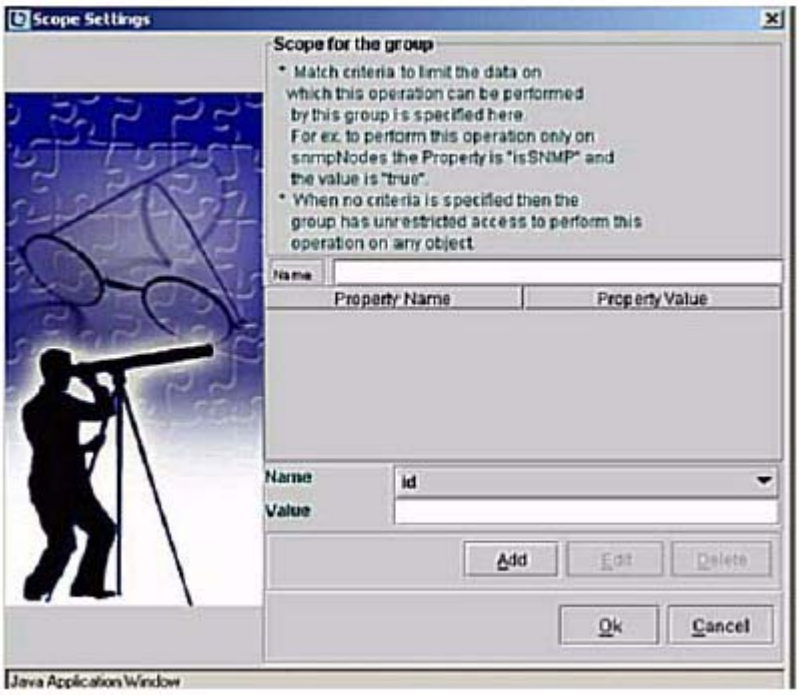
2 **2** Select the required group under the Groups node in the Security tree.

3 **3** Click the **Custom View Scope for Group** tab in the right-hand panel. The "Custom View Scope for the groups" window opens, as shown in the following figure.



4 **4** Select the Topology / Inventory custom view scope name from the drop-down menu.

5 **5** Click the **Add AuthorizedScope** button. The Scope Settings dialog opens, as shown in the following figure.



6 **6** Specify a name for the created custom view in the **Name** text field. Then select a “Property Name” from *Name* drop-down box. This

drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes. The property names and the values for Topology/Inventory currently used in Integrated EMS are listed in the table below. List of all property names that can be use for partitioning, see Properties used in IEMS for CVS

Property Name	Property Value
DisplayName	Name assigned to the device added to IEMS Example (GWC*, CO*, MG*, etc)
Ipaddress	IP address of the devices added to IEMS Example (47.142.106.220, 47.142.*.* for particular subnet etc)
EmIpaddress	IP address of the Element Manager added to IEMS Example (47.142.122.200, 47.142.*.* for particular subnet etc)
Managed	True, False
Status	1(i.e., Critical), 2(i.e., Major), 3(i.e., Minor), 4(i.e., Warning), 5(i.e., Clear), 6(i.e., Info), 7(i.e., Unknown)
DeviceVersion	Version of the devices added to IEMS Example (7.0, 8.0, 9.0)

7 **7** Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.

8 **8** Click the **OK** button to update the scope details in the Integrated EMS Server.

Note: To identify more than one property value, separate each value using the appropriate operators (refer to the "Setting custom view scope properties"). Example: !GWC* -> This will show all the NEs except starting name with GWC

Note: The multiple criteria can be form by using the composite CVS rule. Example: Partitioning based on the set of Display Names and belonging to one subnet, this can be achieved by setting two rules in same module.

displayName as GWC*

IPaddress as 47.1.*.*

1.3 Configuring Rules using the Event module

Integrated EMS administrator can add the authorized custom view scope to non-Carrier Voice over IP group using the Event. This section describes Integrated EMS Security and Administration procedure to add the authorized custom view scope to a group using the Event module

To add an authorized custom view scope to the group using the Event, follow these steps:

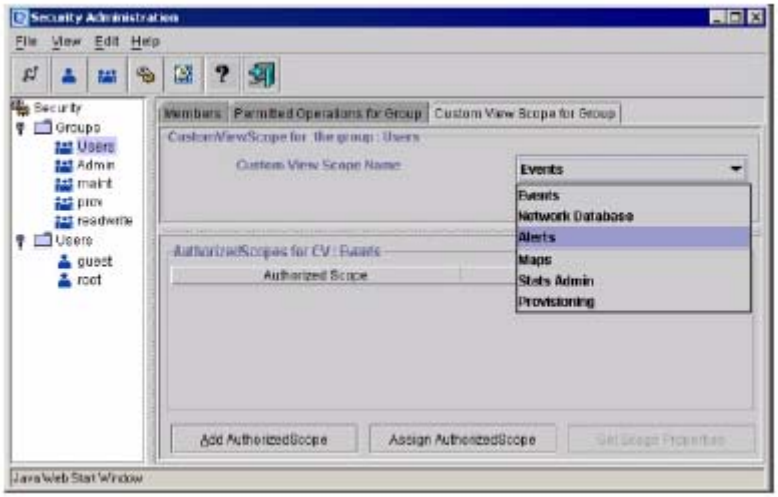
In the Security Administration tool of Integrated EMS

9 **1** Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

10 **2** Select the required group under the Groups node in the Security tree.

11 **3** Click the **Custom View Scope for Group** tab in the right-hand panel.

12 The "Custom View Scope for the groups" window opens, as shown in the following figure.



13 **4** Select the Event custom view scope name from the drop-down menu.

14 **5** Click the **Add AuthorizedScope** button. The Scope Settings dialog opens, as shown in the following figure.

15 **6** Specify a name for the created custom view in the **Name** text field. Then select a "Property Name" from *Name* drop-down box. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes. The property names currently used in Integrated EMS and the values it can take are listed in the table below. List of all property names that can be use for partitioning, see Properties used in IEMS for CVS

Property Name	Property Value
Category	Category of Events Example (communication, processingError, qualityOfService, equipment, others etc)
LogName	Generated log name Example (IEMS, EMJS, PP etc)
LogNumber	Generated log number Example (398, 640, 641 etc)
LogKey	Combination of both LogName and LogNumber Example (IEMS398, EMJS640, PP318 etc)
EventType	Type of event Example (TBL, INFO, FLT etc)
ComponentId	Example (SAM21, STORM etc)

ProbableCause	Cause of event Example (communicationSubsystemFailure, underlyingResourceUnavailable etc)
EquipmentIdentifier	Identifier of devices added to IEMS Example (IpAddress of NE/EM etc)
EventLabel	Label on Event Example (Alarm set, IEMS OM collection job alarm etc)
Severity	1(i.e., Critical), 2(i.e., Major), 3(i.e., Minor), 4(i.e., Warning), 5(i.e., Clear), 6(i.e., Info), 7(i.e., Unknown)

16 **7** Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.

17 **8** Click the **OK** button to update the scope details in the Integrated EMS Server.

Note: To identify more than one property value, separate each value using the appropriate operators (refer to the "Setting custom view scope properties"). Example: IEMS* -> This will show all the Events starting with IEMS as a LogKey property .

1.4 Configuring Rules using the Alert module

Integrated EMS administrator can add the authorized custom view scope to non-Carrier Voice over IP group using the Alert. This section describes Integrated EMS Security and Administration procedure to add the authorized custom view scope to a group using the Alert module

To add an authorized custom view scope to the group using the Alert, follow these steps:

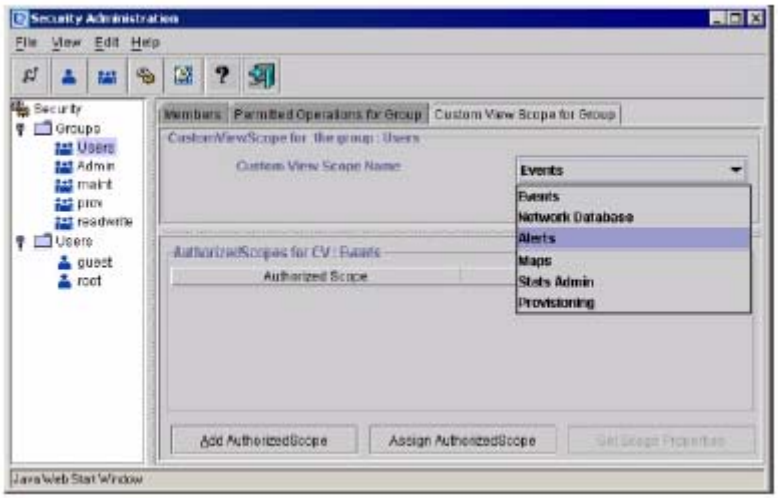
In the Security Administration tool of Integrated EMS

18 **1** Launch the Security Administration tool (refer to the "Starting the Security Administration tool").

19 **2** Select the required group under the Groups node in the Security tree.

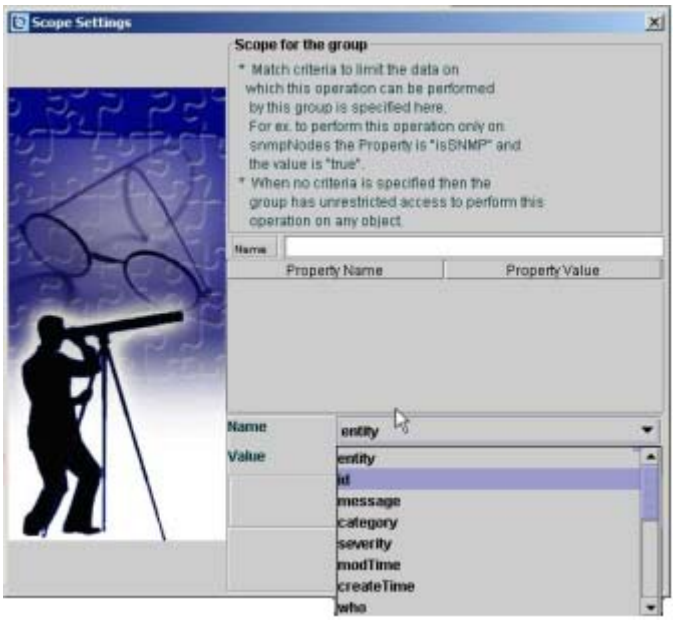
20 **3** Click the **Custom View Scope for Group** tab in the right-hand panel.

21 The "Custom View Scope for the groups" window opens, as shown in the following figure.



22 **4** Select the Alert custom view scope name from the drop-down menu.

23 **5** Click the **Add AuthorizedScope** button. The Scope Settings dialog opens, as shown in the following figure.



24 **6** Specify a name for the created custom view in the **Name** text field. Then select a “Property Name” from *Name* drop-down box. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes. The property names currently used in Integrated EMS and the values it can take

are listed in the table below. List of all property names that can be use for partitioning, see Properties used in IEMS for CVS

Property Name	Property Value
Category	Category of Events Example (communication, processingError, others etc)
EquipmentIdentifier	Identifier of devices added to IEMS Example (IpAddress of NE/EM, Display name of NE/EM etc)
LogKey	Combination of both LogName and LogNumber Example (IEMS398, EMJS640, PP318 etc)
ProbableCause	Cause of event Example (communicationSubsystemFailure, underlyingResourceUnavailable etc)
Severity	1(i.e., Critical), 2(i.e., Major), 3(i.e., Minor), 4(i.e., Warning), 6(i.e., Info), 7(i.e., Unknown)

25 **7** Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.

26 **8** Click the **OK** button to update the scope details in the Integrated EMS Server.

Note: To identify more than one property value, separate each value using the appropriate operators (refer to the "Setting custom view scope properties"). Example: IEMS* -> This will show all the Alerts starting with IEMS as a LogKey property

1.5 Configuring Rules using the Stats Admin module

Integrated EMS administrator can add the authorized custom view scope to non-Carrier Voice over IP group using the Stats Admin. This section describes Integrated EMS Security and Administration procedure to add the authorized custom view scope to a group using the Stats Admin module. Stats Admin module is basically for partitioning the Performance Collection Data using supported properties.

To add an authorized custom view scope to the group using the Stats Admin, follow these steps:

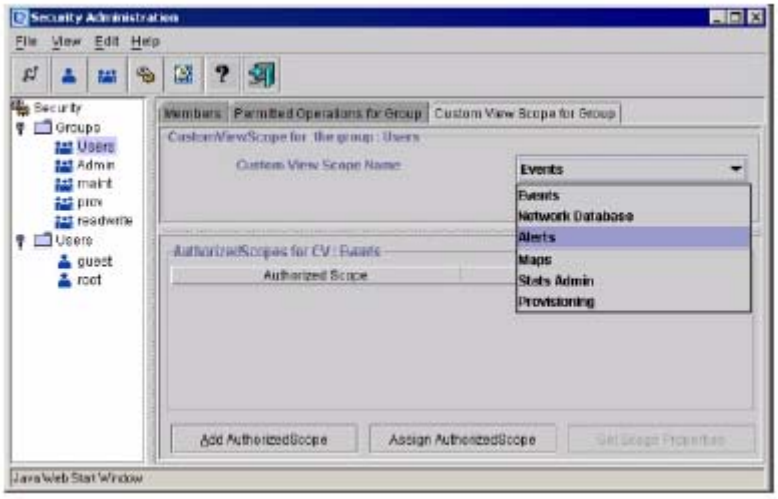
In the Security Administration tool of Integrated EMS

27 **1** Launch the Security Administration tool (refer to the “Starting the Security Administration tool”).

2 **2** Select the required group under the Groups node in the Security tree.

3 **3** Click the **Custom View Scope for Group** tab in the right-hand panel.

4 The "Custom View Scope for the groups" window opens, as shown in the following figure.



5 **4** Select the Stats Admin custom view scope name from the drop-down menu.

6 **5** Click the **Add AuthorizedScope** button. The Scope Settings dialog opens, as shown in the following figure.

33 **6** Specify a name for the created custom view in the **Name** text field. Then select a “Property Name” from *Name* drop-down box. This drop-down box lists the property names (which can be used for creating the authorized scopes) specific to each of the custom view scopes. The property names currently used in Integrated EMS and the values it can take are listed in the table below. List of all property names that can be use for partitioning, see Properties used in IEMS for CVS

Property Name	Property Value
Name	Name of Job Example (CollectionJob*)
Agent	Name of component for which Collection is enable Example (GWC*)
DNSName	Name of DNS used (can use IP address also) Example (47.166.56.10)
ID	Poll ID Example (1, 2, 100 or 243 etc)
Protocol	Used Protocol Example (SNMP etc)
NumericType	1 for numbers and 2 for string
OID	Identifier for Object that is Data Identifier Example (.1.3.6.1.2.1.1.1.0)
Threshold	The value is set to true if the threshold value is set for the collection data and false if threshold value is not set
IsMultiplePolledData	True, False

34 **7** Click the **Add** button to add the Authorized Scope for the selected Custom View Scope of the group.

35 **8** Click the **OK** button to update the scope details in the Integrated EMS Server.

Note: To identify more than one property value, separate each value using the appropriate operators (refer to the "Setting custom view scope properties"). Example: !GWC* -> This will show all the Agent’s Collection except starting name with GWC

1.5.1 Properties used in IEMS for CVS

All the property names currently used in Integrated EMS and the respective modules are listed in the table below.

Modules	Property Name
Topology	name, displayName, managed, status, isContainer, ipAddress, primaryIpAddress, secondaryIpAddress, timeZone, deviceVersion, FIState, SystemUnmanageState, platformAddress
Events	id, text, category, severity, time, source, node, logName, logNumber, logKey, sequenceNumber, eventType, componentId, probableCause, specificProblem, equipmentIdentifier
Alerts	entity, id, message, category, severity, modTime, createTime, who, source, logName, logKey, sequenceNumber, eventLabel, eventType, componentId, probableCause, specificProblem, equipmentIdentifier
Inventory	name, displayName, managed, status, isContainer, ipAddress, primaryIpAddress, secondaryIpAddress, timeZone, deviceVersion, FIState, SystemUnmanageState, platformAddress
Stats Admin	name, id, agent, oid, threshold, isMultiplePolledData, numericType, previouslySeverity, statsDataTableName, protocol, dnsName, lastTimeValue

Product = Integrated EMS

A00009320 -- Remote Ping and Traceroute for Gateway Controller and SSPFS Platforms

Functional Description

1: Applicable Solution(s)

UA-IP, PT-AAL2

1.1 Description

The purpose of this feature is to provide a centralized, graphical user interface on IEMS to allow users to launch ping and traceroute operations remotely on the Gateway Controller (GWC) and SSPFS platforms; including IEMS, CMT, MG9K Manager and CBM. This addresses the concerns of allowing non-root users access to these potentially harmful commands.

1.2 Hardware Requirements or Dependencies

This feature has no HA dependencies, so any customer-supported hardware configuration will provide a valid IT platform

IEMS Server: T1400, N240 (cluster or simplex)

CMT: T1400, N240 (cluster or simplex)

GWC - any supported hardware

1.3 Software Requirements or Dependencies

IEMS SN09 combo load week 11 or later

CMT - SN09

GWC - SN09 week 11 or later (gn090ap or later)

SSPFS - SN09 week 10 or later

1.4 Limitations and restrictions

This feature provides a centralized interface to the native ping and traceroute functionality on remote platforms. Command options and behavior for ping and traceroute may vary between remote launch points.

Central account users requiring SSPFS remote ping/traceroute capability must be granted restricted platform access (by setting their default shells to "restricted-access shell".

1.5 Interactions

Remote command launch allows users to troubleshoot network connectivity problems from a single location using the same user interface. It initiates an operation on a remote platform or device as if the user had logged on to the device and issued the command himself. In SN09, remote ping and traceroute functionality has been provided through the IEMS GUI client. These remote operations are supported in this release for the GWC and SSPFS platforms.

This feature adds two new launch menu buttons to the GWC and the SSPFS platform managed objects in the IEMS GUI: one for remote ping, and one for traceroute.

1.5.1 Launching:

This feature is accessed from the drop-down menu available when the a GWC or SSPFS unit managed object is right-clicked. Two new menu items have been added to the list:

- **“Launch Remote Ping”**
- **“Launch Remote TraceRoute”**

Figure 1 GWC Ping/Traceroute Launch Menu

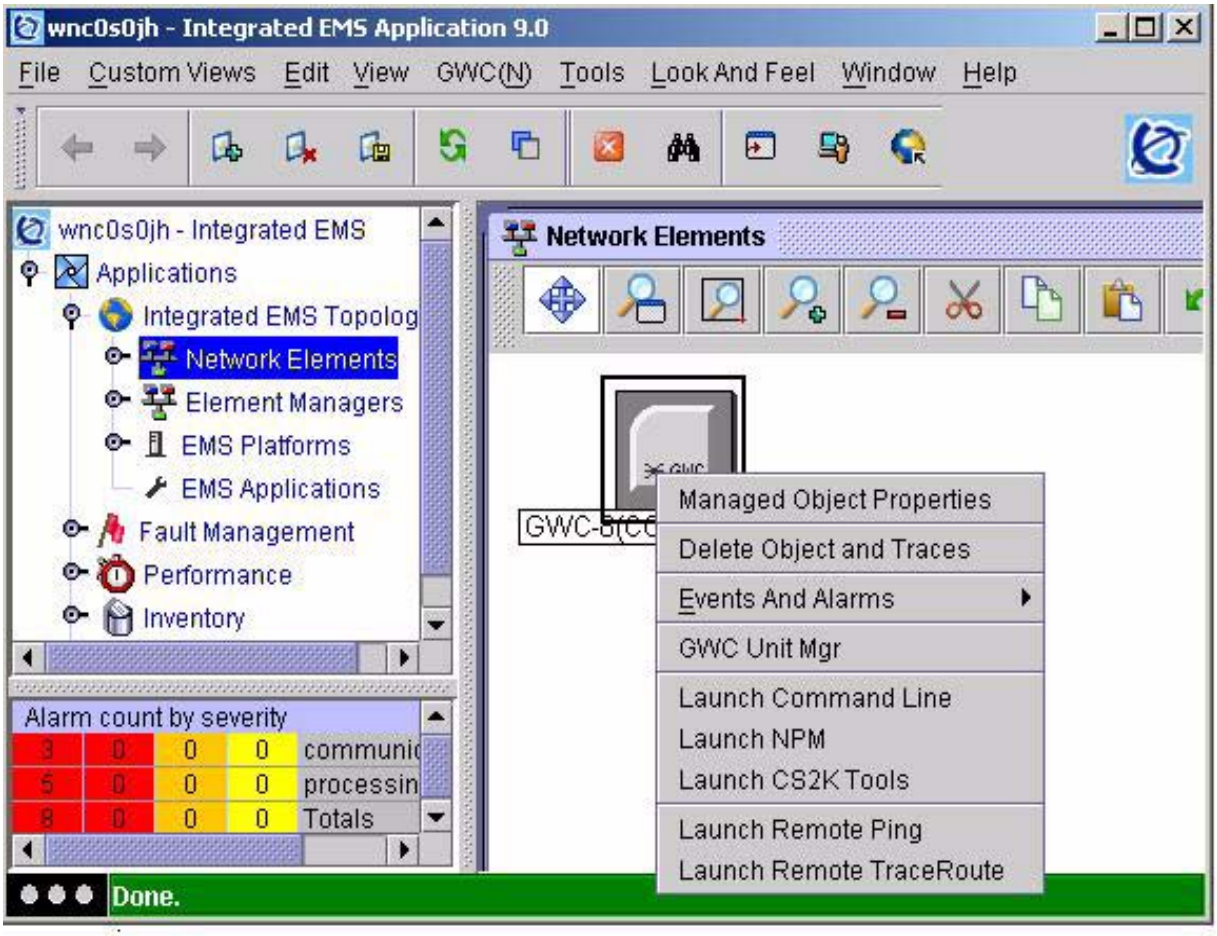
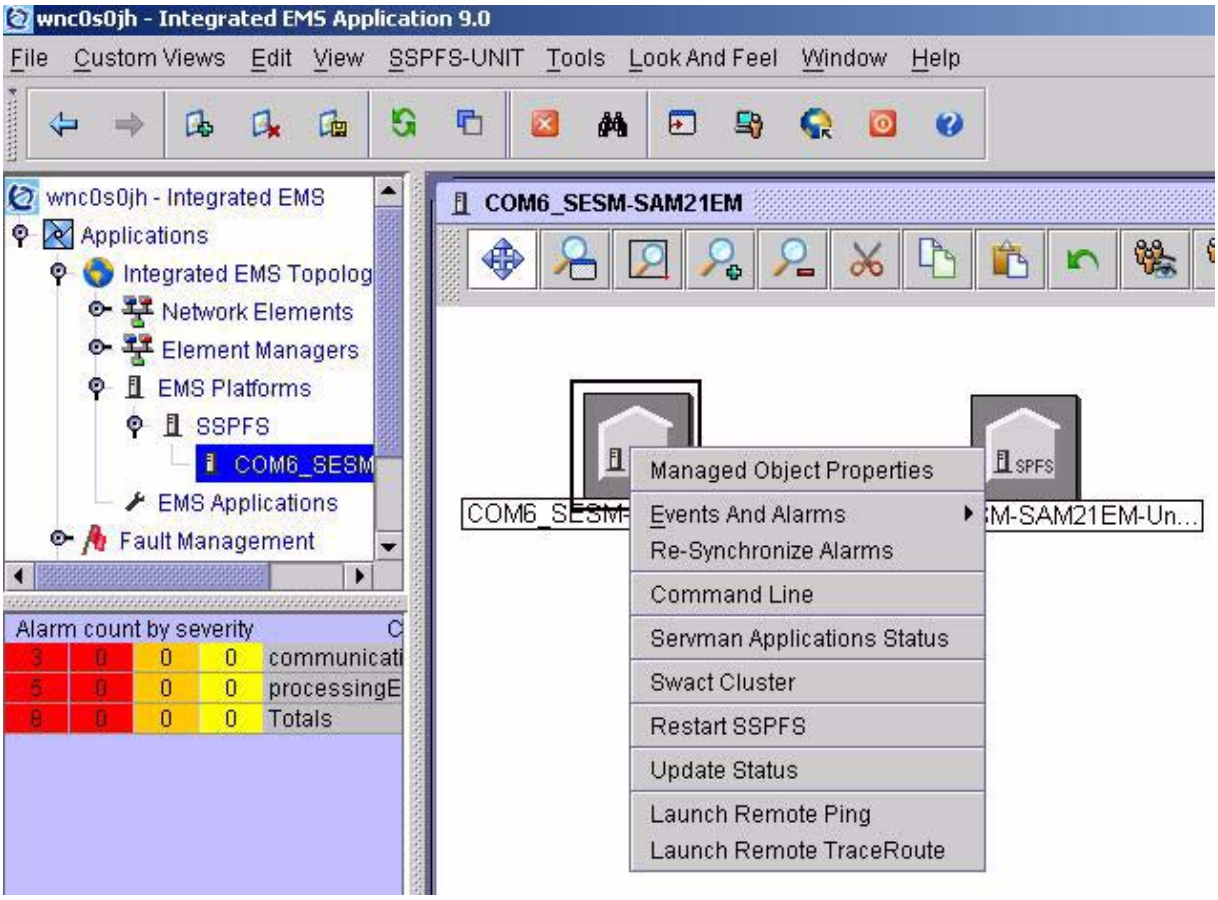


Figure 2 SSPFS Ping/Traceroute Launch Menu



The dialog for either operation is presented when selected from the menu. Each will be discussed in turn.

1.5.1.1 User Authorization

Remote operations are only available to a restricted set of users. For security purposes, only users belonging to one or more of the following groups for supported platforms will have access to these functions: ADM, MTC RW.

The following table lists the authorization groups for remote operations.

Table 2: authorization groups for remote operations

SSPFS	GWC
emsadm	mgcadm
emsmtc	mgcmtc
emsrw	mgcrw

Remote launch menu options will not appear in the above drop-down menus for unauthorized users.

1.5.1.2 Single Sign-on Support

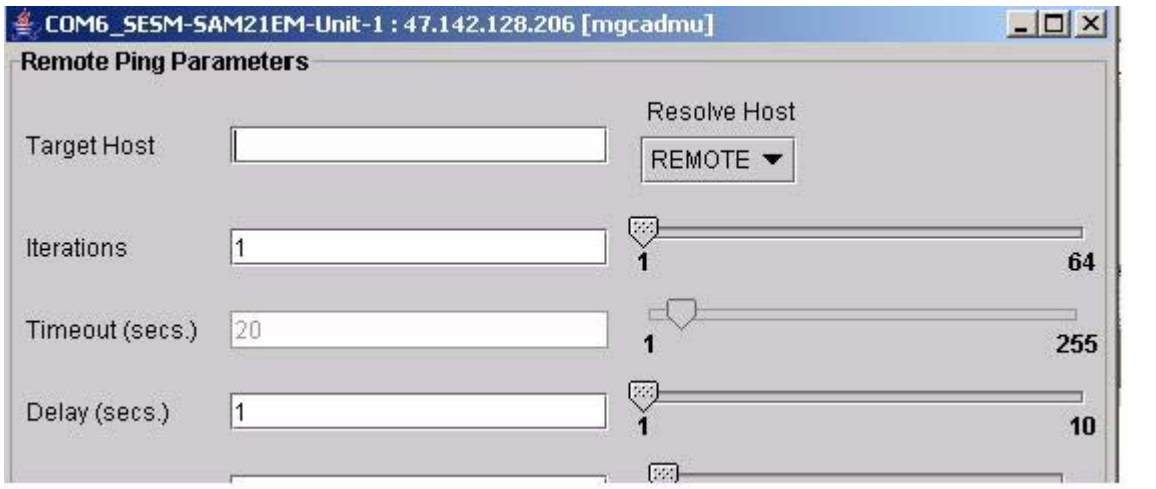
Once an authorized user has launched a remote operations GUI and entered the required parameters, the command should be sent to the remote host for execution without any further input required by the user. The client will use the security information obtained from the user at initial login , and use this to obtain access to the remote launch host. There is one exception to this rule:

When configured for CBM, the SSPFS platform does not integrate its security with the central security services used to provide single sign-on capabilities to users. In this case, the user will be presented with a dialog prompting for a username and a password to allow remote execution of the ping/traceroute command on the CBM platform.

1.5.2 Notes on Remote Operations:

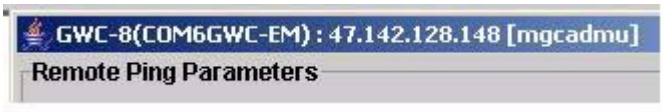
- Only one remote operation (ping or traceroute) is permitted on each managed object at a time. This effectively denies concurrent requests on the same device or platform. For example, user A launches a ping command on GWC 13. User B will be unable to launch any command on GWC 13 until the command completes for user A.
- The RemoteOps interface is constrained by the actual ping and traceroute functionality provided by a remote device. The interface acts as a proxy and invokes the command from the remote host as if a user had logged on and run it manually. Supported values and their ranges may vary between devices. Although a generic set of options, defaults, and ranges have been defined to constrain these operations in the network, they may be constrained even further by the remote host. The supported parameters and ranges for each device will be shown on the client screens when presented for input. The user does not need to know about this. An example of this is packet size. SSPFS platforms support a range of 1-65535 bytes, while the GWC only supports 1-1472 byes. Each range will be automatically enforced on client invocation.
- Ping and traceroute user parameters are common across all device and platform types. If a parameter is unsupported or unconfigurable for a selected managed object, the option will be displayed as read-only with a default value specified (if supported). For example, the screen in figure 3 displays the ***Delay*** parameter as Read-Only. The value shown will be used for the operation and cannot be changed by the user.

Figure 3 Read-Only Parameter example



Title Bar - The displayName and ipAddress properties of the managed object on the IEMS GUI are displayed in the top left corner of the screen. This is the source host for the remote operation (IP address of object right-clicked on GUI). Following the host infomation is the login user name enclosed in square brackets.

Figure 4 Remote Host Identifier



1.5.3 Remote Ping

The main screen for remote ping allows the user to set the following parameters:

Target Host:

This is the destination host to be ping'ed by the remote platform (GWC, for example). This value can be specified as a host name or IP address (see notes on DNS resolution).

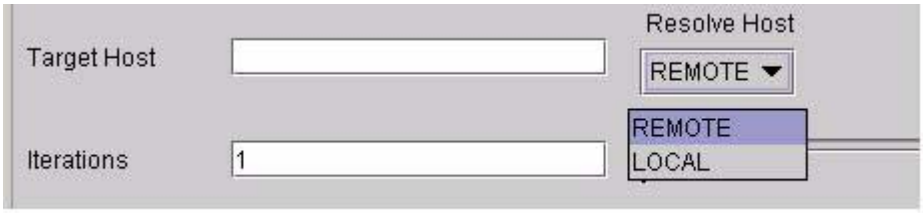
DNS Resolution

- specifies whether target address resolution should be attempted using the name service configured for IEMS server (*LOCAL*), or the name service of the remote launch host (*REMOTE*). This setting defaults to *REMOTE*.

Note: If DNS is not used in the network, then an attempt will be made to resolve the host name or IP using the default resolver on the IEMS server or remote device/platform.

Limitation: When using the "*REMOTE*" option on the GWC platform, target hosts MUST be entered as fully qualified domain names (FQDN). Host names provided without the full domain component will *fail* DNS resolution in the GWC. Target hosts can be specified this way by selecting "*LOCAL*" DNS resolution.

Figure 5 DNS Resolution Options



Iterations:
Specifies how many times to repeat the command.

Timeout:
Specifies the timeout for the remote host to use when running the remote operation. This value is given in seconds.

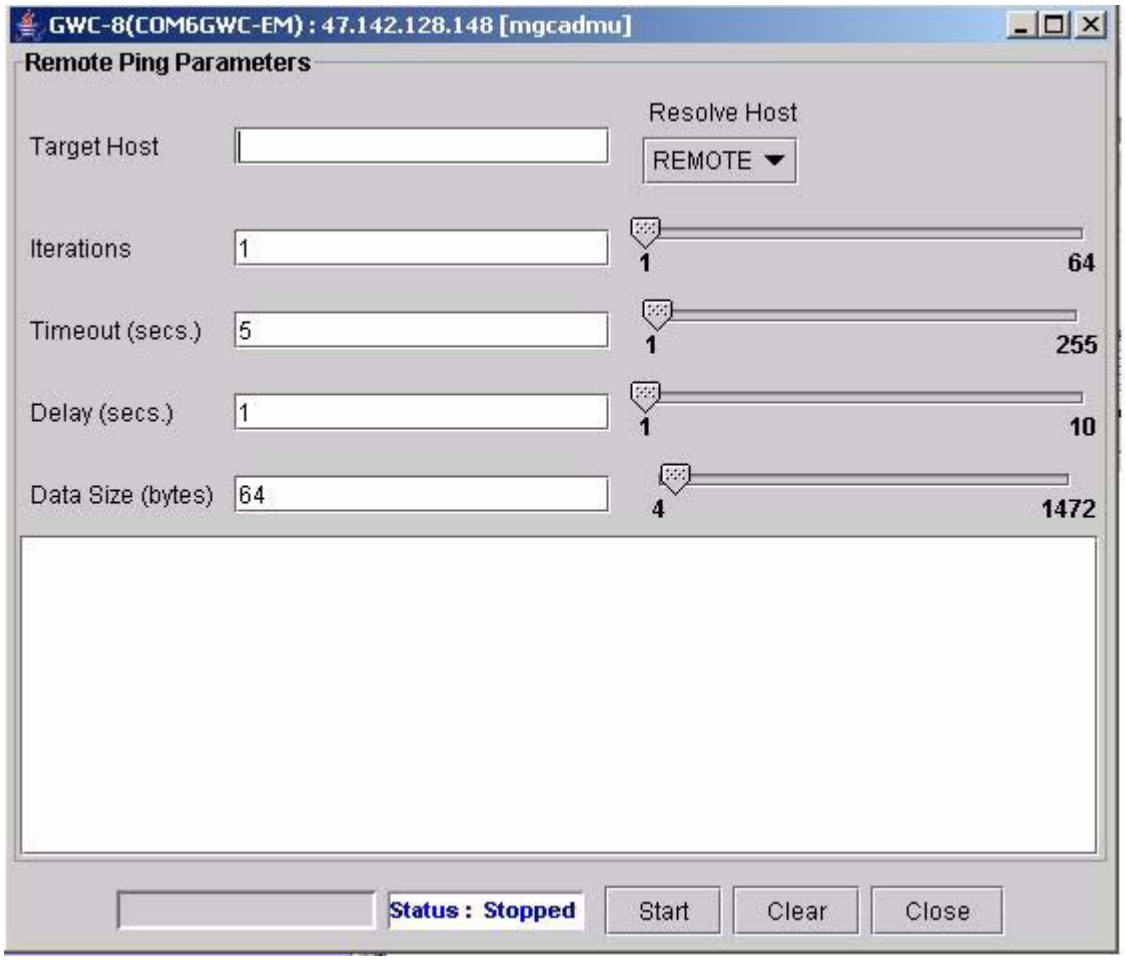
Delay:
Specifies the delay to use between each ping operation (ie: pause between iterations). This is given in seconds.

Packet Size:
Specifies (in bytes) the data size of each ping probe packet to use in the operation.

Table 1 Ping Dialog User Parameters

User Parameter	GWC Values	SSPFS Values	Default
Target IP	Host Name or IP address	Host Name or IP address	none
Iterations	1-64	1-64	1
Delay (seconds)	1-10	1-10	1
Timeout (seconds)	1-255	1-255	5
DNS Resolution	local/remote	local/remote	local
Packet size	1-1472 bytes	1-65507 bytes	64 bytes

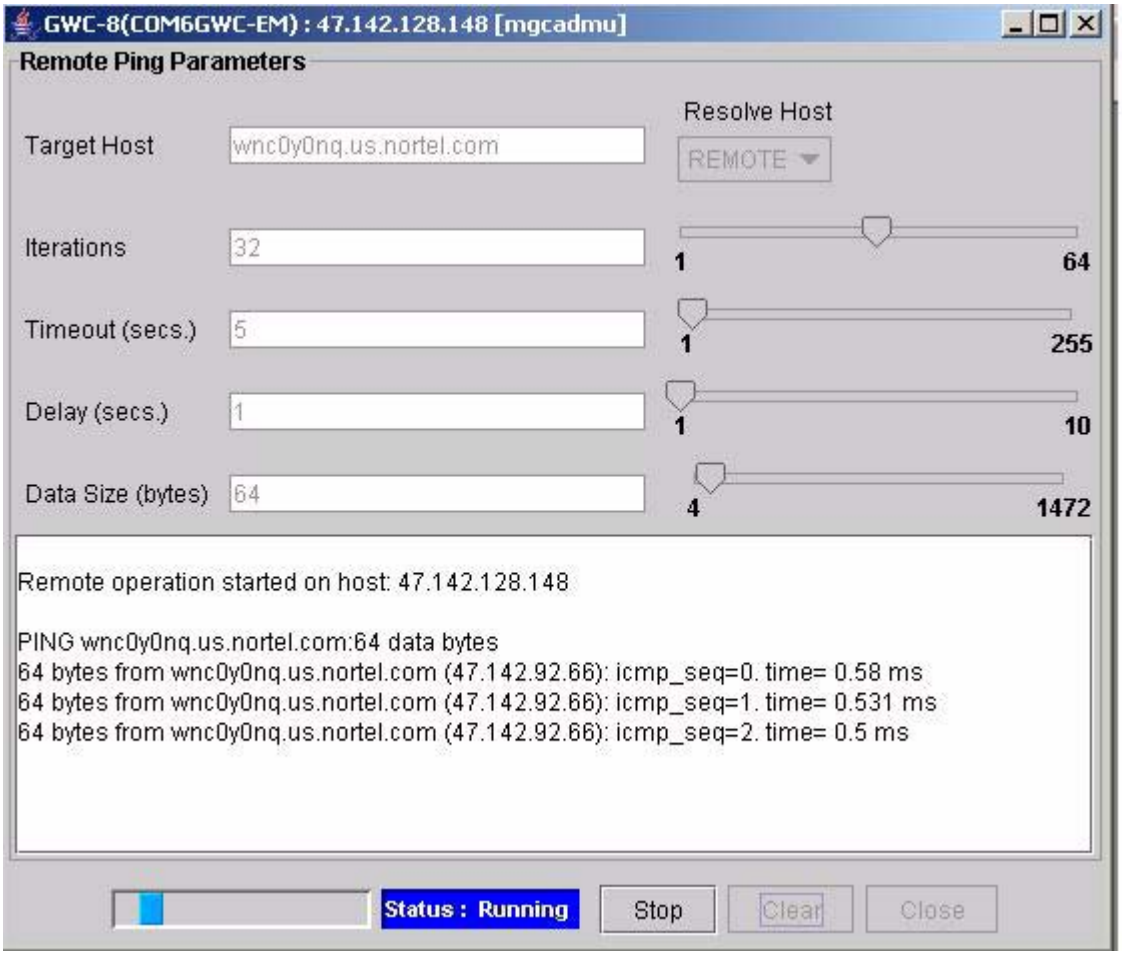
Figure 6 Remote Ping Launch Screen



Start button

starts remote operation with entered user parameters. Once the operation is started, all user input is disabled and the Start button changes its function to allow the command to be stopped (cancelled). This ensures that only operation can be launched at a time from the GUI. See figure 7

Figure 7 Remote Ping while running



Clear Button

clears text screen

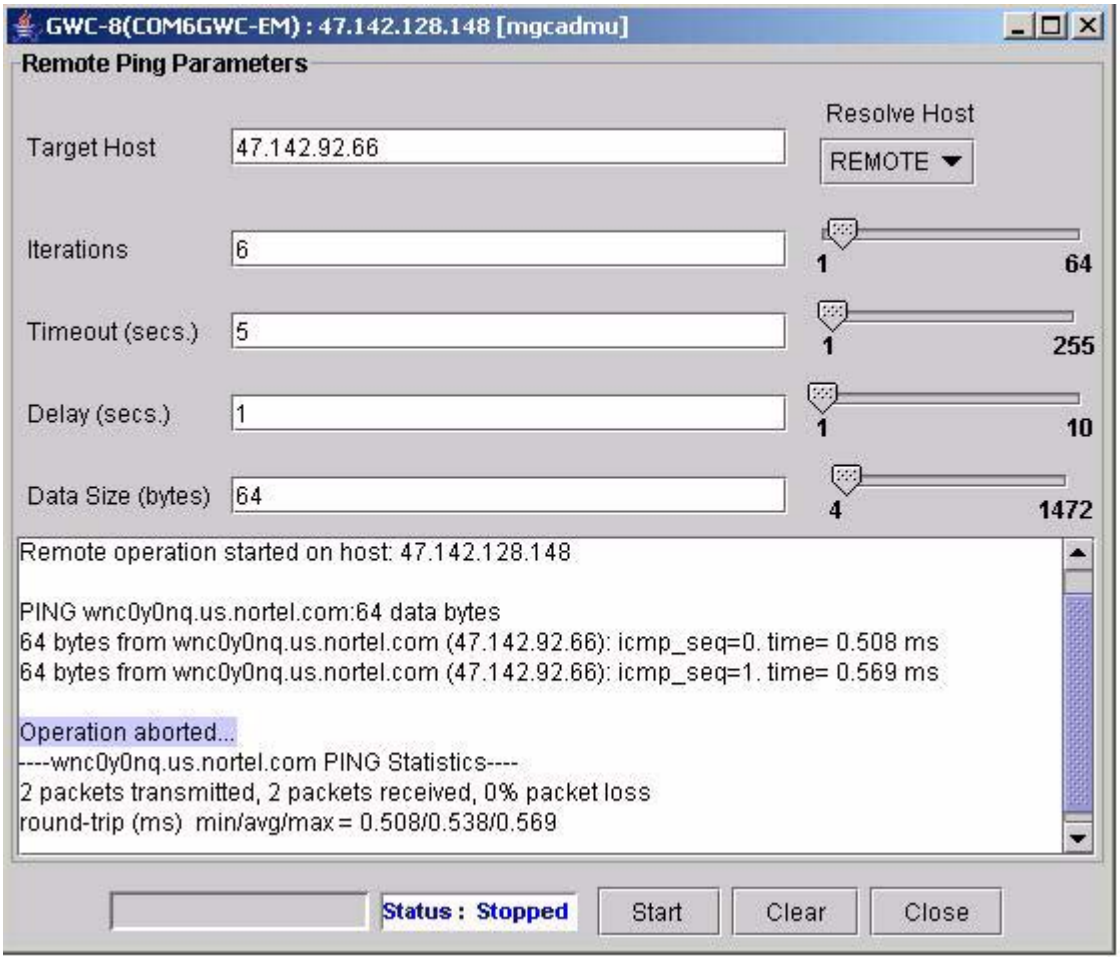
Close

closes window

1.5.3.1 Command ABORT

Running commands can be cancelled by the user by clicking the “Stop” button while the status bar indicates “Running”. The command will terminate and provide statistics for the packets sent and received up to the point of cancellation. The text output provides a message indicating the command was aborted.

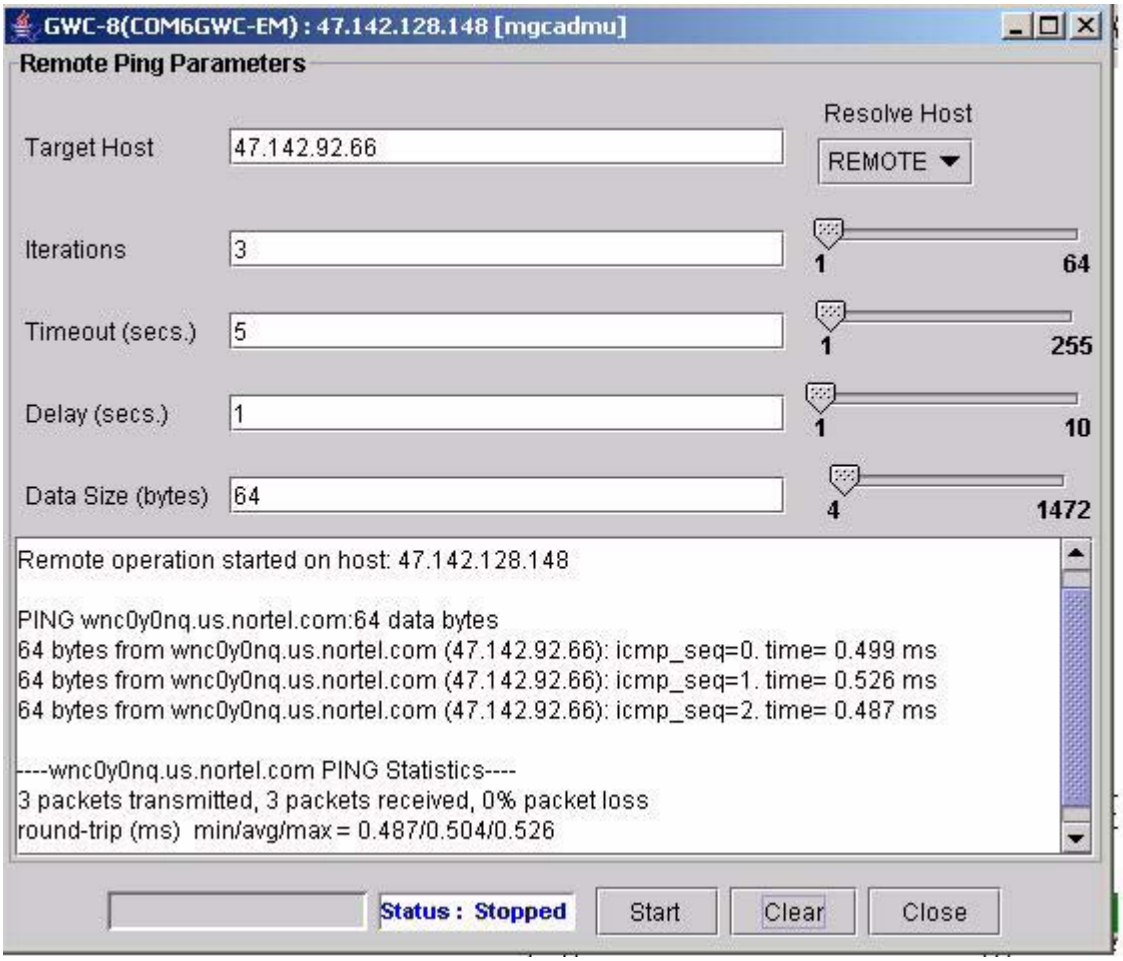
Figure 8 Cancel remote Ping Operation



1.5.3.2 Command output

The response output for the requested command will be output to the text window similar to that show shown in figure 6. The application communicates with the GWC over SNMP and formats the results to appear similar to UNIX command line ping output :

Figure 9 Ping output Screen



1.5.4 Remote TraceRoute

The main screen for remote ping allows the user to set the following parameters:

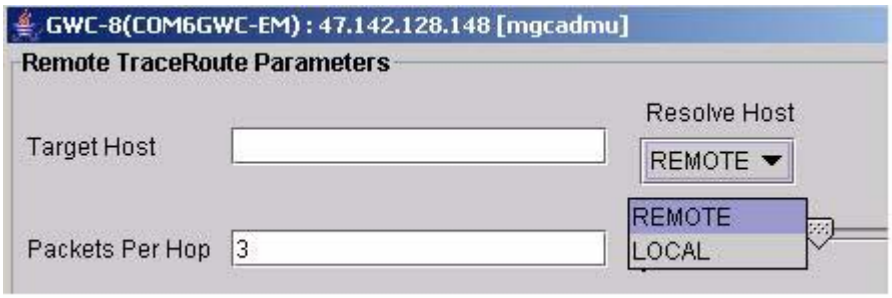
Target Host:
This is the destination host to find a route by the remote platform (GWC , for example). This value can be specified as a host name or IP address (see notes on DNS resolution).

DNS Resolution
Specifies whether target address resolution should be attempted using the name service configured for IEMS server (*LOCAL*), or the name service of the remote launch host (*REMOTE*). This setting defaults to *REMOTE*.

Note: If DNS is not used in the network, then an attempt will be made to resolve the host name or IP using the default resolver on the IEMS server or remote device/platform.

Limitation: When using the "*REMOTE*" option on the GWC platform, target hosts MUST be entered as fully qualified domain names (FQDN). Host names provided without the full domain component will *fail* DNS resolution in the GWC. Target hosts can be specified this way by selecting "*LOCAL*" DNS resolution.

Figure 10 DNS Resolution Options



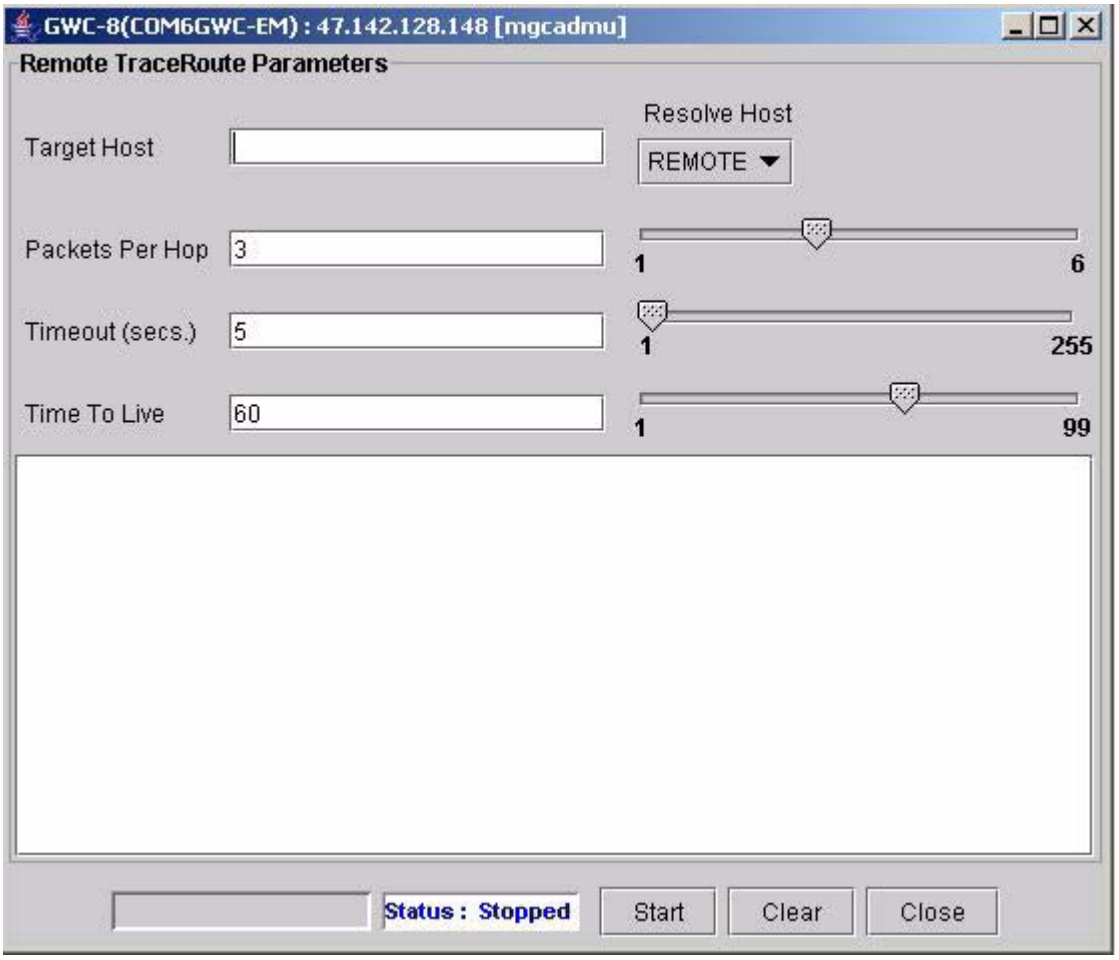
Timeout:
Specifies the timeout for the remote host to use when running the remote operation. This value is given in seconds.

Packet Size:
Specifies (in bytes) the data size of each ping probe packet to use in the operation.

Table 2 Traceroute Dialog User Parameters

User Parameter	GWC Values	SSPFS Values	Default
Target IP	Host Name or IP address	Host Name or IP address	none
Probes per Hop	1-6	1-6	3
TTL (Time To Live)	1-99	1-99	60
Timeout (seconds)	1-255	1-255	5
DNS Resolution	local/remote	local/remote	remote

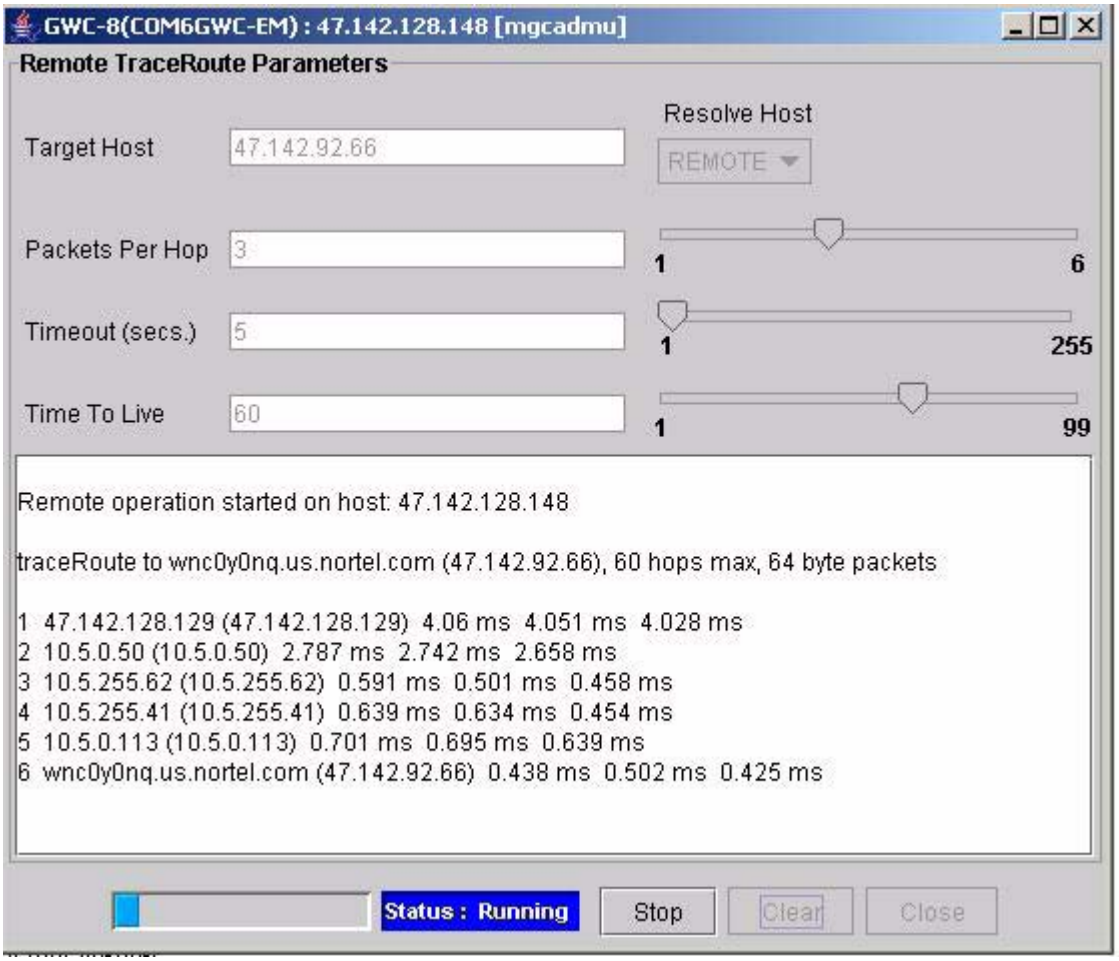
Figure 11 Remote Traceroute Launch Screen



Start button

starts remote operation with entered user parameters. Once the operation is started, all user input is disabled and the Start button changes its function to allow the command to be stopped (cancelled). This ensures that only operation can be launched at a time from the GUI. See figure 12.

Figure 12 Remote TraceRoute in operation



Clear Button

clears text screen

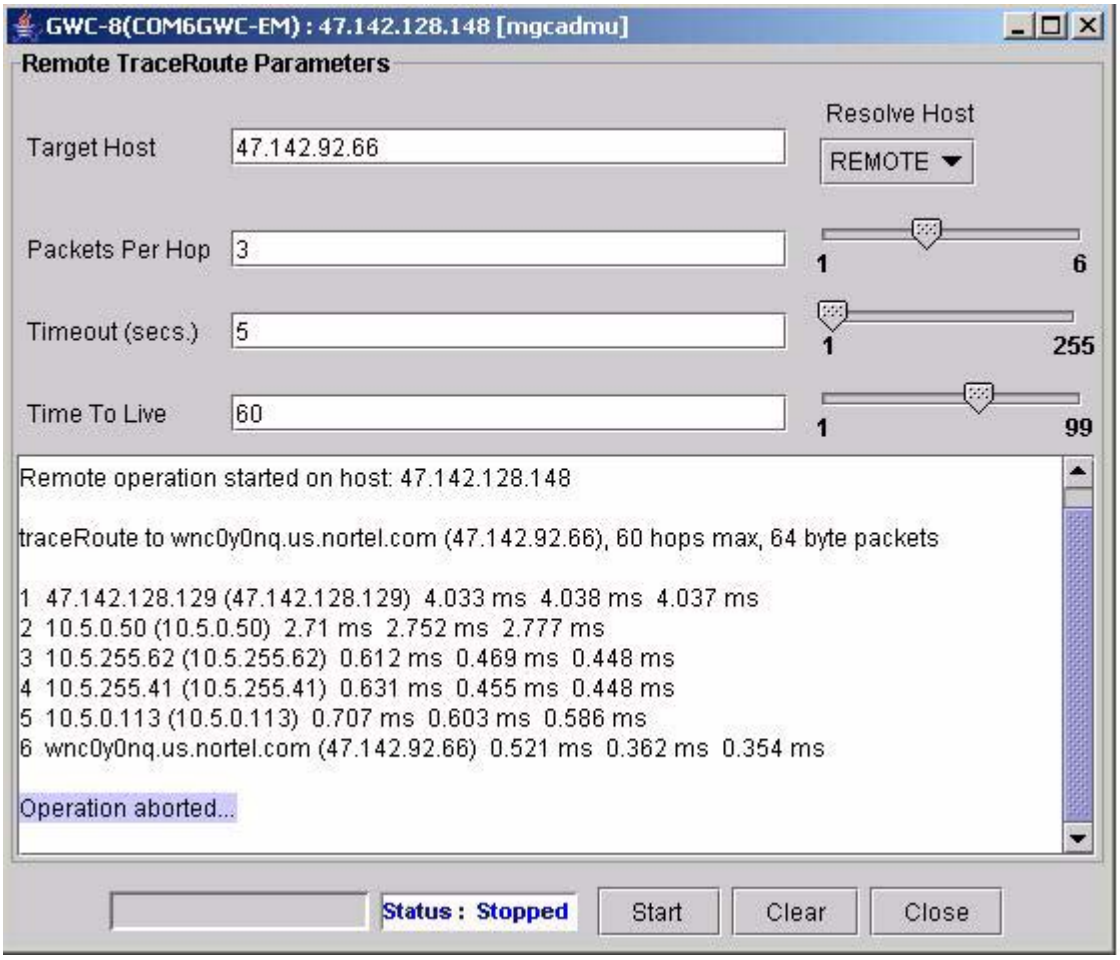
Close

closes traceroute window

1.5.4.1 Command ABORT

Running commands can be cancelled by the user by clicking the “Stop” button while the status bar indicates “Running”. The command will terminate and provide statistics for the packets sent and received up to the point of cancellation. The text output provides a message indicating the command was aborted.

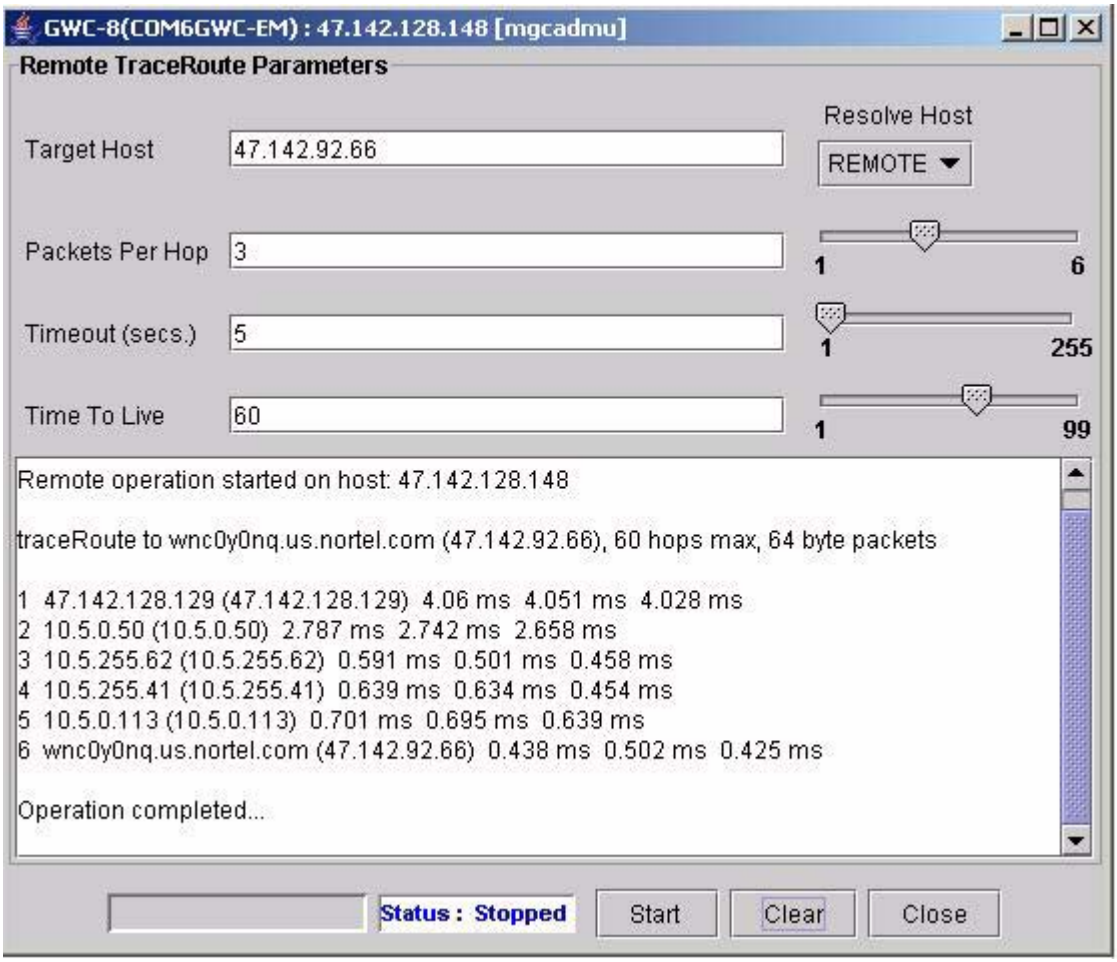
Figure 13 Cancel Remote Traceroute operation



1.5.4.2 Command output

The response output for the requested command will be output to the text window similar to that shown in figure 6. The application communicates with the GWC over SNMP and formats the results to appear similar to UNIX command line traceroute output :

Figure 14 Remote TraceRoute output



1.6 Glossary

Term	Description
IEMS	Integrated Element Management System
GWC	Gateway Controller
MG9K	Media Gateway 9000
CBM	Core Billing Manager
SNMP	Standard Network Management Protocol
SSH	Secure Shell

Product = Integrated EMS

A00009336 -- Refer to A00009320

Functional Description

1: Applicable Solution(s)

UA-IP

Product = Integrated EMS

A00009532 -- Support Host to Host Tunnels for all Northbound OSS Connections

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP, PT-AAL2

1.1 Description

This feature name is: Support host to host tunnels for all northbound OSS connections (in addition to existing security mechanisms).

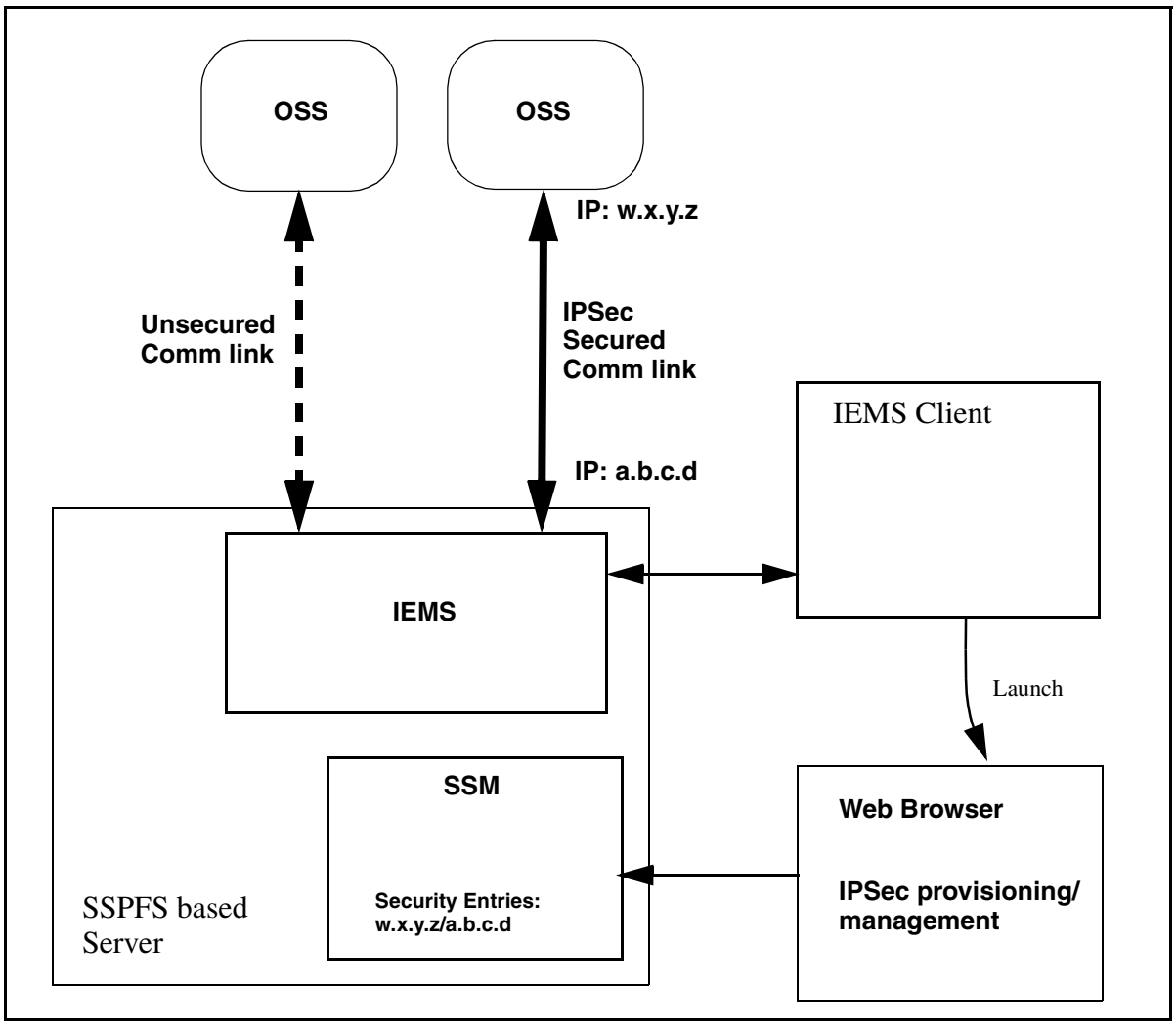
This activity is to test, verify and document host to host IPSec between SSPFS servers (namely IEMS, but not exlusively) and northbound OSSs. Securing this communications link will provide additional protection and encapsulation of OSS to IEMS traffic. The IPSec implementation will be in all other ways compliant with encryption key management and encryption protocol requirements in the Verizon agreement.

This activity will use the existing IPSec provisioning and management framework provided by SSPFS's Server Security Manager (SSM). SSM is currently used by the MG9K EM to secure communications channels with MG9K Network Elements.

All testing encompassing this feature will be based on the Solaris 9 software platform for SSPFS servers as well as OSS simulation. A Sun Netra 240 will be used for the SSPFS servers and a Sun Ultra 10 will be used for simulating the OSS.

The figure below gives a functional layout of the components involved with this feature. The main component of interest is the IEMS application running on a SSPFS based server. It provides input to the northbound OSS links. IEMS has a native GUI for craftsperson interaction. Another important component within SSPFS is the Server Security Manager (SSM). This component is used to provision and manage all IPSec related parameters for the SSPFS server and by extension all applications running on the server, such as IEMS. SSM is accessed using a standard web browser. The last component is the OSS which receives messaging output from IEMS. In this feature, for testing purposes, the OSS will be simulated.

Figure 1 Functional Layout



1.2 Hardware Requirements or Dependencies

No new hardware requirements or dependencies are introduced in the feature for the IEMS server.

1.3 Software Requirements or Dependencies

The latest SN09 IEMS software will be required for IPSec.

1.4 Limitations and restrictions

IEMS will not have direct control over the provisioning and management of IPSec security. This functionality is the domain of the Server Security Manager (SSM).

No new security parameters are being introduced in the Server Security Manager (SSM). This feature will utilize the existing functionality of SSM. That means Internet Key Exchange with preshared keys is the only supported mechanism for relaying encryption key information.

1.5 Interactions

Using IPSec to secure the northbound OSS interface will be invisible to the functionality and not have any impact to managing the traffic except for the additional step of provisioning the IPSec security parameters.

1.6 Glossary

Term	Description
IEMS	Integrated Element Manager System
SSM	Server Security Manager

2: Fault Management for A00009532

2.1 Fault management strategy

Not applicable.

2.2 Fault management tools and utilities

Not applicable.

2.3 Logs

No new logs are being added because of this feature. The following section is added for informational purposes.

2.3.1 IPsec syslog messages

The Solaris implementation of IPsec automatically sends all failure logs to syslog /var/adm/messages. We do not have control over this. However when the Server Security Manager (SSM) makes any changes to the IPsec security rules, the wrapper scripts will output any attempted changes to /var/log/securitylog.

The Solaris IPsec itself does not seem to generate any failure messages because security could be compromised, however IKE does seem to generate failure messages to syslog.

Sample IKE failure message would look like the following:

```
messages.0:Mar 25 15:40:04 wnc1s01h /usr/lib/inet/in.iked: [ID
313954 daemon.notice] IKE_DELETE_PAYLOAD_RECEIVED:
20040325204004:   Source addr:47.142.217.23 Destination
addr:47.142.217.22 SPI:0x0100005d350a7d6c0100006b743037d4
Description:Received delete notification
```

All other possible failure messages that could get generated to syslog is shown below for IKE.

```
IKE_AH_IP_FRAGMENT

IKE_AH_SA_LOOKUP_FAILURE

IKE_AH_SEQUENCE_NUMBER_FAILURE

IKE_AH_ICV_FAILURE

IKE_ESP_SEQUENCE_NUMBER_OVERFLOW

IKE_ESP_IP_FRAGMENT

IKE_ESP_SA_LOOKUP_FAILURE,

IKE_ESP_SEQUENCE_NUMBER_FAILURE

IKE_ESP_ICV_FAILURE

IKE_INVALID_COOKIE

IKE_INVALID_ISAKMP_VERSION

IKE_INVALID_EXCHANGE_TYPE

IKE_INVALID_FLAGS

IKE_INVALID_MESSAGE_ID

IKE_INVALID_NEXT_PAYLOAD

IKE_INVALID_RESERVED_FIELD

IKE_INVALID_DOI

IKE_INVALID_SITUATION

IKE_INVALID_PROPOSAL

IKE_INVALID_SPI

IKE_INVALID_TRANSFORM

IKE_INVALID_ATTRIBUTES
```

IKE_INVALID_KEY_INFORMATION

IKE_INVALID_ID_INFORMATION

IKE_INVALID_CERTIFICATE

IKE_INVALID_CERTIFICATE_TYPE

IKE_INVALID_CERTIFICATE_AUTHORITY

IKE_INVALID_HASH_INFORMATION

IKE_INVALID_HASH_VALUE

IKE_INVALID_SIGNATURE_INFORMATION

IKE_INVALID_SIGNATURE_VALUE

IKE_INVALID_PROTOCOL_ID

IKE_INVALID_MESSAGE_TYPE

IKE_CERTIFICATE_TYPE_UNSUPPORTED

IKE_CERTIFICATE_UNAVAILABLE

IKE_NOTIFICATION_PAYLOAD_RECEIVED

IKE_DELETE_PAYLOAD_RECEIVED

IKE_UNEQUAL_PAYLOAD_LENGTHS

IKE_BAD_PROPOSAL_SYNTAX

IKE_RETRY_LIMIT_REACHED

2.4 Alarms

No new alarms are being added because of this feature.

2.5 Related documentation

3: Configuration for A00009532

3.1 Hardware and Software Requirements

SN09 or later software load for the SSPFS server (such as Integrated Element Manager System (IEMS)).

3.2 Initial Configuration

3.2.1 Security

From a high-level here are the steps to enable security for a northbound OSS.

1. Load SSPFS server (such as IEMS) with required SN09 or later software load.

2. Enable security on the OSS to secure the connection to the SSPFS server. Details of this step are beyond the scope of this document as each OSS provisioning mechanism is different.
3. The craftsperson will then use a web browser and connect to the SSPFS server machine's Server Security Manager (SSM). This is done using the item under the EMS Platforms, SSPFS menu at the top, or manually by entering the correct address information in a supported web browser. *Only users with the necessary security privileges can access to SSM . This is done using a separate Succession Login to SSM.*
4. After logging in, the craftsperson will enable security for communications with the OSS IP address.
5. This will complete securing the OSS link.

3.2.1.1 OSS

Details of OSS operation are beyond the scope of this document as each OSS provisioning mechanism is different.

IPSec and IKE configuration parameters that are provisioned on the OSS must match the corresponding IPSec and IKE parameters on the IEMS, provisioned via the Server Security Manager.

3.2.1.2 SSPFS Server System

IPSec and IKE configuration parameters that are provisioned, via the server security manager, must match the corresponding IPSec and IKE parameters on the OSS.

3.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable

3.4 Upgrade Impact

Not applicable

3.5 Data schema (DS) (CM, MIBS, RDB)

Not applicable

3.6 OSS Changes

Not applicable

3.7 External Interface Changes

Not applicable

3.8 Integrated Element Manager System

3.8.1 Security Button

A new security item under the EMS Platforms, SSPFS menu at the top, is now available in IEMS to launch the Server Security Manager. The URL will be http://<SSPFS server ip address>/ipsec/security.html.

3.8.2 Server Security Manager

3.8.2.1 Functional description

This HTML webpage will be used to define security parameters to secure communications into and out from the SSPFS server machine. This includes IEMS to OSS communications.

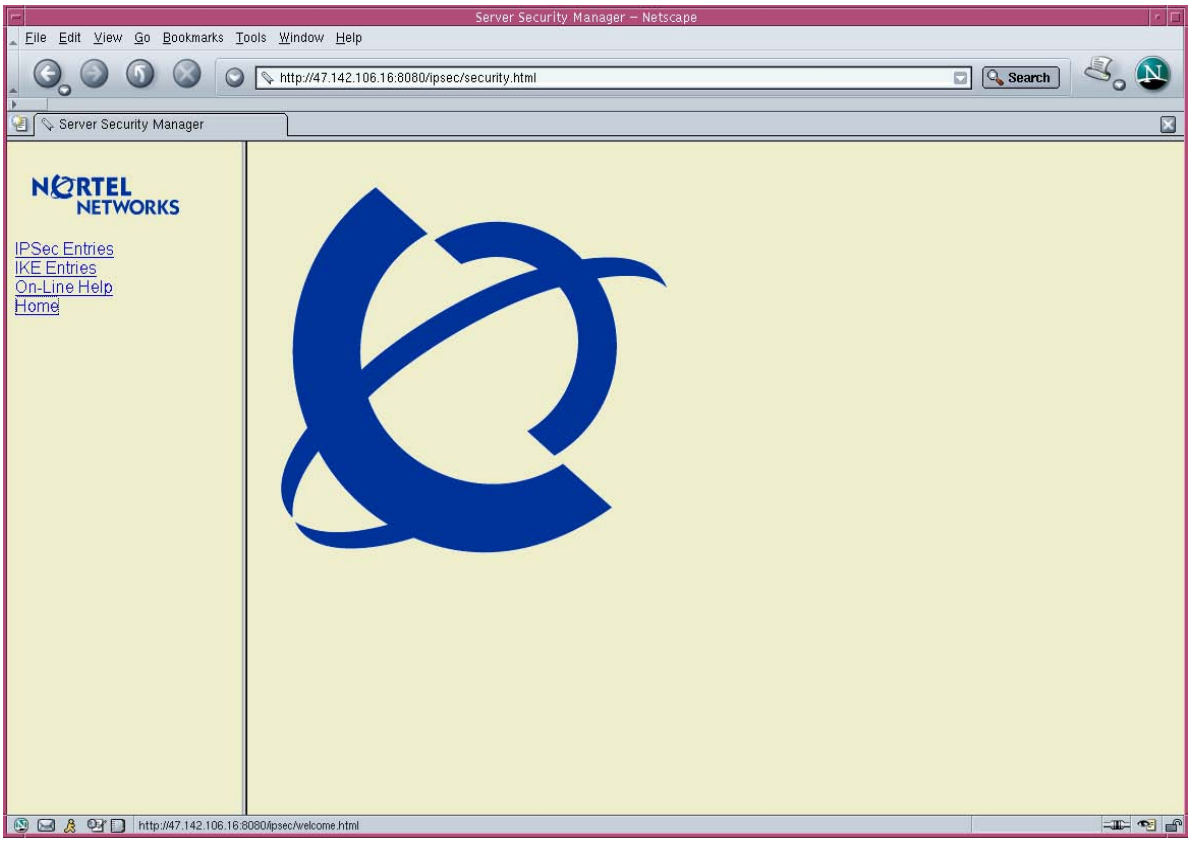
The craftsperson will be presented with two tables representing currently provisioned security parameters. One for IPSec parameters and one for IKE parameters. Options to add and delete entries are available. Adding entries will be performed using HTML forms.

The IPSec Entries page allows retrieval and manipulation of IPSec policies for a host server. Once the policies are configured, all outbound and inbound datagrams are subject to policy checks as they exit and enter the host server. If no entry is found, no policy checks will be made, and all the traffic will pass through unimpeded. Depending upon the match of the policy entry, a specific action will be taken.

The IKE Entries page allows retrieval and manipulation of Internet Key Exchange policies for a host server. Once a policy is configured, the IKE daemon running on the IEMS server can negotiate with a remote host to establish the actual IPSec keys used to secure messages between IEMS and the OSS host.

Note: Only users with the necessary security privileges can access SSM. This is done using a separate Succession Login to SSM.

The following is the first page presented to the craftsperson upon opening the Server Security Manager:



Navigation is performed using the links on the left frame. User input is performed or operation output is displayed in the right frame.

3.8.2.2 GUI usage and implications

Primary usage of this interface in SN09 is to secure the communications channel between SSPFS server application such as IEMS and an OSS.

First, IPSec entries are created using the desired parameters. If the craftsperson has chosen to use the “IPSec” action, the second step is to create a corresponding IKE entry using the desired parameters.

Note: This interface provides for securing all network communications and not just OSS communications. Care must be taken when provisioning or deleting the security parameters, so as not to effect other essential communications, such as telnet, ftp, etc.

3.8.2.3 IPSec fields

The following table lists the security fields for IPSec parameters.

Table 1 IPSec field descriptions

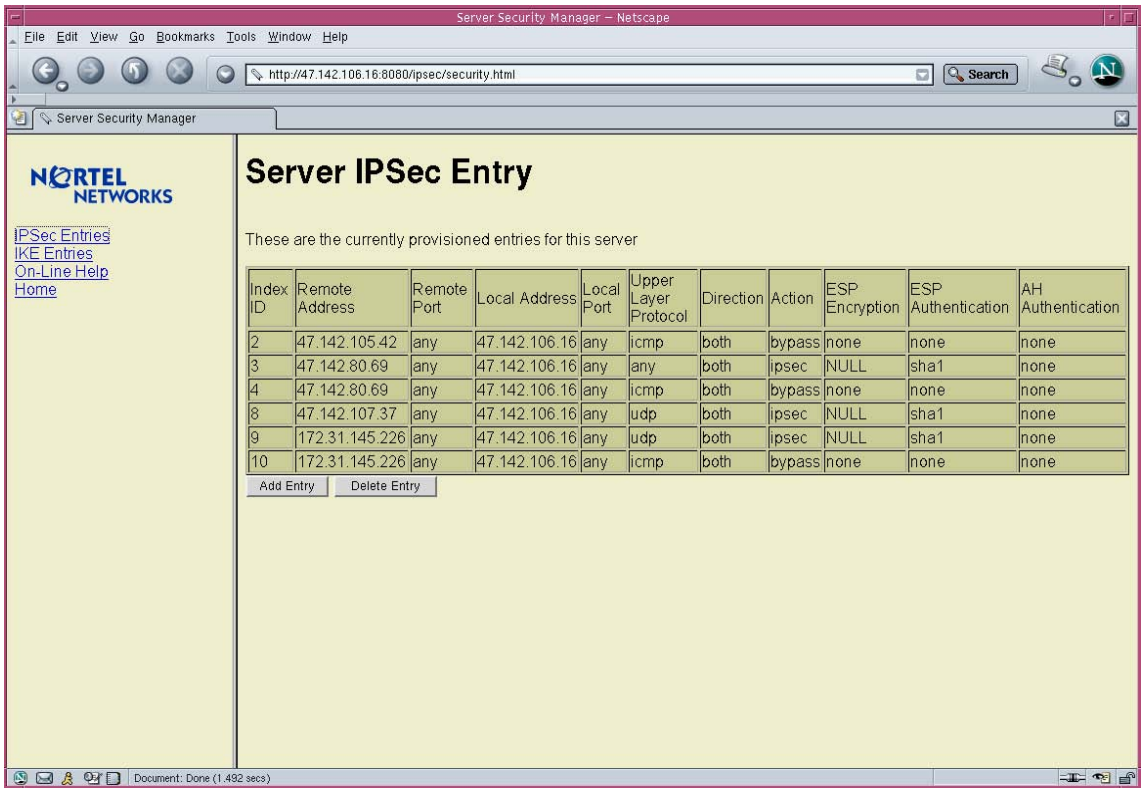
Field	New or Changed	Subfield	Entry	Explanation and action
Index ID	New	No	Integer	Internal index used by the server to track and reference IPSec entries.
Remote Address	New	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	Remote Address means the source address on incoming packets and destination address on outgoing packets.
Remote Port	New	No	1 - 65535, any	IP port of the remote system communicating with this server.
Local Address	New	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	Local Address means the destination address on incoming packets and source address on outgoing packets.
Local Port	New	No	1 - 65535, any	IP port of this server.
Upper Layer Protocol	New	No	any, icmp, tcp, and udp.	Determines which protocol traffic this entry is matched against.
Direction	New	No	in, out, and both.	Determines whether this entry is for inbound or outbound traffic.
Action	New	No	bypass, drop, and ipsec.	Determines the action to take when the traffic pattern is matched.
ESP Encryption	New	No	none, any, NULL, des, 3des.	Describes the encryption algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.

Table 1 IPSec field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action
ESP Authentication	New	No	none, any, sha1, and md5.	Describes the authentication algorithm that will be used to apply the IPSec ESP protocol to outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.
AH Authentication	New	No	none, any, sha1, and md5.	Describes the encryption algorithm that will be used to apply the IPSec AH header on outbound datagrams and verify it to be present on inbound datagrams. Only valid when action is set to “ipsec”.

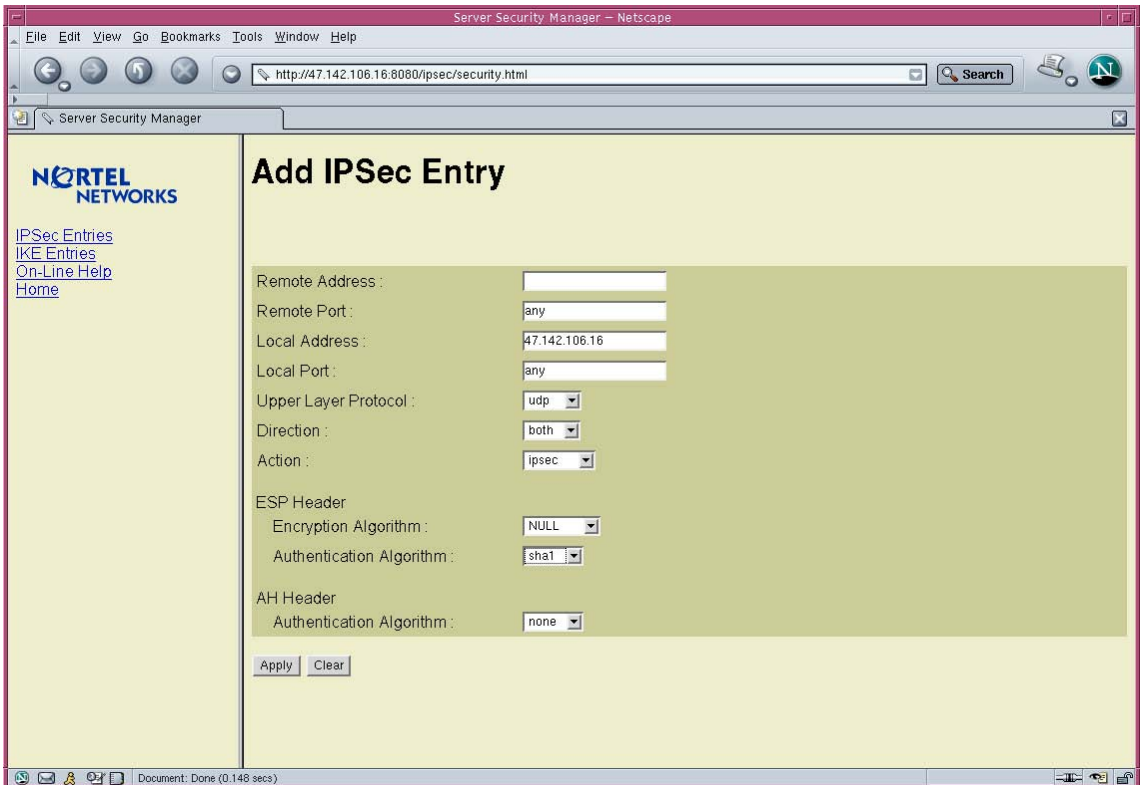
3.8.2.4 IPSec provisioned entries example

The following example shows a number of IPSec entries for an IEMS server:



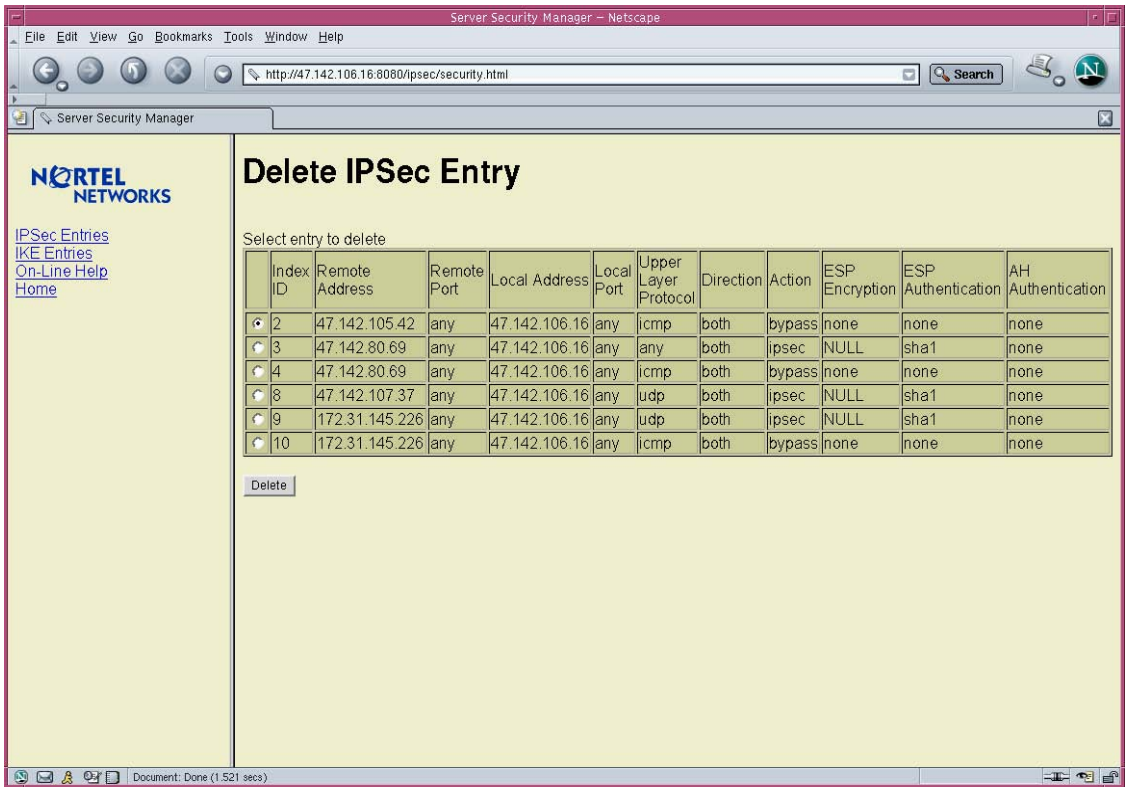
3.8.2.5 IPSec entry form example

The following example shows a form for creating IPSec entries for an IEMS server:



3.8.2.6 IPSec entry deletion example

The following example shows a table for deleting IPSec entries for an IEMS server:



	Index ID	Remote Address	Remote Port	Local Address	Local Port	Upper Layer Protocol	Direction	Action	ESP Encryption	ESP Authentication	AH Authentication
◉	2	47.142.105.42	any	47.142.106.16	any	icmp	both	bypass	none	none	none
○	3	47.142.80.69	any	47.142.106.16	any	any	both	ipsec	NULL	sha1	none
○	4	47.142.80.69	any	47.142.106.16	any	icmp	both	bypass	none	none	none
○	8	47.142.107.37	any	47.142.106.16	any	udp	both	ipsec	NULL	sha1	none
○	9	172.31.145.226	any	47.142.106.16	any	udp	both	ipsec	NULL	sha1	none
○	10	172.31.145.226	any	47.142.106.16	any	icmp	both	bypass	none	none	none

3.8.2.7 Recommended Parameter settings

******This section will need to be verified.******

The following are the recommended parameters to be used when connecting to an OSS

1. Remote Address is the address of the OSS as seen by SSPFS server application, such as IEMS.
2. Remote Port is “any”.
3. Local Address is the address of the SSPFS server as seen by the OSS.
4. Local Port is “any”.
5. Upper Layer Protocol is “any”.
6. Direction is “both”.
7. Action is “ipsec”.
8. ESP Encryption Algorithm is “3des”. (if encryption of data is required)

9 ESP Authentication Algorithm is “sha1”.

10 AH Authentication Algorithm is “none”.

3.8.2.8 IKE fields

The following table lists the security fields for IKE parameters.

Table 2 IKE field descriptions

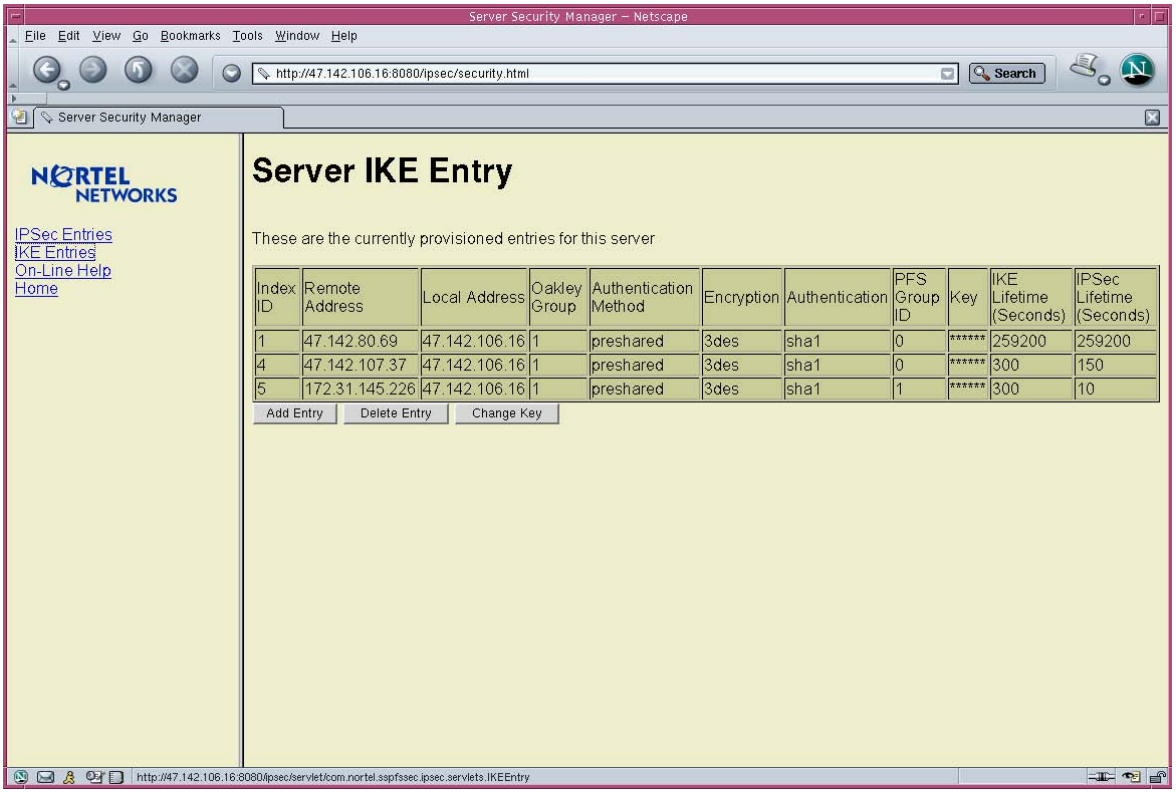
Field	New or Changed	Subfield	Entry	Explanation and action
Index ID	New	No	Integer	Internal index used by the server to track and reference IKE entries.
Remote Address	New	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of the remote system communicating with this server.
Local Address	New	No	A numeric internet IP address of the form: www.xxx.yyy.zzz	IP address of this server.
Oakley Group	New	No	1 (768-bit), 2 (1024-bit), or 5 (1536-bit).	The Oakley Diffie-Hellman group used for IKE Security Association key derivation.
Authentication Method	New	No	Preshared is the only supported option.	The authentication method used for IKE phase 1.
Encryption	New	No	des and 3des	Specifies the encryption algorithm for a Security Association.
Authentication	New	No	sha1 and md5.	Specifies the authentication algorithm for a Security Association.
PFS Group ID	New	No	0 (do not use Perfect Forward Secrecy for IPsec SAs), 1 (768-bit), 2 (1024-bit), and 5 (1536-bit).	The Oakley Diffie-Hellman group used for IPsec Security Association key derivation.
Key	New	No	20 - 120 character ASCII string	Specifies the preshared key for this Security Association.

Table 2 IKE field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action
IKE Lifetime	New	No	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days.	Specifies the lifetime for a IKE phase 1 Security Association.
IPSec Lifetime	New	No	Maximum allowed value is 2,419,200 seconds, 40,320 minutes, 672 hours or 28 days.	Specifies the lifetime for an IPSec Security Association.

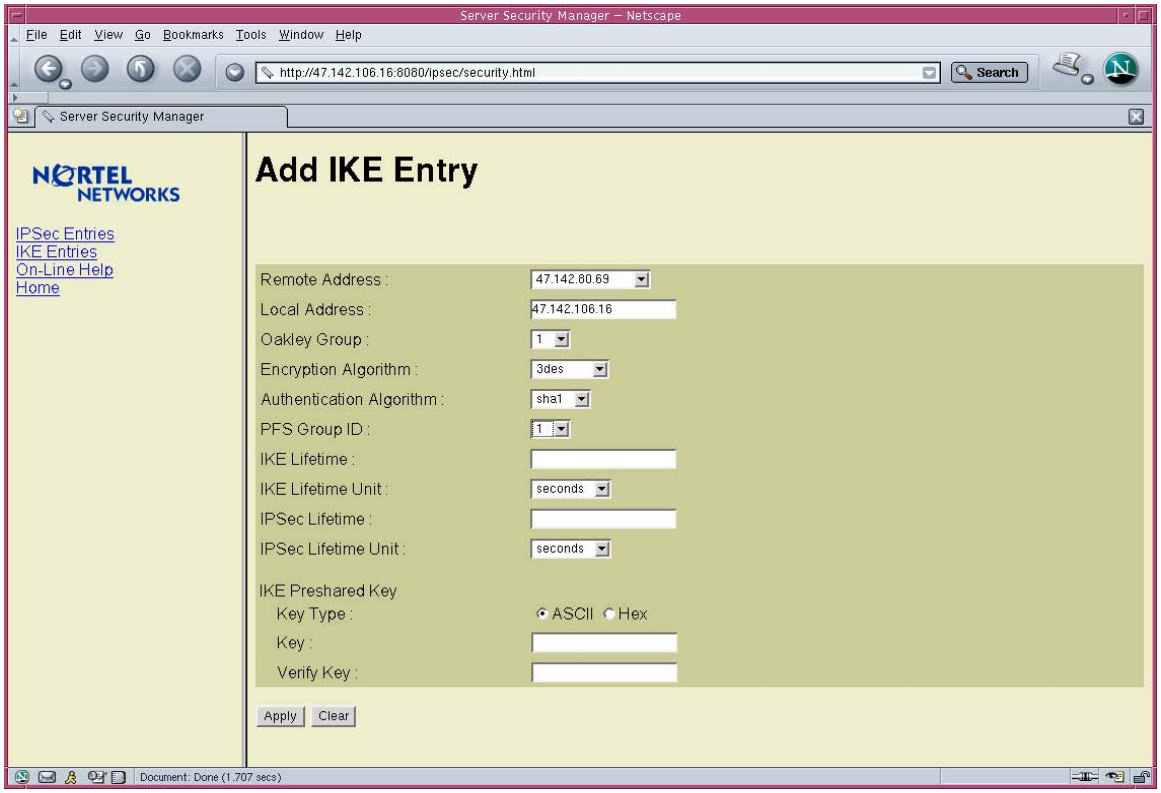
3.8.2.9 IKE provisioned entries example

The following example shows a number of IKE entries for an IEMS server:



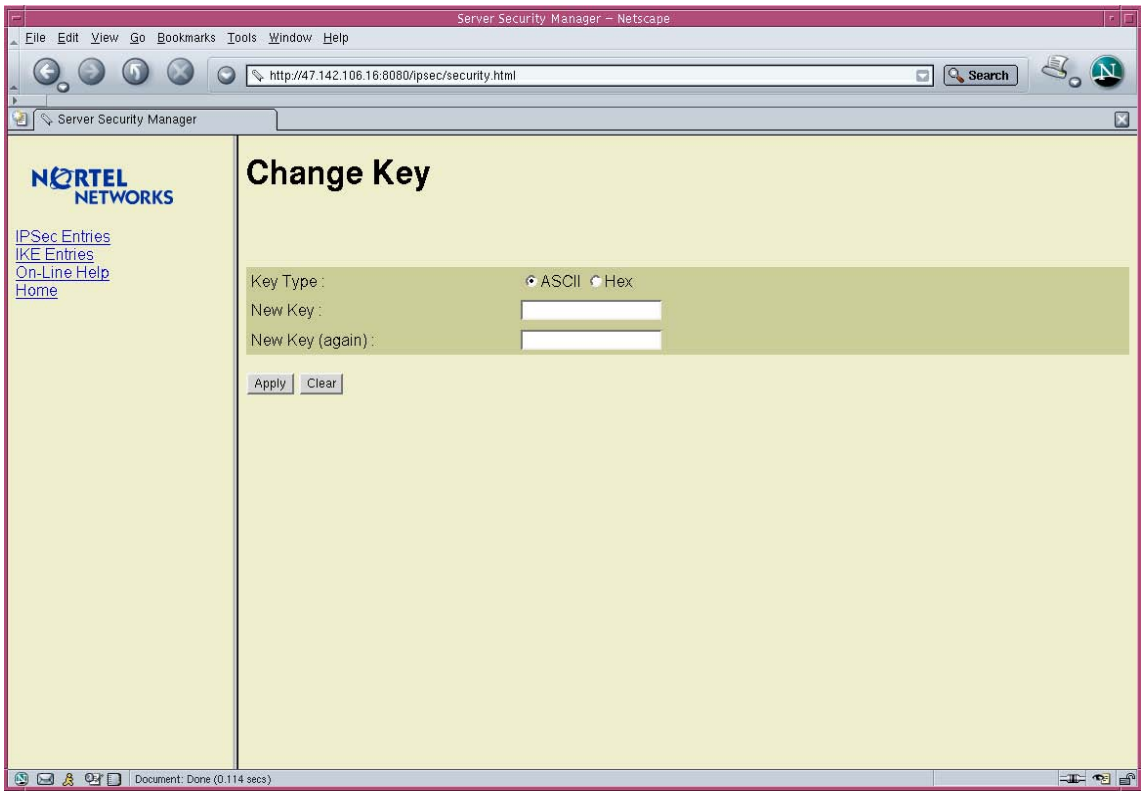
3.8.2.10 IKE entry form example

The following example shows a form for creating IKE entries for an IEMS server:



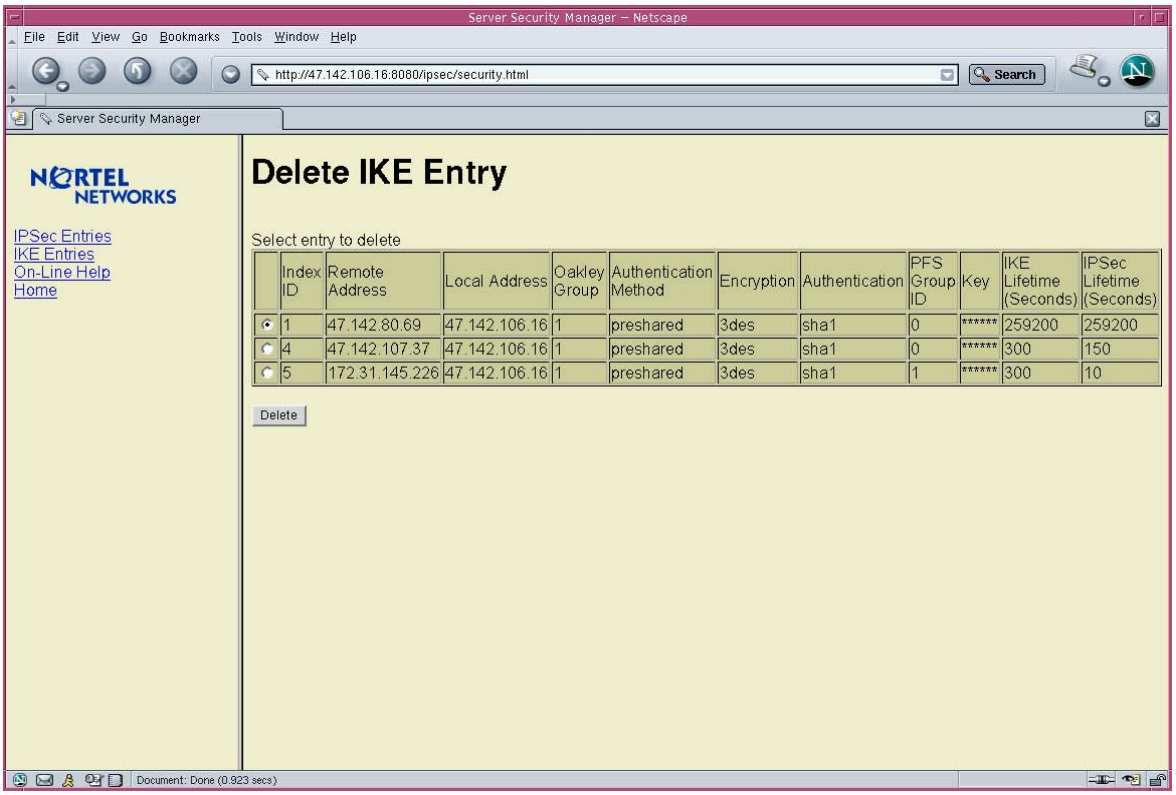
3.8.2.11 IKE change key form example

The following example shows a form for changing an IKE key entry for an IEMS server:



3.8.2.12 IKE entry deletion example

The following example shows a table for deleting IKE entries for an IEMS server:



3.8.2.13 OSS Parameter settings

******This section will need to be verified.******

For each OSS provisioned and requiring IPSec security, one IPSec entry must be created. For each “ipsec” entry there must be a corresponding IKE entry.

The IKE entry must be provisioned as follows:

1. Remote Address is the address of the OSS as seen by SSPFS based application, such as IEMS.
2. Local Address is the address of the OSS as seen by SSPFS based application, such as IEMS.
3. Oakley Group is “1”.
4. Encryption Algorithm is “3des”.
5. Authentication Algorithm is “sha1”.
6. PFS Group ID is “1”.
7. IKE Lifetime is “8”.

8. IKE Lifetime Unit is “hours”.
9. IPSec Lifetime is “8”.
10. IPSec LIfetime Unit is “hours”.
11. Key Type is “ASCII”.
12. Enter the same key that is entered at the OSS. Twice for verification.

3.8.2.14 GUI release history update

The following information was added:

Initial availability.

3.8.2.15 Supplementary information

None

3.8.2.16 CLUI Interface

Not applicable

3.9 Command interface changes

Not applicable

3.10 Security

3.10.1 Network configuration

UDP Port 500 needs to be open on any firewall for IKE.

UDP Port 500 needs to be open on any firewall for IPSec.

3.10.2 Key management

3.10.2.1 IKE Preshared key

The IKE preshared key is input by the user in the Server Security Manager. This key is secured by the use of secure http, if configured, from the browser to the server.

Note: Solaris stores all keys in a hidden system file not accessible by common users but is available to the ROOT user.

3.10.3 Protocol

IPSec is being used on the Solaris machine.

3.10.4 Authentication

A separate Succession Login will be used for Server Security Manager.

3.11 Configuration Walkthrough

3.11.1 OSS Security

From a high-level here are the steps to enable security on the northbound OSS.

1. Load SSPFS server with required SN09 or later software load.
2. Enable security on the OSS to secure the connection to the SSPFS server. Details of this step are beyond the scope of this document as each OSS provisioning mechanism is different.
3. The craftsperson will then use a web browser and connect to the SSPFS server machine's Server Security Manager (SSM). This is done using the item under the EMS Platforms, SSPFS menu at the top, or manually by entering the correct address information in a supported web browser.
4. After logging in, the craftsperson will enable security on communications with the OSS IP address.
5. This will complete securing the OSS link.

Product = Integrated EMS

A00009611-- IEMS Keymile Integration

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Introduction

The UMUX Multi-service Access platform comprises a range of modular multi-service network elements (UMUX 1500/1200/900) and can be configured/managed by Keymile's UMUX Network Element Manager (UNEM).

IEMS serves as an integrated platform for managing various devices. The Keymile devices UNEM/ UMUX NEs Multi-service Access platform will also be managed by IEMS. This document lists the changes that are required in IEMS in order to manage a UMUX device.

The UMUX implements two network management interfaces: GUI and SNMP. IEMS will use the SNMP interface for inventory and fault management. GUI would be used in the form of launches.

1.2 Acronyms used

IEMS – Integrated Element Management System
GUI – Graphical User Interface
SNMP – Simple Network Management Protocol

1.3 IEMS Changes

1.3.1 UNEM Provisioning

The UNEM can be provisioned in IEMS as an Element Manager. The UNEM can be added from the existing Tools-->Add-->EMS / NE menu. The IPAddress field represents the IP of the UNEM . 'Type' should be selected as EMS. In the 'Device Type' a new entry, named 'UNEM Mgr', will be added. The SNMP details can be filled up on the next screen. This would be the same as the existing Fault Interface screen for other snmp devices.

1.3.2 Topology

The UNEM would be listed under the Element Managers node of the topology tree. As there can be multiple UNEM networks, each network is represented as a separate tree node. The topology tree for the UNEM device is as below

1.3.2.1 Element Mangers

- EMS-UNEM-Mgr (displayName of the UNEM)
- EMS-UNEM-Mgr (displayName of the UNEM)

1.3.2.2 Network elements

The UMUX Network Elements (UMUX 900/UMUX1200 & UMUX1500) will be auto discovered and added to the inventory. These network Elements will be represented in the tree as below

Network Elements
|-UMUX-1200
|-UMUX-1200-(displayName of the UNEM)
|-UMUX-1200-(displayName of the UNEM)
|-UMUX-900
|-UMUX-900-(displayName of the UNEM)
|-UMUX-900-(displayName of the UNEM)
|-UMUX-1500
|-UMUX-1500-(displayName of the UNEM)
|-UMUX-1500-(displayName of the UNEM)

The UMUX -1200 map will contain all the nodes of NE type (UMUX-1200) of a given UNEM Mgr which will be indicated using the displayName of the UNEM Mgr.

The UMUX -900 map will contain all the nodes of NE type (UMUX-900) of a given UNEM Mgr which will be indicated using the displayName of the UNEM Mgr.

The UMUX -1500 map will contain all the nodes of NE type (UMUX-1500) of a given UNEM Mgr which will be indicated using the displayName of the UNEM Mgr.

The neTable with the below mentioned information will be used to populate the Inventory table for the UMUX devices.

neFamily,neIndex,neName,neUNEMAdress,neType,

neFamily + neIndex -- will be the unique name of the UMUX devices

neName -- will be mapped to the displayName

neType – will represent the type of the device (family)

1.3.2.3 Inventory Synchronization

The Inventory Synchronization can happen on the below mentioned conditions:

- While IEMS is restarted
- When ever a trap loss is detected, IEMS will automatically invoke reSync of Inventory.
- Manually invoking the ReSync Inventory

1.3.3 Topology Trap handling

The below mentioned topology traps will be handled:

- neAddedTrap -- IEMS checks for the type of the device and if the type is either
- (neType-11, neType-8, neType-7) the same will be added to the inventory table. All other traps will be considered as traps from unknown devices and the traps will anyway be forwarded to the north bound as INFO events.
- neDeletedTrap – IEMS checks for the corresponding entry in the inventory table and deletes the device. For all the traps originating from the unknown device and the trap will be forwarded as an INFo event to north bound.
- neNameChangeTrap – IEMS checks for the corresponding entry in the inventory table and changes the neName (displayName) of the device. For all the traps originating from the unknown device and the trap will be forwarded as an INFo event to north bound.
- neOpStatModifiedTrap – IEMS will just forward the trap to the NorthBound as INFO events and will not store them in the Alarms table.

- nePollStatModifiedTrap - IEMS will just forward the trap to the NorthBound as INFO events and will not store them in the Alarms table.
- CardAddedTrap – IEMS will forward the trap to the NorthBound as INFO events and will not store them in the Alarms Table.
- CardDeletedTrap – IEMS will forward the trap to the NorthBound as INFO events and will not store them in the Alarms Table.

All the system traps (alarmNEFamily – 4 & alarmNE – 9999) will be mapped to the UNEM

2: Fault Management for A00009611

2.1 Fault management strategy

The Fault management interface employed by IEMS for the Keymile UNEM and UMUX devices will be based on SNMP. The design uses the fault data that the UNEM server sends on behalf of the UMUX devices it manages as well as itself in the northbound direction and makes the required conversions into a well-defined format at the IEMS layer. The IEMS does not provide a one-to-one mapping between the Keymile UNEM and UMUX alarms, rather it groups the alarms based on X.733 categories.

2.2 Northbound Events (Alarm and Logs)

2.2.1 Communication Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing communication condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 3: Communication Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	300
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised
Category	Communication
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text

Table 3: Communication Alarm

Field	Value
Action	Please refer to the alarm text and consult the appropriate UNEM or UMUX User Guide for the appropriate action.

2.2.1.1 NTSTD Format Sample

wnc0s0jn *** UMUX300 MAR29 05:09:44 0482 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: communication
Cause: others
Time: Mar 29 05:09:44 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Specific Problem: others
Description: AIS Received

2.2.1.2 SCC2 Format Sample

**46 UMUX300 0009 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: communication
Cause: others
Time: Mar 17 13:46:27 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Specific Problem: others
Description: Loss of Signal

2.2.1.3 Syslog Format Sample

Apr 8 01:27:24 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9447~~ UMUX300 CRIT TBL UMUX FLT^M Location: OTT_UMUX_1200^M Notification ID: 0^M State: Raised^M Category: communication^M Cause: others^M Time: Apr 08 01:54:45 2005^M Component Id: LOMIF <12> 2Mbit/s-1 / E12^M Specific Problem: others^M Description: AIS Received

2.2.1.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 11 minutes, 8 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.305:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.18.50.48.48.53.45.52.45.56.44.54.58.51.52.58.48.46.48.44.23905:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 22 00 00:

.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;AIS Received:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX300:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 16:

2.2.2 Equipment Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing equipment condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 4: Equipment Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	301
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised
Category	Equipment
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate Keymile UNEM or UMUX User Guide for the appropriate action.

2.2.2.1 NTSTD Format Sample

wnc0s0jn *** UMUX301 MAR23 08:36:30 0483 TBL UMUX FLT
Location: RTP_UMUX_1500
Notification ID: 0
State: Raised
Category: equipment
Cause: others

Time: Mar 23 08:36:30 2005
Component Id: COBUX <11> Board / Network Element
Specific Problem: others
Description: SW Installation Error

2.2.2.2 SCC2 Format Sample

*C16 UMUX301 0011 TBL UMUX FLT
Location: RTP_UMUX_1500
Notification ID: 0
State: Raised
Category: equipment
Cause: others
Time: Mar 30 08:16:32 2005
Component Id: COBUX <12> Board
Specific Problem: others
Description: Unit Not Available

2.2.2.3 Syslog Format Sample

Apr 8 01:22:48 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9442~~ UMUX301 CRIT TBL UMUX FLT^M Location: OTT_UMUX_1200^M Notification ID: 0^M State: Raised^M Category: equipment^M Cause: others^M Time: Apr 08 01:49:02 2005^M Component Id: LOMIF <12> Board^M Specific Problem: others^M Description: Unit Not Available

2.2.2.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 7 minutes, 51 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.305:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.53.45.52.45.56.44.54.58.51.48.58.52.51.46.48.44.23882:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 1e 2b 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;Unit Not Available:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX301:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 15:

2.2.3 Environmental Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing environmental condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 5: Environmental Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	302
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised
Category	Environmental
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate UNEM or UMUX User Guide for the appropriate action.

2.2.3.1 NTSTD Format Sample

wnc0s0jn *** UMUX302 MAR23 08:36:32 0483 TBL UMUX FLT
Location: RTP_UMUX_1500
Notification ID: 0
State: Raised
Category: environmental
Cause: others
Time: Mar 23 08:36:30 2005
Component Id: COBUX <11> Board / Network Element
Specific Problem: others
Description: Alarm Active

2.2.3.2 SCC2 Format Sample

24 UMUX302 0001 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: environmental
Cause: others
Time: Mar 17 00:24:26 2005

Component Id: COBUX <11> Board / External Input-1
Specific Problem: others
Description: Alarm Active

2.2.3.3 Syslog Format Sample

Apr 8 01:38:28 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9452~~ UMUX302 TBL UMUX FLT^M Location: OTT_UMUX_1200^M Notification ID: 0^M State: Raised^M Category: environmental^M Cause: others^M Time: Apr 08 02:05:48 2005^M Component Id: COBUX <11> Board / External Input-1^M Specific Problem: others^M Description: Alarm Active

2.2.3.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 16 minutes, 50 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.302:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.53.45.52.45.56.44.54.58.51.57.58.51.56.46.48.44.23930:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 27 26 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;Alarm Active:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX302:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 18:

2.2.4 Processing Error Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing processing error condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 6: Processing Error Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	303
Severity	Minor, Major, or Critical

Table 6: Processing Error Alarm

Field	Value
Event Type	TBL
State	Raised
Category	Processing Error
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate UNEM or UMUX User Guide for the appropriate action.

2.2.4.1 NTSTD Format Sample

wnc0s0jn *** UMUX303 APR21 09:39:32 0483 TBL UMUX FLT
Location: SIMULATED
Notification ID: 0
State: Raised
Category: processingError
Cause: others
Time: Apr 21 08:55 2005
Component Id: SIMULATED
Specific Problem: others
Description: SIMULATED

2.2.4.2 SCC2 Format Sample

34 UMUX303 0001 TBL UMUX FLT
Location: SIMULATED
Notification ID: 0
State: Raised
Category: processingError
Cause: others
Time: Mar 17 10:24:26 2005
Component Id: SIMULATED
Specific Problem: others
Description: SIMULATION

2.2.4.3 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 4 hours, 16 minutes, 55 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.302:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.53.45.52.45.56.44.54.58.51.57.58.51.56.46.48.44.23930:

.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 27 26 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;Alarm Active:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX303:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=SIMULATED;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 18:

2.2.5 Quality of Service Alarms

The UNEM proxy agent sends an alarmRaisedTrap when an event on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) causes a standing quality of service condition and has immediate or potential impact on the operation or performance of the entity in question.

Table 7: Quality of Service Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	304
Severity	Minor, Major, or Critical
Event Type	TBL
State	Raised
Category	Quality of Service
Probable Cause	Please refer to the alarm text
Description	Please refer to the alarm text
Action	Please refer to the alarm text and consult the appropriate UNEM or UMUX User Guide for the appropriate action.

2.2.5.1 NTSTD Format Sample

wnc0s0jn * UMUX304 MAR29 05:40:44 0499 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: qualityOfService
Cause: others

Time: Mar 29 05:40:44 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Specific Problem: others
Description: Near End Degraded Performance

2.2.5.2 SCC2 Format Sample

45 UMUX304 0001 TBL UMUX FLT
Location: OTT_UMUX_1200
Notification ID: 0
State: Raised
Category: qualityOfService
Cause: others
Time: Mar 17 12:24:26 2005
Component Id: COBUX <11> Board / External Input-1
Specific Problem: others
Description: Near End Degraded Performance

2.2.5.3 Syslog Format Sample

Apr 8 01:28:28 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9449~~ UMUX304 MINOR TBL UMUX FLT^M Location: OTT_UMUX_1200^M Notification ID: 0^M State: Raised^M Category: qualityOfService^M Cause: others^M Time: Apr 08 01:55:49 2005^M Component Id: LOMIF <12> 2Mbit/s-1 / E12^M Specific Problem: others^M Description: Near End Degraded Performance

2.2.5.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 12 minutes, 24 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.303:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.116.19.50.48.48.53.45.52.45.56.44.54.58.51.53.58.49.51.46.48.44.23909:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 06 23 0d 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;Near End Degraded Performance:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX304:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.6: INTEGER: 1:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 17:

2.2.6 Alarm Clear

The UNEM proxy agent sends an alarmClearedTrap when a standing condition on a UNEM managed entity (i.e. a managed UMUX NE or the UNEM itself) has been removed.

Table 8: Alarm Clear Event

Field	Value
Log Name	UNEM or UMUX
Log Number	500
Event Type	INFO
State	Cleared
Description	The standing alarm condition has been cleared
Action	N/A

2.2.6.1 NTSTD Format Sample

wnc0s0jn UMUX500 DEC31 19:00:00 0503 INFO UMUX Clear
Location: OTT_UMUX_1200
State: Cleared
Time: Mar 29 05:37:27 2005
Component Id: COBUX <11> Board / External Input-1
Description: Alarm Active

2.2.6.2 SCC2 Format Sample

00 UMUX500 0018 INFO UMUX Clear
Location: OTT_UMUX_1200
State: Cleared
Time: Mar 31 03:48:34 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Description: Loss of Signal

2.2.6.3 Syslog Format Sample

Apr 8 01:25:04 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9445~~ UMUX500 NONE INFO
UMUX Clear^M Location: OTT_UMUX_1200^M State: Cleared^M
Time: Apr 08 01:25:04 2005^M Component Id: LOMIF <12> Board^M
Description: Unit Not Available

2.2.6.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 2 minutes, 31 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.301:

.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.10: STRING:
.1.3.6.1.2.1.118.1.2.2.1.10.12.78.111.114.116.101.108.95.102.97.117.108.11
6.18.50.48.48.53.45.52.45.56.44.51.58.57.58.51.52.46.48.44.23459:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.2: 07 d5 04 08 03 09 22 00:
.iso.org.dod.internet.mgmt.mib-2.118.1.2.2.1.11: STRING:
DeviceSpecificInfo=;H.248 Association Failure:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.1: INTEGER: 5:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.2: INTEGER: 1024:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.3: STRING: :
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.4: STRING:
UMUX500:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.5: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-33;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.1.1.7: INTEGER: 14:

2.2.7 Operational State Change

The following notification type defines the neOpStatModified trap. It indicates a change in the operational state of a UMUX NE.

Table 9: Operation State Change Event

Field	Value
Log Name	UMUX
Log Number	501
Event Type	INFO
State	INFO
Description	The operational state of a UMUX NE has changed
Action	Please refer to the UMUX User Guide for the appropriate action.

2.2.7.1 NTSTD Format Sample

wnc0s0jn UMUX501 MAR29 05:37:27 0515 neOperationalState Change
Location: OTT_UMUX_1200_Test
State: INFO
Time: Mar 29 05:37:27 2005
Component Id: OTT_UMUX_1200_TestOTT_UMUX_1200_Test
Description: op state has transitioned

2.2.7.2 SCC2 Format Sample

33 UMUX501 0014 INFO neOperationalState Change
Location: OTT_UMUX_1200
State: INFO
Time: Mar 31 03:33:27 2005

Component Id: OTT_UMUX_1200OTT_UMUX_1200
Description: op state has transitioned

2.2.7.3 Syslog Format Sample

Apr 8 00:58:13 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9433~~ UMUX501 NONE INFO neOperationalState Change^M Location: OTT_UMUX_1200^M State: INFO^M Time: Apr 08 00:58:13 2005^M Component Id: OTT_UMUX_1200OTT_UMUX_1200^M Description: OTT_UMUX_1200 op state has transitioned 52

2.2.7.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 41 minutes, 42 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING: IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: 07 d5 04 08 06 25 0a 00:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING: UMUX501:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 37 UMUX501 0000 INFO neOperationalState Change :
OTT_UMUX_1200_TESTING op state has transitioned 52:

2.2.8 Polling State Change

The following notification type defines the nePollStatModified trap. It indicates that the UNEM's polling status of the UMUX NE has been modified

Table 10: Polling State Change Event

Field	Value
Log Name	UMUX
Log Number	502
Event Type	INFO
State	INFO
Description	The Polling state of a UMUX NE has changed
Action	Please refer to the UMUX User Guide for the appropriate action.\

2.2.8.1 NTSTD Format Sample

wnc0s0jn UMUX502 MAR29 05:26:57 0508 nePollState Change

Location: OTT_UMUX_1200
State: INFO
Time: Mar 29 05:26:57 2005
Component Id: OTT_UMUX_1200OTT_UMUX_1200
Description: op state has transitioned

2.2.8.2 SCC2 Format Sample

24 UMUX502 0006 INFO nePollState Change
Location: OTT_UMUX_1200
State: INFO
Time: Mar 31 03:24:15 2005
Component Id: OTT_UMUX_1200OTT_UMUX_1200
Description: op state has transitioned

2.2.8.3 Syslog Format Sample

Apr 8 00:44:59 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9430~~ UMUX502 NONE INFO nePollState Change^M Location: RTP_UMUX_1500^M State: INFO^M Time: Apr 08 00:44:59 2005^M Component Id: RTP_UMUX_1500RTP_UMUX_1500^M Description: RTP_UMUX_1500 polling state has transitioned 1

2.2.8.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours, 28 minutes, 48 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING: IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: 07 d5 04 08 05 18 10 00:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING: UMUX502:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 24 UMUX502 0000 INFO nePollState Change :
OTT_UMUX_1200 polling state has transitioned 1:

2.2.9 Alarm Acknowledgment

The UNEM proxy agent sends an alarmAckedTrap when an outstanding alarm has been acknowledged. IEMS will simply forward the event northbound. IEMS will not reflect this trap in its alarm list.

Table 11: Alarm Acknowledgment

Field	Value
Log Name	UNEM or UMUX

Table 11: Alarm Acknowledgment

Field	Value
Log Number	600
Event Type	INFO
State	INFO
Description	This informational log is sent when an alarm is acknowledged by the UNEM system.
Action	N/A

2.2.9.1 NTSTD Format Sample

wnc0s0jn UMUX600 MAR29 05:38:44 0485 INFO UMUX Ack
Location: OTT_UMUX_1200
State: INFO
Time: Mar 29 05:38:44 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Description: AIS Received

2.2.9.2 SCC2 Format Sample

00 UMUX600 0016 INFO UMUX Ack
Location: OTT_UMUX_1200
State: INFO
Time: Mar 31 03:48:34 2005
Component Id: LOMIF <12> 2Mbit/s-1 / E12
Description: Loss of Signal

2.2.9.3 Syslog Format Sample

Apr 8 01:25:44 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9446~~ UMUX600 NONE INFO
UMUX Ack^M Location: OTT_UMUX_1200^M State: INFO^M
Time: Apr 08 03:52:32 2005^M Component Id: LOMIF <12> Board^M
Description: Unit Not Available

2.2.9.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 3 hours, 8 minutes, 43 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING: IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: 07 b1 0c 1f 07 00 00 00:

.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX600:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 00
UMUX600 0057 INFO UMUX Ack :
Unit Not Available:

2.2.10 NE Add

The UNEM proxy agent sends an neAdded trap when a UMUX NE has been added to the UNEM topology inventory. In addition to adding the NE to it's topology, IEMS forwards the informational event NB.

Table 12: Communication Alarm

Field	Value
Log Name	UMUX
Log Number	601
Event Type	INFO
State	INFO
Description	<UMUX Name> NE Added
Action	N/A

2.2.10.1 NTSTD Format Sample

wnc0s0jn UMUX601 MAR29 05:35:35 INFO UMUX Added
Location: OTT_UMUX_1200_Test
State: INFO
Time: Mar 29 05:35:35 2005
Component Id: OTT_UMUX_1200_Test797322492
Description: OTT_UMUX_1200_Test NE Added

2.2.10.2 SCC2 Format Sample

54 UMUX601 0023 INFO UMUX Added
Location: OTT_UMUX_TESTING
State: INFO
Time: Mar 31 03:54:48 2005
Component Id: OTT_UMUX_TESTING 47.134. 44.110
Description: OTT_UMUX_TESTING NE Added

2.2.10.3 Syslog Format Sample

Apr 8 00:59:37 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9434~~ UMUX601 NONE INFO
UMUX Added^M Location: MYTest^M State: INFO^M Time:

Apr 08 00:59:37 2005^M Component Id: MYTest 10. 1. 5. 1^M
Description: MYTest NE Added

2.2.10.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours, 48 minutes, 38 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING: IEMS=wcarhw4e.ca.nortel.com-UMUX-37;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E,^F^B:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING: UMUX601:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 44 UMUX601 0047 INFO UMUX Added :
UMUX_TESTING(10. 10. 1. 1) NE Added :

2.2.11 NE Deleted

The UNEM proxy agent sends an neDeleted trap when a UMUX NE has been deleted from the UNEM topology inventory. In addition to adding the NE to it's topology, IEMS forwards the informational event NB.

Table 13: Communication Alarm

Field	Value
Log Name	UMUX
Log Number	602
Event Type	INFO
State	INFO
Description	<UMUX Name> NE Deleted
Action	N/A

2.2.11.1 NTSTD Format Sample

wnc0s0jn UMUX602 MAR29 05:40:38 0524 INFO UMUX Deleted
Location: OTT_UMUX_1200_Test
State: INFO
Time: Mar 29 05:40:38 2005
Component Id: OTT_UMUX_1200_Test797322492
Description: OTT_UMUX_1200_Test NE Deleted

2.2.11.2 SCC2 Format Sample

33 UMUX602 0051 INFO UMUX Deleted
Location: RTP_UMUX_1500_TEST
State: INFO
Time: Mar 31 04:33:36 2005
Component Id: RTP_UMUX_1500_TEST 47.142. 87.102
Description: RTP_UMUX_1500_TEST NE Deleted

2.2.11.3 Syslog Format Sample

Apr 8 01:00:18 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9435~~ UMUX602 NONE INFO
UMUX Deleted^M Location: MYTest^M State: INFO^M Time:
Apr 08 01:00:18 2005^M Component Id: MYTest 10. 1. 5. 1^M
Description: MYTest NE Deleted

2.2.11.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours,
50 minutes, 9 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-37;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E-%:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX602:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 45
UMUX602 0048 INFO UMUX Deleted :
UMUX_TESTING(10. 10. 1. 1) NE Deleted :

2.2.12 NE Name Modified

The UNEM proxy agent sends an neNameModified trap when a UMUX NE Name is changed in the UNEM. IEMS forwards this information event northbound.

Table 14: Communication Alarm

Field	Value
Log Name	UMUX
Log Number	603
Event Type	INFO
State	INFO
Description	<UMUX Name> NE Name Change

Table 14: Communication Alarm

Field	Value
Action	N/A

2.2.12.1 NTSTD Format Sample

wnc0s0jn UMUX603 MAR29 05:36:25 0514 INFO UMUX Name Change
Location: OTT_UMUX_1200_Test
State: INFO
Time: Mar 29 05:36:25 2005
Component Id: OTT_UMUX_1200_Test 47.134. 44.252
Description: OTT_UMUX_1200_Test NE Name Change

2.2.12.2 SCC2 Format Sample

31 UMUX603 0013 INFO UMUX Name Change
Location: OTT_UMUX_1200
State: INFO
Time: Mar 31 03:31:50 2005
Component Id: OTT_UMUX_1200 47.134. 44.252
Description: OTT_UMUX_1200 NE Name Change

2.2.12.3 Syslog Format Sample

Apr 8 01:01:54 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9436~~ UMUX603 NONE INFO
UMUX Name Change ^M Location: RTP_UMUX_1500_MYTEST^M
State: INFO^M Time: Apr 08 01:01:54 2005^M Component Id:
RTP_UMUX_1500_MYTEST 47.142. 87.102^M Description:
RTP_UMUX_1500_MYTEST NE Name Change

2.2.12.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours,
46 minutes, 45 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-15;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E*
:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX603:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 42
UMUX603 0045 INFO UMUX Name Change :
OTT_UMUX_1200_TESTING(797322492) NE Name Changed :

2.2.13 Card Added

The UNEM proxy agent sends a cardAdded event when a card has been added to a managed UMUX inventory. IEMS forwards the event northbound as an informational.

Table 15: Communication Alarm

Field	Value
Log Name	UMUX
Log Number	604
Event Type	INFO
State	INFO
Description	<Card Name> has been added to <NE Name> at <Slot No.>
Action	N/A

2.2.13.1 NTSTD Format Sample

wnc0s0jn UMUX604 APR21 02:54:35 0190 INFO UMUX Card Added
Location: IPSMG
State: INFO
Time: Apr 21 02:54:35 2005
Component Id: IPSMGRTP_UMUX_1500
Description: IPSMG has been added to RTP_UMUX_1500 at 19

2.2.13.2 SCC2 Format Sample

28 UMUX604 0004 INFO UMUX Card Added
Location: RTP_UMUX_1500
State: INFO
Time: Apr 06 00:28:39 2005
Component Id: RTP_UMUX_1500
Description: ISBUQ has been added to RTP_UMUX_1500 at 17

2.2.13.3 Syslog Format Sample

Apr 8 01:09:27 wnc0s0jn IEMS: _V2_~I=~H=wnc0s0jn~A=IEMS~S=9440~~ UMUX604 NONE INFO UMUX Card Added^M Location: ISBUQ^M State: INFO^M Time: Apr 08 01:09:27 2005^M Component Id: ISBUQRTP_UMUX_1500_MYTEST^M Description: ISBUQ has been added to RTP_UMUX_1500_MYTESTat 17

2.2.13.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours, 57 minutes, 19 seconds.:

.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-33;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING:
^G^E4/^B:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX604:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 52
UMUX604 0000 INFO UMUX Card Added :

2.2.14 Card Deleted

The UNEM proxy agent sends a cardDeleted event when a card has been deleted from a managed UMUX inventory. IEMS forwards the event northbound as an informational.

Table 16: Communication Alarm

Field	Value
Log Name	UNEM or UMUX
Log Number	605
Event Type	INFO
State	INFO
Description	<Card Name> has been deleted from <NE Name> at <Slot No.>
Action	N/A

2.2.14.1 NTSTD Format Sample

wnc0s0jn UMUX605 APR21 02:54:35 0190 INFO UMUX Card Deleted
Location: IPSMG
State: INFO
Time: Apr 21 02:54:35 2005
Component Id: IPSMGRTP_UMUX_1500
Description: IPSMG has been deleted from RTP_UMUX_1500 at 19

2.2.14.2 SCC2 Format Sample

30 UMUX605 0004 INFO UMUX Card Deleted
Location: RTP_UMUX_1500
State: INFO
Time: Apr 06 00:38:35 2005
Component Id: RTP_UMUX_1500
Description: ISBUQ has been deleted from RTP_UMUX_1500 at 17

2.2.14.3 Syslog Format Sample

Apr 8 01:07:18 wnc0s0jn IEMS:
_V2_~I=~H=wnc0s0jn~A=IEMS~S=9437~~ UMUX605 NONE INFO
UMUX Card Deleted^M Location: ISBUQ^M State: INFO^M
Time: Apr 08 01:07:18 2005^M Component Id:
ISBUQRTP_UMUX_1500_MYTEST^M Description: ISBUQ has been
deleted from RTP_UMUX_1500_MYTESTat 17

2.2.14.4 SNMP Format Sample

.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0: TimeTicks: 2 hours,
54 minutes, 12 seconds.:
.iso.org.dod.internet.6.3.1.1.4.1.0: Object ID: .1.3.6.1.4.1.562.29.6.1.0.306:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.1: STRING: .0.0:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.2: STRING:
IEMS=wcarhw4e.ca.nortel.com-UMUX-33;:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.3: STRING: ^G^E1(
:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.4: STRING:
UMUX605:
.iso.org.dod.internet.private.enterprises.562.29.6.1.3.1.5: STRING: 49
UMUX605 0000 INFO UMUX Card Deleted :

3: Configuration for A00009611

3.1 UNEM GUI Launch

- Launch UNEM Network browser
- UMUX shelf Configuration GUI

3.1.1 Launch UNEM Network Browser

While adding the UNEM, an additional parameter is provided to specify if the SSH is enabled or not in the device

3.1.2 SSH Enabled

Linux
While launching the UNEM Network browser / UMUX Shelf Configuration a dialog will come up to provide the username/password, IEMS will use the X11 port forwarding and bring up the appropriate GUI.

Windows
While launching the UNEM Network browser/UMUX Shelf Configuration, a dialog box with provision to provide Exceed file path and the login/password using which the appropriate GUI will be brought up.

3.1.3 SSH Disabled

Linux

For solaris clients IEMS will invoke the default Telnet prompt. User has to do the rest manually for invoking the GUI.

Windows
While invoking the UNEM Network Browser / UMUX Shelf Configuration, IEMS client will use the xstart.exe(Exceed tool) to launch the GUI in non-encryption mode.

3.1.4 Launching from the UMUX

The SSH enabled (true/false) value provided for the UNEM while addition will be updated for all the UMUX (NEs). If the SSH is enabled in the UNEM, the launch UMUX shelf configuration from the UMUX devices will try to launch through SSH. If SSH is not enabled in the UNEM device, the launch will fail and the user can subsequently modify the SSH property to disable and proceed with the launch.

3.1.5 Commands used for launch

UNEM Network Browser -- **/usr/local/bin/nocslogin -e ec**

UMUX Shelf Configuration -- **/usr/local/bin/nocslogin -e ne -i**

Windows NON SSH Mode

UNEM Network Browser -- **/usr/local/bin/nocrlogin -e ec -s auto -d**

UMUX Shelf configuration -- **/usr/local/bin/nocrlogin -e ne -i**

3.2 Launching UNEM Browser for UNEM

The UNEM browser for UNEM version 9.0 can be launched from Integrated EMS Java Web Start Client. This procedure describes how to launch the UNEM browser from Integrated EMS Java Web Start Client.

Note: The launching of UNEM Browser works only if the Patch Collection 1 is installed on the UNEM Server.

3.2.1 To launch UNEM browser for UNEM version 9.0, follow these steps:

At Integrated EMS workstation

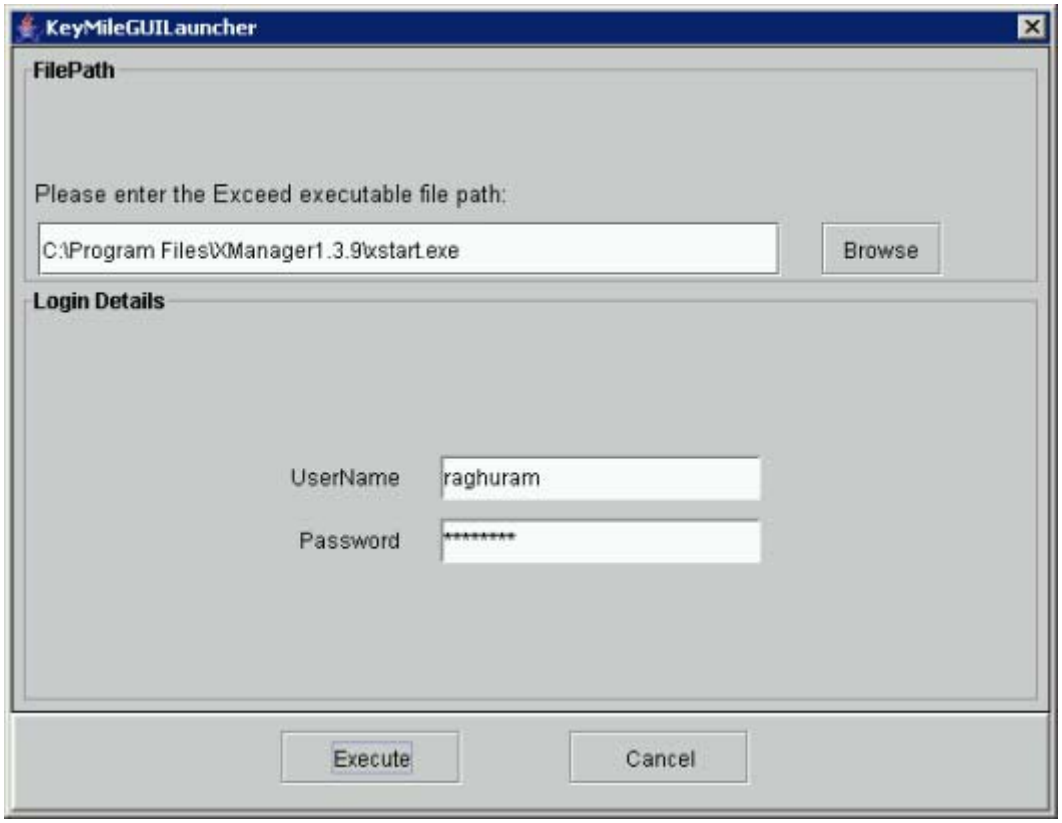
1 Launch the Integrated EMS Java Web Start Client (refer to "Launching the Integrated EMS Java Web Start Client.")

2 Go to the **Element Managers** topology in the Integrated EMS tree.

3 Select an UNEM map symbol.

4 Right-click the map symbol and select the **Launch UNEM Browser** menu item.

The system displays a window similar to the following screen shot for the Integrated EMS Client in Microsoft Windows platform.



5 For Microsoft Windows-based client, click the **Browse** button to select the Exceed application executable file path. This step is not applicable for Solaris-based clients as this field is not present.

Note: For launching the application without SSH, "xstart.exe" must be selected and "exceed.exe" must be selected for launching the application with SSH enabled.

6 Type the user name and password in the respective fields.

7 Click the **Execute** button to execute the specified command.

Note: Integrated EMS saves the location of the script or the executable file and commands in the client system from which the Integrated EMS Java Web Start Client is launched.

3.3 Launching applications for UMUX NEs

The UNEM browser and UMUX Shelf Configuration GUI for UMUX NEs (UMUX 1500, UMUX 1200, and UMUX 900 NEs) version 9.0 can be

launched from Integrated EMS Java Web Start Client. This procedure describes how to launch the UNEM browser from Integrated EMS Java Web Start Client

Note: The launching of UNEM Browser or UMUX Shelf Configuration works only if the Patch Collection 1 is installed on the UNEM Server.

3.3.1 To launch UNEM browser or UMUX Shelf Configuration GUI for UMUX NEs version 9.0, follow these steps:

At Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to "Launching the Integrated EMS Java Web Start Client.")

2 Go to the **Element Managers** topology in the Integrated EMS tree.

3 Select an UMUX NE map symbol.

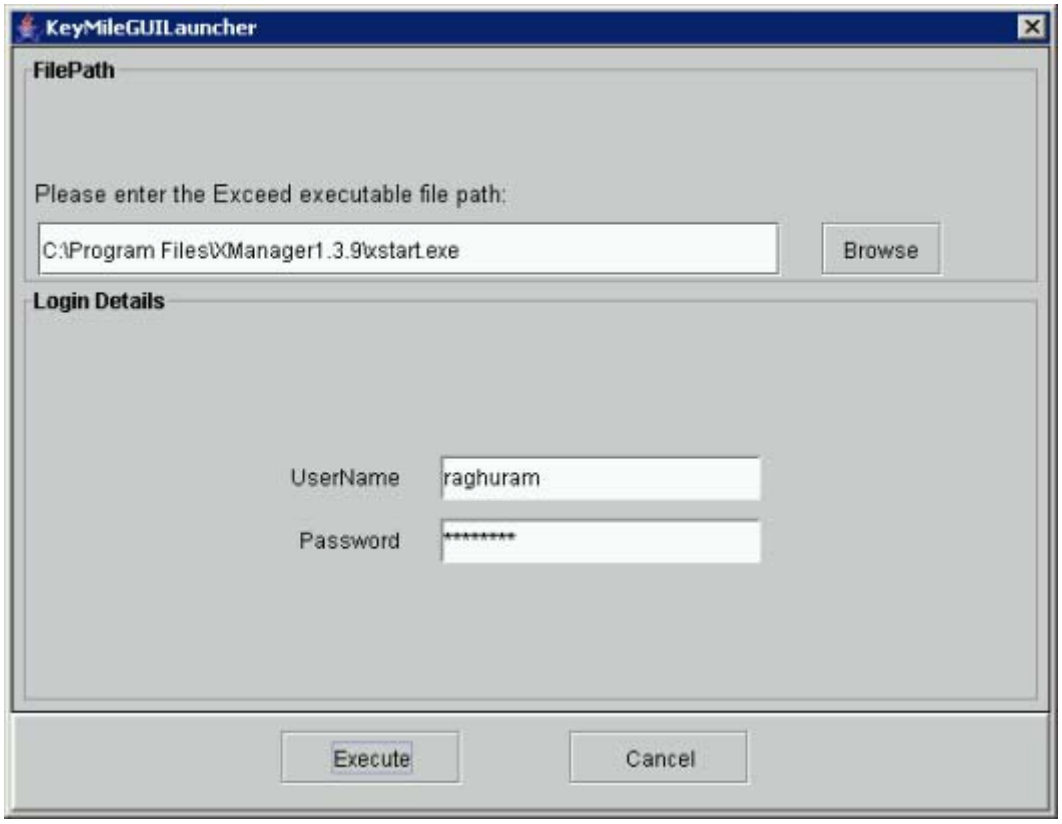
4 Right-click the map symbol and select the **Launch UNEM Browser** menu item.

The system displays a window similar to the following screen shot for the Integrated EMS Client in Microsoft Window platform.

OR

Right-click the map symbol and select the **Launch UMUX Shelf Configuration** menu item.

The system displays a window similar to the following screen shot for the Integrated EMS Client in Microsoft Windows platform.



5 For Microsoft Windows-based client, click the **Browse** button to select the Exceed application executable file path. This step is not applicable for Solaris-based clients as this field is not present.

Note: For launching the application without SSH, "xstart.exe" must be selected and "exceed.exe" must be selected for launching the application with SSH enabled.

6 Type the user name and password in the respective fields.

7 Click the **Execute** button to execute the specified command.

Note: Integrated EMS saves the location of the script or the executable file and commands in the client system from which the Integrated EMS Java Web Start Client is launched.

3.4 Adding a UMUX Network Element Manager (UNEM)

UNEM manages UMUX 1500, UMUX 1200, and UMUX 900 NEs in the UMUX network. The UMUX stands for Universal Multiplexer. When you add an UNEM, these NEs are added as a map symbol under the **Network Elements** topology and **UMUX-1500**, **UMUX-1200**, and **UMUX-900** topology (under **Network Elements** node) respectively. The UNEM is added

as a map symbol in the **Element Managers** topology. Also, the UNEM is added as map symbols in the **EMS-UNEM-Mgr** topology (with added UNEM display name in brackets). This procedure describes how to add the UNEM to the Integrated EMS topology using Integrated EMS Java Web Start Client.

The following list provides the operations available for UNEM in Integrated EMS.

Tasks Supported in Integrated EMS for UNEM

Task in Integrated EMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes
Updating status	Yes	No
Managing or unmanaging the object	Yes	Yes
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	Yes	Yes
Deleting alarms	Yes	Yes
Resynchronizing alarms	Yes	No
Resynchronizing inventory	Yes	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No

Tasks Supported in Integrated EMS for UNEM

Task in Integrated EMS	Availability	
	Java Web Start Client	Web Client
Other operations		
Launching corresponding applications	Yes	No

3.4.1 To add the UNEM to the topology, follow these steps:

At Integrated EMS workstation

1 Launch the Integrated EMS Java Web Start Client (refer to "Launching Integrated EMS Java Web Start Client").

2 Select the **Tools-->Add-->EMS/NE** menu command to invoke the **Add EMS/NE** dialog.

3 Enter the values for the Host Name/IP Address, Time Zone, and Display Name fields in the wizard. For details on these fields, refer to the following table:

Description of fields in Add EMS/NE Wizard

Field	Description
Host Name/IP Address	The field for the host name or IP address of the element manager.
Time Zone	A list box to select the time zone associated with the object.
Display Name	The name that must be displayed in the topology for the map symbol.

4 Select "EMS" from the **Type** list box.

5 Select "UNEM" from the **Device Type** list box.

6 Select the **SSH enabled** field if the SSH is enabled in the UNEM device.

Note: If the SSH enabled field is selected and the UNEM server does not have SSH installed, the launching of UNEM Browser from UNEM and UMUX NEs and launching of UMUX Shelf Configuration fails. For procedure to launch UNEM Browser for UNEM, refer to "Launching UNEM browser for UNEM"

7 Click the **Next** button.

8 In the **Port** field, enter the port value (in which the EMS communicates with Integrated EMS).

9 Enter the community in the **Community** field.

10 Select the SNMP version "v1" from the **Version** list box.

Note: The port value and the SNMP version are dependent on the UNEM configuration that is added.

11 Click the **Next** button.

12 Click the **Finish** button to add the UNEM.

Once the UNEM is added, a message appears in the status bar of the wizard as in the following screen shot:

The UNEM with the specified name is added to the **Element Managers** topology panel. Also, the UNEM is added as map symbols in the topology node named **EMS-UNEM-Mgr** (with the specified display name in brackets).

3.5 Adding UMUX NEs

UNEM manages UMUX 1500, UMUX 1200 and UMUX 900 NEs in the UMUX network. Refer to “Adding a UMUX Network Element Manager (UNEM)” on page 1656 procedure to add a UNEM. When you add an UNEM, these NEs are automatically discovered and added as map symbols under the **Network Elements** topology. Also they are added as map symbols under the **UMUX-1500**, **UMUX-1200**, and **UMUX-900** topology (under **Network Elements** node) respectively.

The following list provides the operations available for UNEM NEs in Integrated EMS.

Tasks Supported in Integrated EMS for UNEM NEs

Task in Integrated EMS	Availability	
	Java Web Start Client	Web Client
Configuration Management		
Editing object properties	Yes	Yes

Tasks Supported in Integrated EMS for UNEM NEs

Task in Integrated EMS	Availability	
	Java Web Start Client	Web Client
Updating status	No	No
Managing or unmanaging the object	No	No
Fault Management		
Viewing associated events or alarms	Yes	Yes
Clearing alarms	No	No
Deleting alarms	No	No
Resynchronizing alarms	No	No
Resynchronizing inventory	No	No
Performance Management		
Data collection job	No	No
Report job	No	No
Transfer job	No	No
Configuring thresholds	No	No
Security		
Centralized authentication and authorization (RADIUS client)	No	No
Other operations		
Launching corresponding applications	Yes	No

3.6 References

IEMS-Keymile_Integration_DID_v2.0.pdf

UMUX (R7) User Guide, LZTBU 320 115 /3

UNEM (R7) User Guide Basic Package, LZTBU 310 106 /2

UNEM (R7) User Guide Networking Package, LZTBU 310 306 /2

Product = Integrated EMS

A00009612 -- Restricted Shell Access

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

The implementation of A00009310 “Restricted Access Shell” in SN09 provides a new default shell for interactive users. This shell (called rash), unlike sh or ksh or bash will limit the available suite of commands. Additionally a user will not be able to alter their path and will therefore be restricted to only those commands authorized. Additional commands can be registered to be available to rash via servman.

Two of the commands used by IEMS that fall into this restricted access morass are telnet and ssh. As a result, the proxied “Command Line” context menu item used from the IEMS map will no longer work. The invocation of the telnet or ssh command will elicit a “command not found” message when invoked from rash.

In a proxied command line scenario the IEMS client uses SSH (Mindterm) to establish and login to a shell session on the IEMS server. From there the ssh or telnet command is issued and another SSH or telnet session is established with the southbound NE or EMS. The shell session on the IEMS server will use the restricted access shell provided by A00009310 and hence will be prohibited from invoking either the telnet or ssh commands.

This component will rectify this and insure that the proxied command line in SN09 will retain functionality equivalent to that found in SN08. A script (IEMSProxyCommandLine) will be created for the telnet and ssh commands on the IEMS server that will,

1 Perform a check to insure that the logged in user is authorized to access the target device. The check will use the same logic and code provided by IEMS. The users membership in the 30 Succession groups and any policy rules defined in the IEMS server will dictate authorization.

2 Create an audit log for successful authorization or a security log for unsuccessful authorization.

3 invoke the real ssh and telnet command to establish a remote session with the target device.

The script will support all options and parameters of both ssh and telnet and will not alter either the performance or appearance.

Additionally a login to the IEMS server will place the user into a restricted access shell with a home directory as defined in users profile in the security server. A script run from pam during login will create the user's home directory and copy skeleton profiles to it.

1.2 Hardware Requirements or Dependencies

Not applicable

1.3 Software Requirements or Dependencies

This is required due to implementation of A00009310.

1.4 Limitations and restrictions

None

1.5 Interactions

1.5.1 IEMSProxyCommandLine script

The IEMSProxyCommandLine script will support all options and parameters of both ssh and telnet and will not alter either the performance or appearance. It does introduce any new options or arguments.

1.5.2 Home Directory and Skeleton Profiles

The home directory of the user will be created. Additionally, two sub-directories of "data" and ".ssh" will be created. The former is read-write and available at the discretion of the user. The latter is used to store public encryption keys used by ssh. Skeleton profiles, shipped with SSPFS and found in /etc/skel.rash, will be copied into the home directory.

1.5.3 Logs

An Audit Log Entry would be found for a successful authorized access.

Feb 22 11:39:37 comp5iems IEMS: IEMS class_security.ver01 STAT=SUCCESS SRC.USR=gumby EVNT.TYPE =/usr/bin/ssh to 47.142.106.26, device type EMS-CS2K-Mgr

A Security Log Entry would be found for an unsuccessful, unauthorized access. Note that for authorization to succeed both the userid and the target

host ipaddress must be known to the IEMS server. If either is unknown then the authorization will fail.

Feb 22 11:39:37 comp5iems IEMS: IEMS class_security.ver01 STAT=FAILURE SRC.USR=gumby EVNT.TYPE =/usr/bin/ssh to 2.3.4.5, device type GWC

1.6 Glossary

Product = Integrated EMS

A00009614 -- Tamper-proof Key Storage and Event Generation
Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

This document will cover work for IEMS and SSPFS. This document does not address key material owned and controlled by the Security Server.

Key material is defined to be anything that is used to authenticate a user or machine to another machine. This includes X.509 certificates, cryptographic keys, userids, passwords, and SNMP community strings.

This feature will create cron job that will run once a day to:

- Generate a minor alarm for the expiration or warning expiration of certificates.
- Generate an alarm for the expiration of system or local accounts and passwords. A system account is defined to be any account used for program to program or machine to machine authentication.
- Generate an alarm warning that an account or password is about to expire.

Scripts that manage key material will also generate a security log for any attempt to add, delete, or modify key material--whether valid or under attack.

Alarm and log details can be found in the Fault Management (FM) section that follows.

1.2 Hardware Requirements or Dependencies

Not applicable

1.3 Software Requirements or Dependencies

This feature uses:

- the cron facility of unix to run a program periodically.
- the perl interpreter

1.4 Limitations and restrictions

This feature will not cover central user accounts managed by IEMS or certificates automatically generated by IEMS Security Server during installation.

1.5 Interactions

1.6 Glossary

Term	Description

2: Fault Management for A00009614

2.1 Fault management strategy

IEMS and SSPFS will create logs and alarms for:

- Expiration of certificates, expiration of system and local accounts and the passwords for system and local accounts.
- Attempts to add/modify/delete key material including cryptographic keys, userids, passwords, and SNMP community strings.

2.2 Fault management tools and utilities

The scope of this feature in perspective to fault management is to provide a method of reporting information to the end-user; all tools and utilities for the analysis and handling procedures are controlled and maintained by the SESM Alarm Manager or IEMS.

2.3 Logs

Security logs will be created for both successful and failed attempts to add/modify/ delete key material. Security log examples are shown below.

2.3.1 Database Password Change Logs

<date and time> PROG=pfsora_set_pwd SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=Change_password MESSAGE="Database password change for: <user>"

<date and time> PROG=pfsora_set_pwd SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_EMS_Prov CMD=Change_password MESSAGE="Invalid user for database password change: <user>"

<date and time> PROG=pfsora_set_pwd SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_EMS_Prov CMD=Change_password MESSAGE="Invalid machine used for database password change:< networkId>"

2.3.2 Certificate Creation and Change Logs

<date and time> PROG=apache.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=CERT_Add MESSAGE="Fresh certificate installed"

<date and time> PROG=apache.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=CERT_Mod MESSAGE="Certificate changed"

2.3.3 ssh Key Creation/Change Logs

<date and time> PROG=keygen.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=KEY_Mod MESSAGE="ssh key change"

<date and time> PROG=keygen.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=KEY_Mod MESSAGE="Invalid user for ssh key change: <user>"

<date and time> PROG=keygenWithoutBoopTransferr.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=KEY_Mod MESSAGE="ssh key change"

<date and time> PROG=keygenWithoutBoopTransferr.sh SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=KEY_Mod MESSAGE="Invalid user for ssh key change: <user>"

2.3.4 IPSec IKE Policy Creation and Deletion Logs

Currently, when an IKE policy is added or deleted, a security log is generated. Those logs will be replaced with logs in the new format, shown below. Also, logs will be generated from the server (utility) level.

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE rule added. Rule: <IKE rule> "

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE entry added"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE rule deleted. Rule: <IKE rule> "

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE entry deleted"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="Could not Sync IPSec data”

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE rule could not be added. Rule: <IKE rule> ”

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE configuration data could not be updated”

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE preshared key data could not be updated”

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IKE entry could not be added"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE key could not be deleted. Rule: <IKE rule>"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE rule could not be deleted. Rule: <IKE rule>"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE rules could not be updated"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE key could not be updated"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE configuration data could not be updated"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE preshared key data could not be updated"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=ike_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="Could not Sync IPSec data"

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IKE entry could not be deleted""

2.3.5 IPSec Key Change Log

Currently, when an IPSec key is changed, a security log is generated. Those logs will be replaced with logs in the new format, shown below. Also, logs will be generated from the server (utility) level.

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Preshared key modified"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Attempt to modify Preshared key"

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Preshared key modified"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Attempt to modify Preshared key"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Could not change Preshared key"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="IKE preshared key data could not be updated"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=chg_key SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Could not Sync IPSec data"

<date and time> PROG=IKEUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Mod MESSAGE="Could not modify preshared key"

2.3.6 IPSec IPSec Policy Creation and Deletion Logs

Currently, when an IPSec policy is added or deleted, a security log is generated. Those logs will be replaced with logs in the new format, shown below. Also, logs will be generated from the server (utility) level.

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IPSec rule added. Rule: <IPSec rule> "

<date and time> PROG=IPSecUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IPSec entry added"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IPSec rule deleted. Rule: <IPSec rule> "

<date and time> PROG=IPSecUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Success EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IPSec entry deleted"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="Could not Sync IPSec data”

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IPSec rule could not be added. Rule: <IPSec rule> ”

<date and time> PROG=IPSecUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Add MESSAGE="IPSec entry could not be added"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IPSec rule could not be deleted. Rule: <IPSec rule>"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="Problem occurred loading IPSec rules on other cluster unit"

<date and time> PROG=ipsec_policy SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="Could not Sync IPSec data"

<date and time> PROG=IPSecUtil.java SRC.USR=<userName> SRC=<clientNetworkID> STAT=Failure EVNT.TYPE=USER_ACT_Security CMD=PARAM_Del MESSAGE="IPSec entry could not be deleted""

2.4 Alarms

2.4.1 Password Expiration Warning Alarm

```
Component Id     :
cbm850=wnc0s0rv;NODE=wnc0s0rv,CLASS=SEC,SECTYPE=Expiration,OBJECT=password,USER=maint
Severity         : Warn
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : IEMS_EXPIRATION_CHECKER
Algorithm Used   : Algorithm1
Category         : QualityOfService
```

```
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : password expiry
Specific Problem : The password for user 'maint' will expire in 5 day(s)
User Data        :
Recovery Action  :
Time When Raised : Mon Jan 17 12:57:10 2005
```

2.4.2 Password Expiration

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,SECTYPE=Expiration,OBJECT=password,USER=maint
Severity         : Minor
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : IEMS_EXPIRATION_CHECKER
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : TBL
Probable Cause   : unspecifiedReason
Description      : password expiry
Specific Problem : The password for user 'maint' has expired
User Data        :
Recovery Action  :
Time When Raised : <DATE and TIME>
```

2.4.3 Account Expiration Warning Alarm

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,SECTYPE=Expiration,OBJECT=account,USER=maint
Severity         : Warn
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : IEMS_EXPIRATION_CHECKER
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : account expiry
Specific Problem : The account for user 'maint' will expire in 5 day(s)
User Data        :
Recovery Action  :
Time When Raised : <DATE and TIME>
```

2.4.4 Account Expiration Alarm

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,SECTYPE=Expiration,OBJECT=account,USER=maint
Severity         : Minor
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : IEMS_EXPIRATION_CHECKER
Algorithm Used   : Algorithm1
Category         : QualityOfService
```

```
Event Type       : TBL
Probable Cause   : unspecifiedReason
Description      : account expiry
Specific Problem : The account for user 'maint' has expired
User Data        :
Recovery Action  :
Time When Raised : <DATE and TIME>
```

2.4.5 Certificate Expiration Alarm

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,CLASSTYPE=EXPIRED,SUBTYPE=HTTPSCERT,FILE=<FILE>
Severity         : Minor
State            : ISTb
Report Name      : SPFS
Report Number    : 350
Application      : SSPFS_RES_MON
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : TBL
Probable Cause   : unspecifiedReason
Description      : certificate expiration
Specific Problem : https certificate has expired
User Data        :
Recovery Action  :
Time When Raised : <DATE and TIME>
```

2.4.6 Certificate Expiration Alarm Clearing

```
Component Id     :
cbm850=<SERVER>;NODE=<SERVER>,CLASS=SEC,CLASSTYPE=EXPIRED,SUBTYPE=HTTPSCERT,FILE=<FILE>
Severity         : Cleared
State            : InSv
Report Name      : SPFS
Report Number    : 350
Application      : SSPFS_RES_MON
Algorithm Used   : Algorithm1
Category         : QualityOfService
Event Type       : INFO
Probable Cause   : unspecifiedReason
Description      : certificate expiration
Specific Problem : https certificate is no longer expired
User Data        :
Recovery Action  :
Time When Raised : <DATE and TIME>
```

2.5 Related documentation

Product = Integrated EMS

A00009777 -- IEMS Mediant 2000 Integration (POI 896)

Functional Description

1: Applicable Solution(s)

UA-IP, PT-AAL2

1.1 Description

IEMS serves as an integrated platform for managing various devices. This document lists the changes that are required in IEMS in order to manage the new device MG 3200 (Network Element).

IEMS will handle the Fault and Performance Management for this new device through SNMP interface.

1.1.1 Acronyms used

NE - Network Element

OID – Object Identifier

MS2000 - Media Server 2000

MG 3200 - Media Gateway 3200

EMS - Element Management System

MIB – Management Information Base

IEMS - Integrated Element Management Systems

SNMP - Standard Network Management Protocol

HTTPS - Secure Hypertext Transfer Protocol

1.1.2 MG 3200 Provisioning

The MG 3200 Network Element can be added using Tools--> Add--> EMS / NE menu. In the initial screen, the "IP Address" field represents the IP of the MG 3200 device to be added, "Type" represents whether it is a EMS or NE (in our case it is "NE"), "Device Type" represents the name of the device to be added (in our case it is "MG 3200"), "Device Version" represents the version of device (in our case it is "9.0") to be added and the "Web Username and Web Password" are the username and password that are needed for the configuration tool.

The subsequent screens gets all the necessary SNMP interface details that are needed for fault and performance. IEMS supports only SNMP "v1" and "v2c" versions of MG 3200 not of "v3" version.

1.1.3 Automatic INI File Backup

MG 3200 has the IPSec configurations stored in a INI file named BOARD.ini, this file will change based on IPSec Configuration changes. IEMS will be taking a backup of this file at regular intervals (configurable) and store it for future use.

IEMS will have the following abilities with respect to the MG 3200 INI Backup functionality,

IEMS will be using HTTPS to communicate and retrieve the INI Files from the MG 3200 device. The design of the HTTPS communication will be by creating an URLConnection with the specified HTTPS URL and establishing a connection. The Authentication will be
taken care by using the appropriate Headers in the URLConnection (basic and digest authentication).

The Right Click Menu on the MG 3200 will have a new menu item to Configure INI Backup . This will popup the INI Configuration dialog similar to that of a MS 2000 device. This screen will have the provision to configure the INI Backup to occur daily or a weekly basis and at a particular time.

A successful configuration will initiate and schedule the next back up time using the timer scheduler. In the design part IEMS will mostly be using the MS 2000 code for scheduling and the GUI pop up. IEMS will write new code to handle the HTTPS communication, Certificate Handling and Authentication for MG 3200 INI Backup. The following will give a clear picture and what can be done and not done:

- IEMS will be using the following URL to retrieve the INI File - https://<mg3200 ip>/FS/BOARD.ini
- The web username and web password given while datafilling the MG3200 device in to IEMS will be used for Authentication.
- Thus retrieve INI files will be stored in the /data/loads/audiocodes/<mg3200 ip>/<current time>.Board.ini If the file is encoded in the device, the IEMS backup will retrieve and store it in the same way. Please refer Appendix 3 for INI encoding details.
- IEMS will trigger the INI Backup based on earlier configurations during a warmstart of the IEMS.
- IEMS will not push this file to the SDM as it is the case in MS2000
- Configuration of INI back up can be done to all the MG3200 devices configured on the IEMS and not for a single MG3200. And you can schedule it and cannot execute it immediately.

1.1.4 IPSec and IKE Configuration

This feature adds IPSec and IKE configuration capabilities to the MG 3200 node configuration tool. This will allow the craftsperson to enable IPSec for secure messaging between the IEMS and MG 3200 as well as configure the IPSec and IKE parameters necessary for the MG 3200 to securely send and receive messages.

A menu "IPSec and IKE Config Tool" will be available on the right click of the MG 3200 Map Symbol. On clicking this menu, IEMS opens a panel over which the IPSec Configuration frame is embedded.

Refer to the document IPSecFN_CN.pdf for "Add IKE and IPSec parameters to the MG 3200 for IEMS MG 3200 secure messaging."

1.2 References

IPSecFN.pdf

IPSecFN_CN.pdf

2: Fault Management for A00009777

MG 3200 behaves in a similar way as that of MS2000 devices except for a few new Traps. IEMS will use a similar kind of approach as that of MS2000 to handle the faults form MG 3200 and the additional faults.

SNMP Fault Mapping would remain the same as that of MS2000 for the AcBoard Traps (mentioned on the DID - referenced), coldStart and authenticationFailure traps.

A new Trap named dsx1LineStatusChange will also be forwarded from MG 3200 device. This trap will be mapped to an INFO event in the IEMS.

It is expected that MG 3200 will not send ATM MIB Traps which are a part of MS2000 device.

IEMS will take care of synchronizing the alarms between the IEMS and MG 3200 device. Re-synchronization of Alarms will happen using the IETF MIB support and Notification Log MIB Support available in the MG 3200 device. IEMS assumes that everything relating to this implementation is similar to MS200 device. Re-sync Operation will be invoked under following situations:

1. While Configuring the MG 3200 in to IEMS

2. If IEMS misses a Trap (This will be sequence number based and IEMS assumes that MG 3200 supports alarm retrieval based on its sequence number as in MS2000)

3. When invoking re-synchronization Manually.

4. When ever a coldStart trap is received from the MG 3200

5. During IEMS restart (if the device is present in the db)

The Fault Mapping for the MG 3200 traps are as mentioned below,

Trap Name	OID	LogKey
acBoardFatalError	.1.3.6.1.4.1.5003.9.10.1.21.2.0.1	MGTH301
acBoardConfigurationError	.1.3.6.1.4.1.5003.9.10.1.21.2.0.2	MGTH302
acBoardTemperatureAlarm	.1.3.6.1.4.1.5003.9.10.1.21.2.0.3	MGTH303
acBoardEvBoardStarted	.1.3.6.1.4.1.5003.9.10.1.21.2.0.4	MGTH500
acBoardEvResettingBoard	.1.3.6.1.4.1.5003.9.10.1.21.2.0.5	MGTH300
acgwAdminStateChange	.1.3.6.1.4.1.5003.9.10.1.21.2.0.7	MGTH501
acBoardEthernetLinkAlarm	.1.3.6.1.4.1.5003.9.10.1.21.2.0.10	MGTH307
acActiveAlarmTableOverflow	.1.3.6.1.4.1.5003.9.10.1.21.2.0.12	MGTH309
acOperationalStateChange	.1.3.6.1.4.1.5003.9.10.1.21.2.0.15	MGTH312
acKeepAlive	.1.3.6.1.4.1.5003.9.10.1.21.2.0.16	MGTH313
acNATTraversalAlarm	.1.3.6.1.4.1.5003.9.10.1.21.2.0.17	MGTH314
acEnhancedBITStatus	.1.3.6.1.4.1.5003.9.10.1.21.2.0.18	MGTH600
acPerformanceMonitoringThresholdCrossing	.1.3.6.1.4.1.5003.9.10.1.21.2.0.27	MGTH800
dsx1LineStatusChange	.1.3.6.1.2.1.10.18.15.0.1	MGTH601
coldStart	.1.3.6.1.6.3.1.1.5.1	Will not be sent to NB All prior alarms from the device will be cleared and "Re-sync" operation will be invoked as the device has been reset.
authenticationFailure	.1.3.6.1.6.3.1.1.5.5	Will not be sent to NB

Apart from these, the Trap VarBinds will be parsed and mapped in to event properties as follows,

IEMS Event Property	**Values associated for the Property**
Name	From Trap Varbind: *acBoardTrapGlobalsName*
LogName	MGTH
LogNumber	As specified in Fault Mapping table provided above
Source	From Trap Varbind: *acBoardTrapGlobalsSource*
Unique ID	acBoardTrapGlobalsUniqID
Severity	From Trap Varbind: *acBoardTrapGlobalsSeverity* (based on its value severity will vary) dsx1LineStatusChangeTrap will be given a INFO severity
EventType	FLT for "Raise" events and INFO for "Clear" events
State	Will be based on the severity value. For traps with severity Clear (i.e. severity =5) the state will be "*Clear*" , for all other severity the state will be "*Raise*".
Category	From Trap Varbind: *acBoardTrapGlobalsType* (communications | qualityOfService | processingError | equipment | environmental | other)
Probable Cause	From Trap Varbind: *acBoardTrapGlobalsProbableCause*.
Specific Problem	Value to be provided
Description	From Trap Varbind: *acBoardTrapGlobalsTextualDescription*.
Info1	From Trap Varbind: *acBoardTrapGlobalsAdditionalInfo1*
Info2	From Trap Varbind: *acBoardTrapGlobalsAdditionalInfo2*
Info3	From Trap Varbind: *acBoardTrapGlobalsAdditionalInfo3*
Time	From Trap Varbind: *acBoardTrapGlobalsDateAndTime*

NorthBound SCC2 Log format:

*C32 MGTH301 0001 FLT MG3200 FAULT
Location: MG;192.168.113.144
State: Raised
Category: communications
Cause: congestion
Time: Apr 08 12:32:34 2005
Component Id: MG 3200
Trap Name: 1
Description: Fake trap generated for the trap acBoardFatalError

NorthBound NTSTD Log format:

Nortel *** MGTH301 APR08 12:32:34 0001 FLT MG3200 FAULT
Location: MG;192.168.113.144
State: Raised
Category: communications
Cause: congestion
Time: Apr 08 12:32:34 2005
Component Id: MG 3200
Trap Name: 1
Description: Fake trap generated for the trap acBoardFatalError

3: Performance Management for A00009777

IEMS will collect the Performance metrics from the MG 3200 as it is being done for the MS2000 via SNMP. The below mentioned PMs from the acPerfMediaGateway MIB will be included for data collection for MG 3200 device.

The OIDs for which data collection would be done are :

PM Name	OID
Call Processing Performance Management	
acPerfCpNumDupsForCompletedTransactions	1.3.6.1.4.1.5003.10.1.1.1
acPerfCpNumDupsForOutstandingTransactions	1.3.6.1.4.1.5003.10.1.1.2
acPerfCpMessageSendSuccesses	1.3.6.1.4.1.5003.10.1.1.3
acPerfCpMessageSendErrors	1.3.6.1.4.1.5003.10.1.1.4
acPerfCpMessageReceiveSuccesses	1.3.6.1.4.1.5003.10.1.1.5
acPerfCpMessageReceiveErrors	1.3.6.1.4.1.5003.10.1.1.6
acPerfCpProtocolSyntaxErrors	1.3.6.1.4.1.5003.10.1.1.7

acPerfCpMessageRetransmissions	1.3.6.1.4.1.5003.10.1.1.8
acPerfCpMessageMaxRetransmissionsExceeded	1.3.6.1.4.1.5003.10.1.1.9
acPerfCpMessagesFromUntrustedSources	1.3.6.1.4.1.5003.10.1.1.10
RTP Performance Measurements	
acPerfRtpSenderPackets	1.3.6.1.4.1.5003.10.1.2.1
acPerfRtpSenderOctets	1.3.6.1.4.1.5003.10.1.2.2
acPerfRtpReceiverPackets	1.3.6.1.4.1.5003.10.1.2.3
acPerfRtpReceiverOctets	1.3.6.1.4.1.5003.10.1.2.4
acPerfRtpRcvrLostPackets	1.3.6.1.4.1.5003.10.1.2.5
acPerfRtpFailedDueToLackOfResources	1.3.6.1.4.1.5003.10.1.2.6
acPerfRtpSimplexInSessionsTotal	1.3.6.1.4.1.5003.10.1.2.7
acPerfRtpSimplexInSessionsCurrent	1.3.6.1.4.1.5003.10.1.2.8
acPerfRtpSimplexOutSessionsTotal	1.3.6.1.4.1.5003.10.1.2.9
acPerfRtpSimplexOutSessionsCurrent	1.3.6.1.4.1.5003.10.1.2.10
acPerfRtpDuplexSessionsTotal	1.3.6.1.4.1.5003.10.1.2.11
acPerfRtpDuplexSessionsCurrent	1.3.6.1.4.1.5003.10.1.2.12
System Performance Measurements	
acPerfSystemPacketEndpoints	1.3.6.1.4.1.5003.10.1.3.1
acPerfSystemPacketEndpointsInUse	1.3.6.1.4.1.5003.10.1.3.2

A new XML file template containing the above OIDs will be created for the performance collection of MG 3200 and all the necessary changes to include this in collection and report jobs will be done in the IEMS.

MG 3200 Integration A00009777 - DID Document

4: Appendix for A00009777: Notes

1. When one MG3200 device is reset, a maximum of 35 traps will be generated.

- acBoardEvResettingBoard
- acEnhancedBITStatus
- acgwAdminStateChange (only if the device was reset gracefully with a lock)
- 1 dsx1LineStatusChange trap for each T1/E1 span as they shutdown (a max of 8 spans)

- 1 dsx1LineStatusChange trap for each T1/E1 span as they come back up (a max of 8 spans)

2. The acEnhancedBITStatus trap (treated as an info log) will be sent once per hour by each MG3200 device.

3. Any .ini files retrieved from the MG 3200, either through automatic backup or through the MG 3200 config gui, should be encoded to keep any IPSec configuration information secure. To insure that the retrieved .ini files are encoded, an encoded .ini file must be placed on the device. It is recommended that an encoded .ini file be generated and placed on the device as part of the installation procedure. Reference section 7.2.2 "Secured Configuration File Downloading" in the MG 3200 User Manual for instructions on how to do this.

4. For AudioCodes reference, refer to the below mentioned Nortel MG3200 documents. These documents belong to the version of SN08/4.6. For SN09, the version of the documents will vary.

* MG 3200 User Manual

Nortel Media Gateway MG3200 H.248 User's Manual

SN07 was LTRT-72702, SN08 is LTRT-72703

* MG 3200 Fast Track Install Guide

Nortel Media Gateway MG3200 H.248/SIP Fast Track

SN07 was LTRT-73802, SN08 is LTRT-73803

* MG 3200 Configuration Guide

Nortel Media Gateway MG3200 H.248 Configuration Guide

SN07 was LTRT-72902, SN08 is LTRT-72903

Product = Integrated EMS

A00009823 -- Security Logging for SSPFS

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

This feature adds security logging to the SSPFS CLI scripts. Security logs are to be generated whenever any security affecting parameter is changed from the CLI.

In the event that a hacker or user were to change a security parameter using the CLI, a discrete entry will be written to the security log. Each security log will contain a description of the action, an action identifier, the identity of the user, source address of the user, and the date and time that the action occurred.

1.1.1 Security Log location

The Security Log file is stored at:

/var/log/securitylog

1.1.2 Affected CLI Scripts

1.1.2.1 Login Retries Limit

SSPFS CLI will log whenever an MSAP access threshold is changed. CLI 2-14-6; Login Retries Limit in login_timeout.ksh.

1.1.2.1.1 Security Log output

Feb 22 16:36:31 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Retries Limit = 3"

1.1.2.2 Login Session (User Inactivity) Timeout

SSPFS CLI will log whenever an MSAP time interval that controls keyboard lockout is changed. CLI 2-14-1; Login Session (User Inactivity) Timeout configuration in login_timeout.ksh.

1.1.2.2.1 Security Log output

Feb 22 16:33:05 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Login Session Timeout = 1440"

1.1.2.3 User Termination Timeout

SSPFS CLI will log whenever an MSAP time interval that controls keyboard lockout is changed. CLI 2-14-2; User Termination Timeout configuration in login_timeout.ksh.

1.1.2.3.1 Security Log output

Feb 22 16:33:28 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Login Session Termination Timeout = 1440"

1.1.2.4 User Reauthentication Disable Timeout

SSPFS CLI will log whenever an MSAP time interval that controls keyboard lockout is changed. CLI 2-14-3; User Reauthentication Disable Timeout configuration in login_timeout.ksh.

1.1.2.4.1 Security Log output

Feb 22 16:33:44 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Login Session Reauthentication Disable Timeout = 30"

1.1.2.5 Login Session Master Server

SSPFS CLI will log whenever an MSAP time interval that controls keyboard lockout is changed. CLI 2-14-4; Login Session Master Server configuration in login_timeout.ksh.

1.1.2.5.1 Security Log output

Feb 22 16:34:14 wnc0y0nr PROG=login_timeout.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=login_timeout.ksh MESSAGE="Setting Login Session Master Server = test"

1.1.2.6 Socks Security Service

SSPFS CLI will log whenever changes to MSAP security profiles and attributes occurs. CLI 2-13-1-1; Socks Security Service configuration in configureSocksPorts.sh.

1.1.2.6.1 Security Log output

Feb 22 16:41:08 wnc0y0nr PROG=configureSocksPorts.sh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=configureSocksPorts.sh MESSAGE="Setting Socks Server port = 10080"

Feb 22 16:41:12 wnc0y0nr PROG=configureSocksPorts.sh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=configureSocksPorts.sh MESSAGE="Setting Socks Client port = 10090"

1.1.2.7 IEMS Server IP Address

SSPFS CLI will log whenever changes to MSAP security profiles and attributes occurs. CLI 2-13-1-1; IEMS Server IP address configuration in chg_iems_ip.ksh.

1.1.2.7.1 Security Log output

Feb 22 16:42:09 wnc0y0nr PROG=chg_iems_ip.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=chg_iems_ip.ksh MESSAGE="Setting IEMS Server IP Address = 4.4.4.4, Domain Name = wnc0y0nr"

1.1.2.8 Default PAM

SSPFS cli will log whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs. CLI 2-13-3-1-1; Default PAM configuration in pam_switch.ksh.

1.1.2.8.1 Security Log output

Feb 22 16:45:12 wnc0y0nr PROG=pam_switch.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=pam_switch.ksh MESSAGE="Setting Default PAM Configuration"

1.1.2.9 Radius PAM

SSPFS cli will log whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs. CLI 2-13-3-1-2; Radius PAM configuration in pam_switch.ksh.

1.1.2.9.1 Security Log output

Feb 22 16:46:25 wnc0y0nr PROG=pam_switch.ksh SRC.USR=root SRC=wnc0y0nr STAT=Success EVNT.TYPE=USER_ACT_EMS_Prov CMD=pam_switch.ksh MESSAGE="Setting PAM Radius Parms: Radius Client Timeout = 12, SAML Connection Timeout = 20, SAML Request Timeout = 10"

1.2 Hardware Requirements or Dependencies

Not applicable.

1.3 Software Requirements or Dependencies

Not applicable.

1.4 Limitations and restrictions

Not applicable.

1.5 Interactions

Not applicable.

1.6 Glossary

Not applicable.

Product = MCS

A00009028 -- CS2K MSM SIP Lines OAM Support

Functional Description

1: Applicable Solution(s)

MCS

1.1 Description

This feature deals with meeting the OAM requirements on CS2K MSM for support of SIP Lines in release MCP 9.0. It is primarily concerned with the configuration of data corresponding to links to the CS2K and the maintenance on those links. All configuration will be done via the CS2K MSM Management Console; no flow through configuration is supported in this release. Once the link configuration is established, the CS2K MSM components are responsible for initiating communication. Additionally, this feature provides for monitoring the registration state of SIP endpoints (CS2K MSM subscribers provisioned with a SIP Lines enabled service package) and performing a line test on the endpoint. This functionality will be accessible from the Management Console. Finally, Accounting will be disabled for the SIP Lines deliverable.

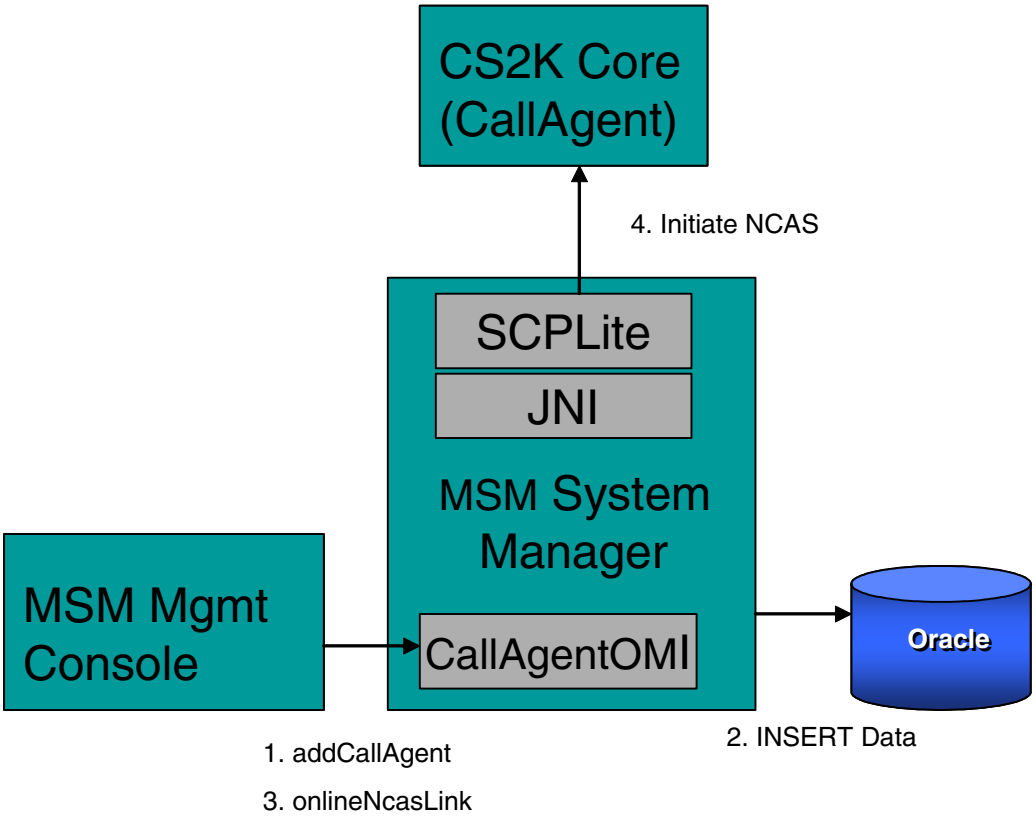
These requirements fall into the following work areas.

- Non-Call Associated Signalling (NCAS) link for Querying SIP (QSIP)
- Gateway Controller (GWC) link for Gateway Control Protocol (GCP)
- Endpoint Maintenance
- Disabling Accounting

1.2 NCAS Link for QSIP

This link will run between the CS2K MSM System Manager and the CS2K Core. Configuration of the link is provided via CallAgentData which contains a name (for database key purposes), an IP Address, and a port. Maintenance on this link will consist of setting a desired state to ONLINE or OFFLINE. The default state when the CallAgent data is added will be OFFLINE, requiring a manual maintenance action by the craftsperson at the Management Console to bring the link ONLINE. (See steps 1 and 3 in the diagram below.) In addition to the desired state, the operational state of the link (CONNECTED or DISCONNECTED) will be reported at the Management Console.

Note: Screenshots of the Management Console will be made available in the Configuration section of this Design Document.



The OMI methods for configuring the CallAgentData are supported by the OMI service located at http://<sysMgrHost>:12121/axis/services/callagent as follows:

- public void RuntimeResult addCallAgent(data CallAgentData)
- public void RuntimeResult updateCallAgent(data CallAgentData)
- public void RuntimeResult deleteCallAgent(key CallAgentNaturalKey)
- public CallAgentData getCallAgent()

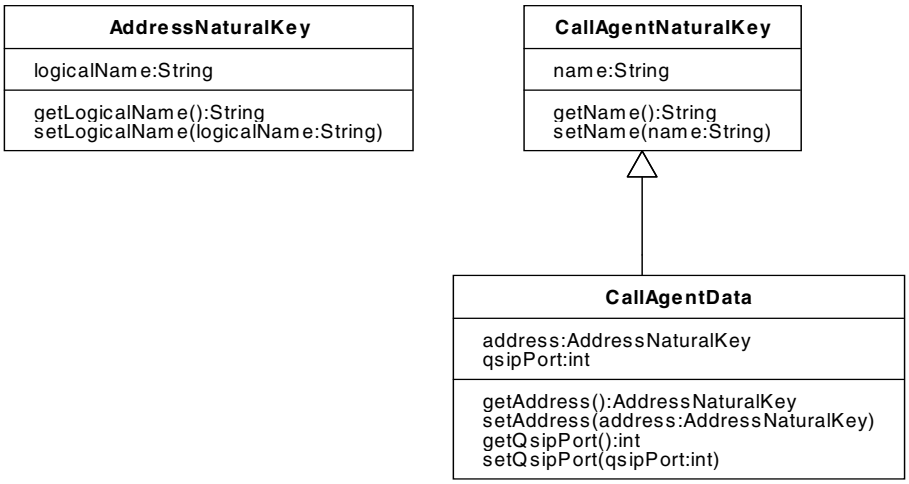


Table 1: CallAgent fields

Field Name	Description
AddressNaturalKey.logicalName	1-16 characters no spaces
CallAgentNaturalKey.name	1-32 characters [Aa-Zz][0-9][-.]
CallAgentData.qsipPort	Integer in the range 4900-4982

The local end of the NCAS link is defined at an offset of 25 from the base port of the System Manager. The address used will be the System Manager's Service Address, if configured, and if not, the Interface One address of the Server on which the System Manager resides.

Maintenance on the NCAS link is provided at the Management Console under the System Manager. The state of the link (CONNECTED, DISCONNECTED) is displayed. The actions to ONLINE or OFFLINE the link will be offered. Note that when the System Manager starts up, it will read the current desired state from the database to determine whether to initiate communication.

The OMI service is located at http://<sysMgrHost>:12121/axis/services/ncasmtc. The methods are are as follows:

public long startNcasLinkMonitor()

public RuntimeResult stopNcasLinkMonitor(long tid)

public NCASLinkStateData getNcasLinkNextState(long tid)

public String[] getNcasLinkAdminStates()

public String[] getNcasLinkOperationalStates()

public RuntimeResult rtsNcasLink()

public RuntimeResult offlineNcasLink()

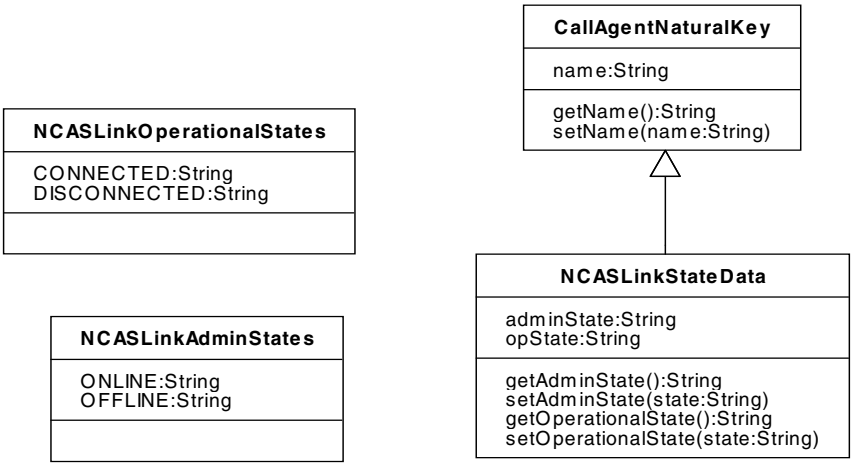


Table 2: NCAS Link State Data

Field	Description
adminState	String. Must be one of the values available from getNCASLinkAdminStates()
opState	String. Must be one of the values availabe from getNCASLinkOperationalStates()

Table 3: NCAS Link Operational States

Operational States
CONNECTED
DISCONNECTED

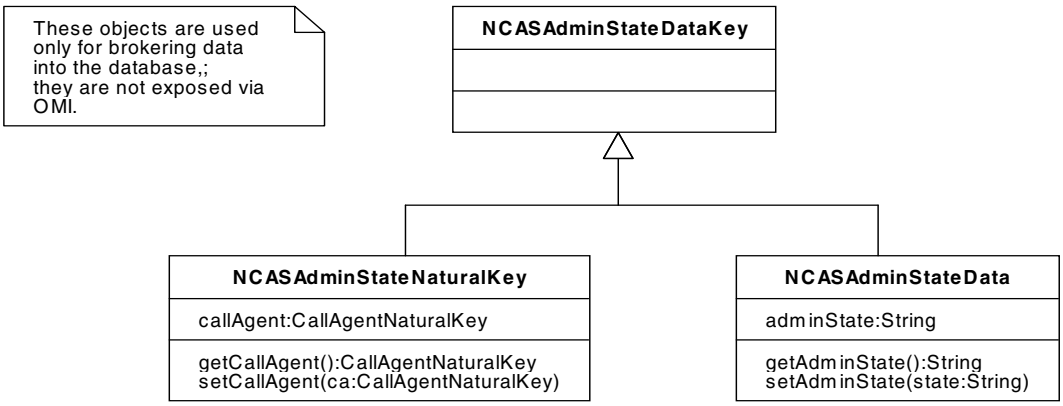
Table 4: NCAS Link Administrative States

Administrative States
ONLINE
OFFLINE

To support the additional data in the Oracle database, two new tables are added. The first contains the configuration data: CS2K_CALL_AGENT consists of three fields, NAME, ADDR and QSIP_PORT. NAME is a 32 character VARCHAR field, restricted to alphanumeric characters. ADDR is a reference to an Object Identification (OID) from the IP_ADDRESS table. QSIP_PORT is an integer field, restricted to the range 4900 and 4982.

Note: All CS2K MSM configuration tables contain an implicit OID column created by the data access framework. This column will not be explicitly named for each table, but will be assumed to be present for foreign key use.

The second stores the administrative state: CS2K_CALL_AGENT_ADMIN_STATE consists of two fields. CALL_AGENT is a contextual foreign key into CS2K_CALL_AGENT. ADMIN_STATE is a 16 character VARCHAR, to contain “ONLINE” or “OFFLINE”.

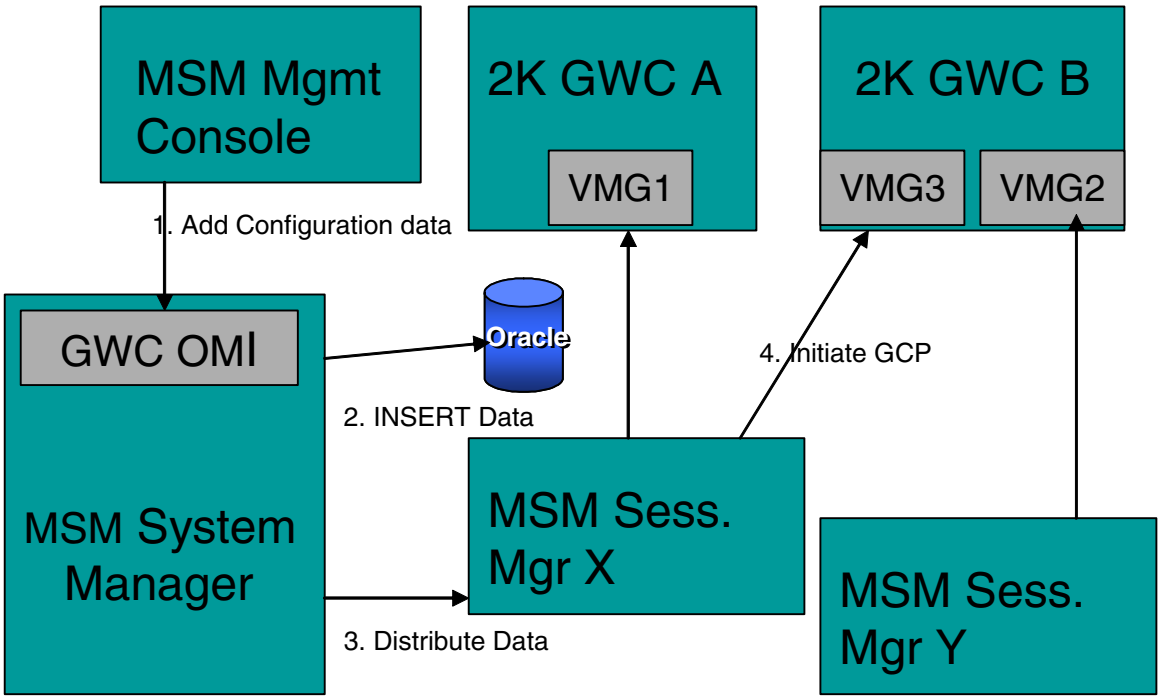


In addition to the configuration and maintenance of the link, enhancements to the Event Distribution framework allow the QSIP coming into the System Manager over NCAS to be answered by request to the active instance of the responding CS2K MSM Network Element (NE). A boolean indicating that only the active instance of an NE is to receive the request is added to the internal event, and is used by the Event Distribution system to determine destination.

1.3 GWC Configuration and Maintenance

A call processing link shipping Gateway Controller Protocol (GCP) over UDP exists between the CS2K MSM Session Manager and the CS2K Gateway Controller (GWC). Its configuration is somewhat more complex than that of the NCAS link, because the relationship between Session Manager and GWC may not be one-to-one, and further, the relationship is viewed from the GWC side through a Virtual Media Gateway (VMG), which is required for Subscriber provisioning (discussed in detail in A00009043 - SIP Lines Provisioning Support).

The diagram below describes an example of how GWCs and Session Managers might be associated via VMGs. The diagram depicts a configuration given GWCs A and B and Session Managers X and Y. Session Manager X appears as VMG1, tied to GWC A, and Session Manager Y appears as VMG2, tied to GWC B. The flow shows the association of VMG3 with Session Manager X. When the association is made, Session Manager X initiates a GCP message to GWC B.



The GWC data is Network Level data shared across all Network Elements. VMG appearances are specific to the Session Manager, and appear only on the appropriate Session Manager. The GatewayControllerData is configured through the OMI service located at http://<sysMgrHost>:12121/axis/services/gwcconfig. The signatures of the OMI methods are as follows:

- public void RuntimeResult addGatewayController(data GatewayControllerData)
- public void RuntimeResult updateGatewayController(data GatewayControllerData)
- public void RuntimeResult deleteGatewayController(key GatewayControllerNaturalKey)
- public GatewayControllerData[] getGatwayControllers()
- public GatewayControllerNaturalKey[] getGatewayControllerNaturalKeys()

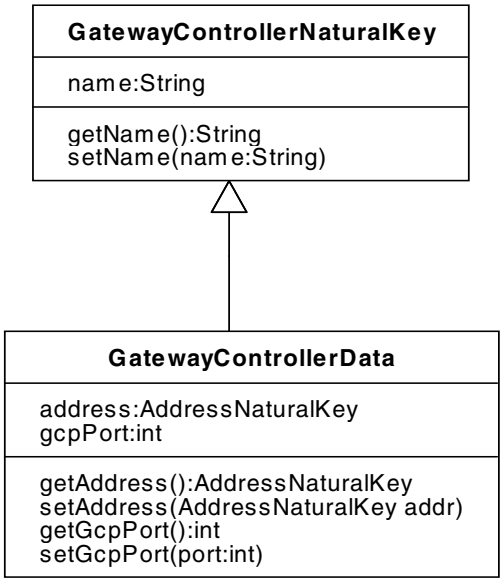


Table 5: Gateway Controller Data

Field	Description
name	Of the form gwc-### where ### may be any integer in the range 0-255, and the characters “gwc-” are fixed
gcpPort	Integer in the range 0-65534

For configuring the VMG the service at http://<sysMgrHost>:12121/axis/services/vmgconfig contains the following methods:

- pubic void RuntimeResult addVmgAppearance(ctxt SessMgrNaturalKey, data VMGAppearanceData)
- public void RuntimeResult deleteVmgAppearance(ctxt SessMgrNaturalKey, data VMGAppearance)
- public VMGAppearanceData[] getVmgAppearances(ctxt SessMgrNaturalKey)
- public VMGAppearanceNaturalKey[] getVmgAppearanceNaturalKeys(ctxt SessMgrNaturalKey)

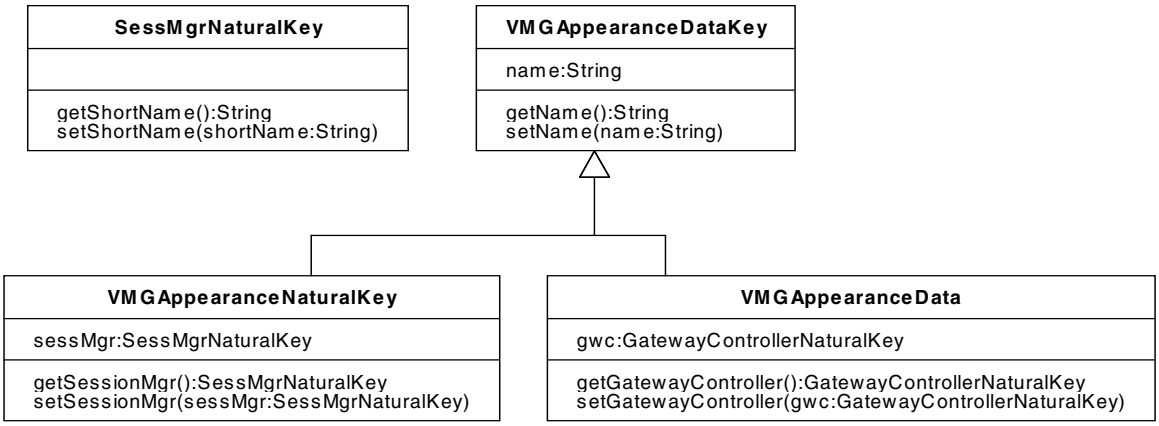


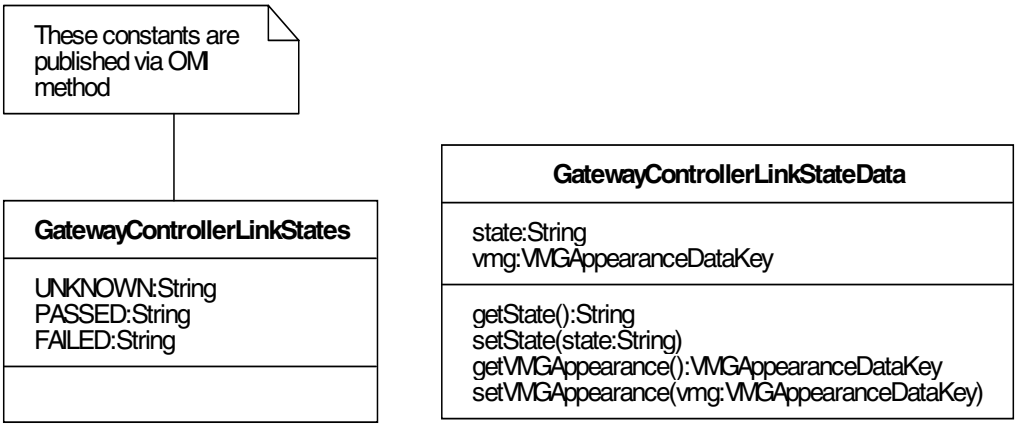
Table 6: VMG Appearance Data

Field	Description
SessMgrNaturalKey.shortName	1-6 characters spaces, dots and underscores for-bidden
VMGAppearanceDataKey.name	1-32 characters [Aa-Zz][0-9][-.]

Maintenance on the links to GWC from Session Manager is available via the Management Console, under each Session Manager. Since the link is over UDP, the only available maintenance command is a line test.

The OMI methods for GWC link test are available through the service located at http://<sysMgrHost>:12121/axis/services/gwcmtc:

- public GatewayControllerLinkStateData[] testGatewayControllerLink(SessMgrNaturalKey ctxt, VMGAppearanceDataKey[] keys)
- public String[] getGatewayControllerLinkStates()



Starting the Gateway Controller Link State maintenance application at the Management Console for a given Session Manager will result in an initial test on the GWC links. Subsequent manual tests of each GWC link are allowed via a test button

Table 7: Gatway Controller Link State Data

Field	Description
state	String. Required to be one of the values available from getGatewayControllerLinkStates

Table 8: The displayed states of the GWC Link

Displayed States
NOT_RUN
TESTING
UNKNOWN
PASSED
FAILED

Table 9: The operational states of the GWC Link

Link States
UNKNOWN
PASSED
FAILED

The configuration requires the addition of two new tables to the Oracle database.The first allows the configuration of GWCs, the second the association of a Session Manager with a GWC via a VMG name.

The CS2K_GWC table contains three fields, NAME, ADDR, and GCP_PORT. NAME is of the form gwc-###, where ### is numeric from 0 to 255, giving a VARCHAR of length 7. ADDR is a reference to an Object Identification (OID) from the IP_ADDRESS table. GCP_PORT stored as an integer, between 0 and 65534.

The CS2KVMG_APPEARANCE table contains three fields, NAME, GWC and a contextual field SESSION_MGR. NAME is a VARCHAR(64) which is globally unique.This name will be used when the Subscriber association with the VMG. is made on the Provisioning Server. GWC is a reference to an OID from the CS2K_GWC table. SESSION_MGR is a reference to an OID from the SESS_MGR table.

Because the VMG is configured and the association of VMG with Subscriber is is provisioned, the use of a VMG associated with the correct server home (Session Manager) is enforced when a Subscriber is added or updated. VMGs may not be deleted while some subscriber is still associated with the VMG.

1.4 Endpoint Monitoring

This feature treats a CS2K MSM subscriber as a SIP Line. Subscribers have dynamic state: OFFLINE, IDLE, and CPB. This information (along with other subscriber data) will be available via a QSIP query over the NCAS link as discussed in section 2.3. Additionally, it will be available from the Management Console as a direct query to the Session Manager to which the subscriber is homed. Also from the Management Console, a maintenance ping can be sent to the subscriber endpoint via an OPTIONS message as a line test, resulting in a line state. The line test functionality is available only through the Management Console. To limit network traffic, the number of lines which can be simultaneously monitored at a single Management Console is limited to five.

The state of a SIP Line is dynamic and is not stored in the Oracle database by the configuration system. Given this, a query must be made to find the

subscribers before monitoring can be initiated. The query may be made by DN or by Subscriber name in the format name@domain. After a user is posted, it may have a line test done on it. The line test will test all devices provisioned against the subscriber in addition to all currently registered devices. The two sets of devices may overlap, and the result will contain data for the superset. The result will indicate for each client whether any response was received, as well as an overall indication of whether all clients responded, some clients responded, or no clients responded.

The OMI methods to monitor and maintain the SIP line are available at http://<sysMgrHost>:12121/axis/services/endpointmtc.

- public SubscriberData[] getSubByDirectoryNumber(String dn)
- public SubscriberData[] getSubByName(String name)
- public long startEndpointStateMonitor(SubscriberNaturalKey[] keys)
- public RuntimeResult stopEndpointStateMonitor(long tid)
- public RuntimeResult updateEndpointStateMonitor(long tid, SubscriberNaturalKey[] keys)
- public EndpointStateData[] getEndpointNextState(long tid)
- public EndpointLineTestStateData[] testState(SubscriberNaturalKey[] keys)
- public String[] getEndpointStates()
- public String[] getEndpointLineStates()

The data returned by the subscriber queries:

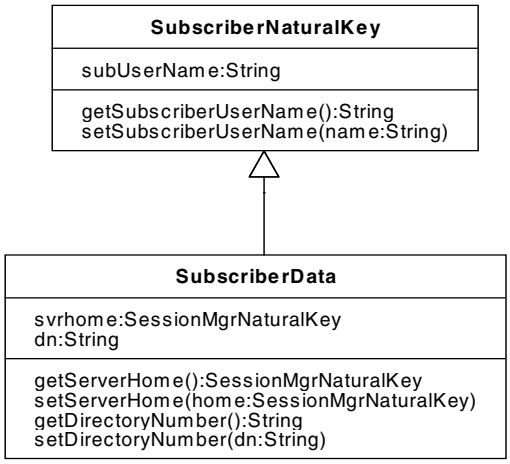


Table 10: Subscriber Data

Field	Description
userName	String of the form <user>@<domainname> where user and domain name each consist of 1-64 alphanumeric characters
dn	String containing 4-18 decimal digits.

The data returned by a line state monitor.

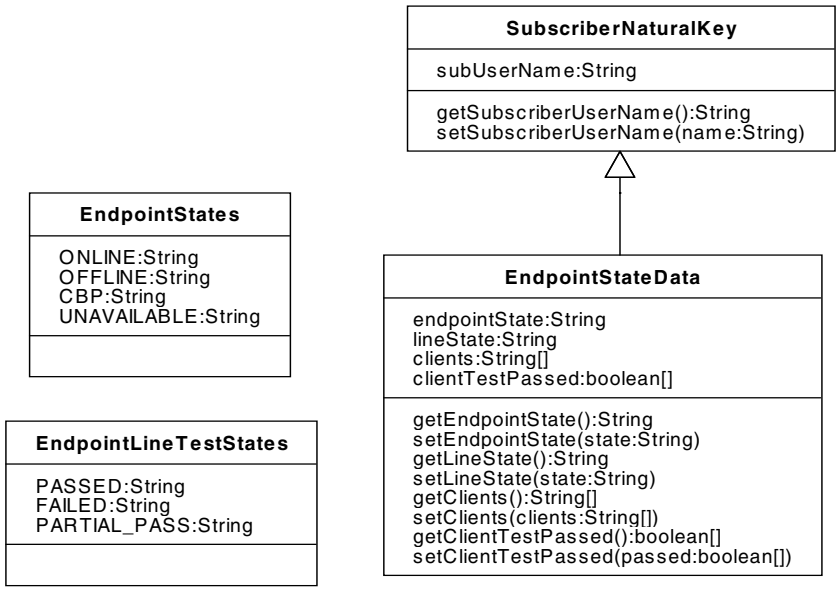


Table 11: Endpoint State Data

Field	Description
endpointState	String. Required to be one of the values available from getEndpointStates
lineState	String. Required to be one of the values available from getEndpointLineStates
clients	Array of strings describing the clients of the subscriber.

Table 11: Endpoint State Data

Field	Description
clientTestPassed	Array of booleans corresponding to the clients array, and indicating whether each client passed the line test (true=passed, false=failed)

Because acquiring the state of a line requires going to the Session Manager where the endpoint is homed, and that Session Manager may not be accessible from the System Manager, the UNKNOWN state is introduced to the list of displayed Additionally, since the line state is not automatically tested, it's initial displayed state is NOT_RUN. A PARTIAL_PASS exists when at least one, but not all of a subscriber's clients can be reached by the line test.

Table 12: SIP Line Endpoint States (displayed)

Subscriber States
UNKNOWN
OFFLINE
IDLE
CPB

Table 13: SIP Line Endpoint Line Test States (displayed)

Line Test States
UNKNOWN
NOT_RUN
TESTING
PASSED
FAILED
PARTIAL_PASS

1.5 Disable Accounting

This feature allows MCS accounting functionality to be disabled. When accounting is turned off, no Accounting Manager (AM_ will be configured against the Session Manager, and no billing records will be spooled. This feature changes the SESS_MGR table to allow NULL in the AM column. The

Management Console provides a selection value of <none> in the AM combo box to support this configuration.

When the AM is set to null, no billing records will be spooled by the recording framework. When the AM is not set to null, billing records will be spooled and sent to the AM.

1.6 Hardware Requirements or Dependencies

Not Applicable.

1.7 Software Requirements or Dependencies

Dependant on SCPLite for NCAS link.

1.8 Limitations and restrictions

1.8.1 NCAS Link for QSIP

Support for a single NCAS link to a single CS2K Core at a time is provided. Therefore, only a single CallAgent can be configured at a time.

Updates to the IP address or port of the CallAgent are allowed only if the CallAgent is in the OFFLINE state.

1.8.2 GWC Link

VMG Appearances can only be added and deleted, not updated.

Global uniqueness is enforced across VMG names

1.8.3 Endpoint Monitoring

A maximum of 5 endpoints can be simultaneously posted from a single Management Console

1.9 Interactions

A00009043 SIP Lines Provisioning Support

A00007544 - NCAS link for service control

A00007545 - GCP to SIP conversation on FPF

1.10 Glossary

Term	Description
Accounting Manager	CS2K MSM component which formats and stores billing records from the Session Manager. Turned off in MSM 9.0
AM	Accounting Manager

Term	Description
CPB	Call Processing Busy. Used to indicate that a SIP Line Subscriber is in the middle of a call.
Endpoint	Refers to a SIP Line Subscriber. In the context of SIP Lines, an endpoint does not actually refer to an IP port pair, but to a subscriber who may have registrations at multiple locations.
GCP	Gateway Control Protocol. Used for communication with GWCs
GWC	Gateway Controller. CS2K component to which Session Managers communicate for call processing
MCS	Multimedia Communication Server
MSM	Multimedia Session Manager
NCAS	Non Call Associated Signalling
NE	Network Element. A managed component of CS2K MSM. Includes Accounting Manager, Session Manager, and System Manager.
OAM	Operations, Accounting, and Management.
OID	Object Identifier. Unique ID used in the CS2K MSM database as a primary key.
OMI	Open Management Interface
Provisioning Manager	CS2K MSM component which manages CS2K MSM provisioning, including subscribers.
Session Manager	CS2K MSM component which manages SIP Sessions and call processing
SIP	Session Initiation Protocol
System Manager	CS2K MSM component which manages CS2K MSM configuration and maintenance.
VMG	Virtual Media Gateway. CS2K view of the CS2K MSM Session Manager.

Product = MCS

A00009043 -- CS2K SS SIP Lines Provisioning Support

Functional Description

1: Applicable Solution(s)

MCS

1.1 Description

The SIP Lines product leverages existing CS2K SS SIP features and CS2K Centrex features. This feature provides the capability to provision data required by CS2K SS for the SIP Lines product for the MCP 9.0 release. Provisioning support that will be provided involves the ability to provision data such as subscriber or SIP end point information used by the Session Manager to provide SIP services.

The following items will be introduced into CS2K SS

- SIP Lines as a service called CS2000 SIP Line
- SIP Lines attributes to the subscriber

The Provisioning of the SIP Line data will be available via both the Provisioning Client and via OPI. OPI is the Open Provisioning Interface, a web service which gives the ability to provision data required on CS2K SS in return for services that it can provide. OPI's capabilities are available via a published WSDL using which the provisioning activities that are required can be determined. For more information on OPI, please refer to the OPI Specification document. Details on the Provisioning Client, which is a GUI based provisioning interface are available in the Provisioning Client User Guide.

1.2 SIP Line data

The data required for SIP Lines primarily consists of:

- End point id
- Virtual media gateway
- Client Type
- Directory Number

In addition to this on the CS2K SS, a new service will be introduced which will qualify a subscriber to be a SIP Line subscriber. All the above mentioned information in addition to a service package containing the new service will be associated to subscribers using which SIP Lines services will be processed.

A more detailed description of the data introduced is given below:

Field Name	Description
End Point Id	Format: <SITE>/<FFF>/<G>/<TTtt> <SITE> = 1-4 Alphanumeric characters. Corresponds to provisioned SITE name in the XACore. <FFF> = 000-511 Corresponds to the frame number used in the logical group name in the XACore. <G> = 0-9 Corresponds to the group number used in the logical group name in the XACore <TTtt> = 0000-1022 Corresponds to the circuit numbers (upper and lower) in the LENs defined against the logical group in the XACore. This is a globally unique field that the user is associated with Maximum length 15 characters; valid character set [Aa-Zz][0-9][/]
Virtual Media Gateway	Virtual gateway name used in GWC provisioning. Maximum Length 64 characters valid character set [Aa-Zz][0-9][-./]
Client Type	This is required for determining if the user has a device that can be queried. The supported client types are: Optical Network Terminator or ONT. If there is no client then the user will not be queried for a device on a line test
Directory Number	This is a globally unique number that is associated with a subscriber, similar to user aliases.

Note: Because of a restriction on the CS2K Session Server in the way the directory number is stored, the username part of the user, i.e. the string before the @domain, cannot be the same as the directory number. This restriction will be taken care of in future release, which will allow both to be same and hence easier to identify.

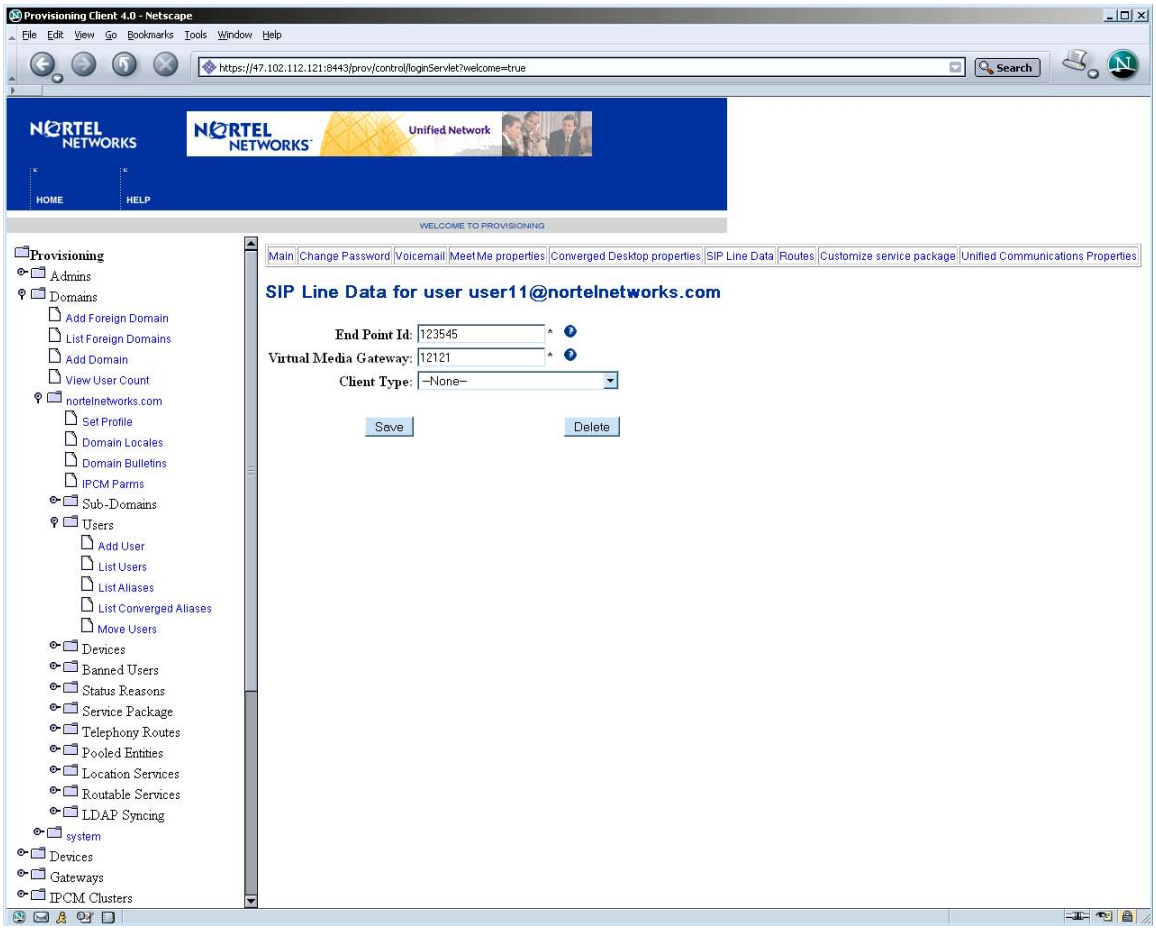


Figure 1 SIP Line Data provisioning for a user from Provisioning Client

Virtual Media Gateways are associated to Session Managers and also to a subscriber. Subscribers are homed on a session manager via the server home attribute associated to the domain that the subscriber belongs to. In case there is a change in the session manager of a domain, then the virtual media gateway information associated to a subscriber is no longer valid. In this scenario the following needs to be done to associate the subscriber to the correct virtual media gateway.

For each SIP Lines subscriber, going though SESM:

- change the end point id on the core
- change the end point id and the VMG via OPI

While changing the server home there will be no check to determine subscribers associated to it

Directory number is a new field associated to the subscriber which is exposed via OPI.

Additional types of clients supported for SIP Lines can be added to CS2K SS via OPI and the Provisioning Client. This interface is shown in the next figure.

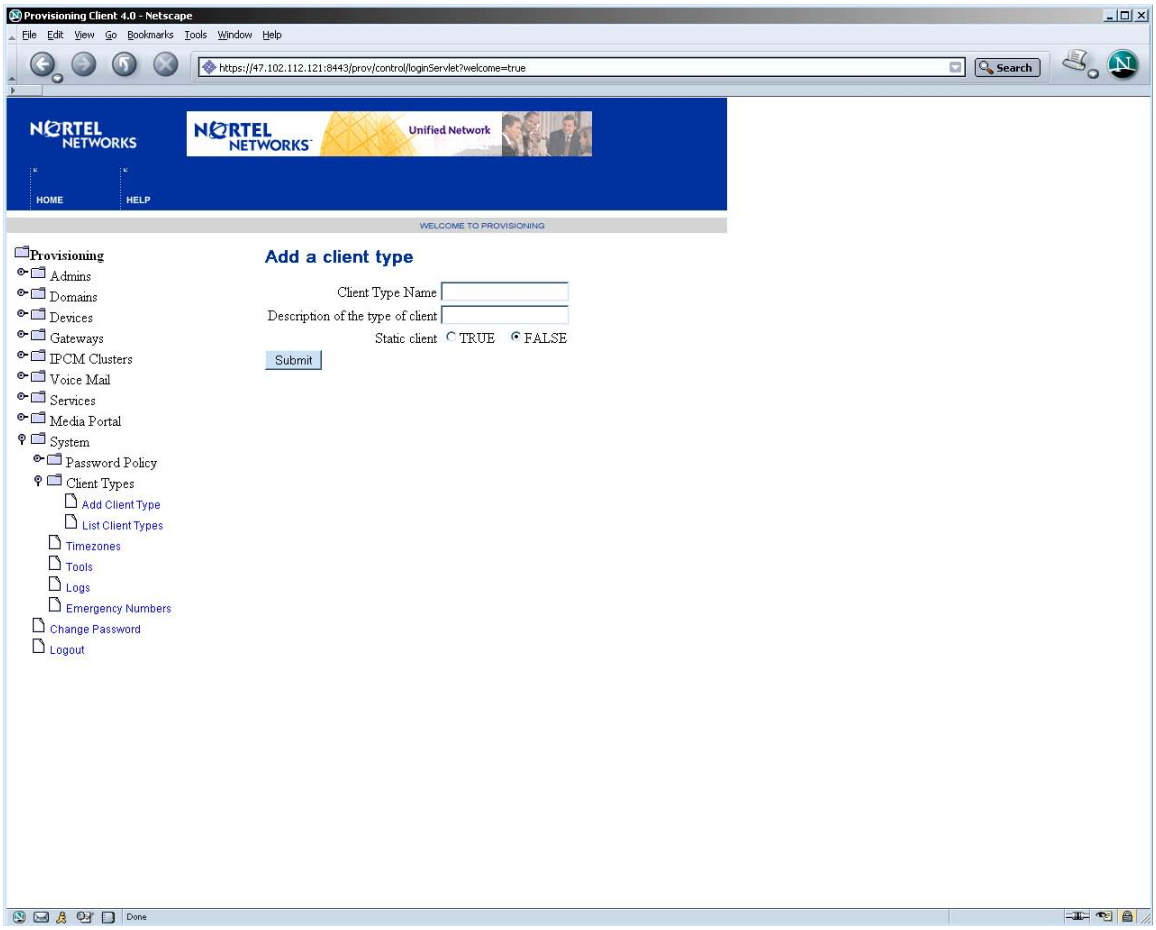


Figure 2 Client type provisioning interface

The OPI methods that can be used for Client Type provisioning are given below.

addClientType(ClientType clientType)
addClientTypes(ClientType[] clientTypes)
modifyClientType(String clientTypeName, ClientType clientType)
removeClientType(String clientType)
getClientTypeByName(String clientType):ClientType

All the client type operations need the administrator to have Full Domain Access privilege. The name of the Client Type information can be upto 60 characters long and the description can be upto 120 characters long.

The data model for the SIP Lines information and its association to the subscriber information is shown below in the figure.

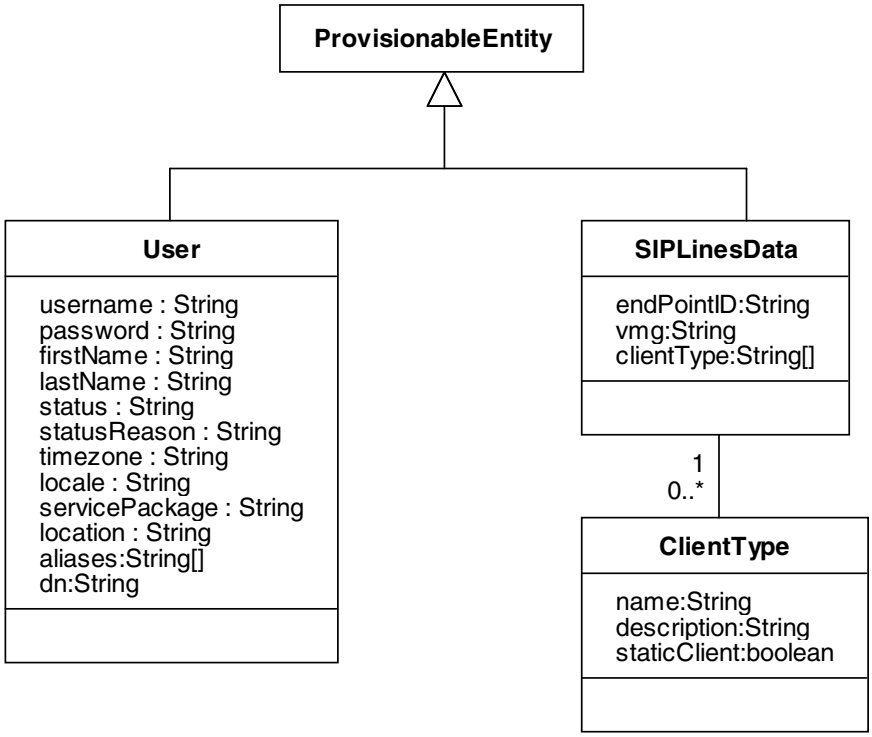


Figure 3 SIP Lines Data Model

The following table gives the required and optional field information for the above

Data	**Field Requirement**	
User	**Required**	Username,password,firstname/lastname,status, timezone, locale, service package, location
	Optional	Aliases, DN, status reason, first name/lastname (one of them)
SIPLineData	**Required**	End Point Id, VMG
	Optional	Client Type

1.3 Non SIP Line data

There is certain data that is required by OPI while adding subscribers which is not SIP Lines specific and hence can be set to a pre-defined value. Given below are three such fields and their valid values:

Field name	Possible Values
Status	ACTIVE, INACTIVE
Locale	French, English, Japanese, Simplified Chinese, Traditional Chinese, German, Spanish, Korean
Timezone	Pacific Standard Time, Mountain Standard Time, Central Standard Time, Eastern Standard Time, GMT-11:00, Hawaii Standard Time, Alaska Standard Time, GMT-04:00, Newfoundland Standard Time, GMT-03:00, Greenwich Mean Time, Central European Standard Time,G MT+02: 00, GMT+03 :00, GMT+03 :30, GMT+04 :00, GMT+05 :00, GMT+05 :30, GMT+06:00, GMT+07 :00, China Standard Time, Japan Standard Time, GMT+09 :30, GMT+10 :00, GMT+11 :00, GMT+12 :00

1.4 SESM and CS2K SS Provisioning

The SESM will be used to provision data onto the Core and CS2K SS in the SIP Lines Product. The data required on CS2K SS will be provisioned using both the Provisioning Client and also via OPI.

The following figure shows the function of the feature deliverables and its use by SESM in the product.

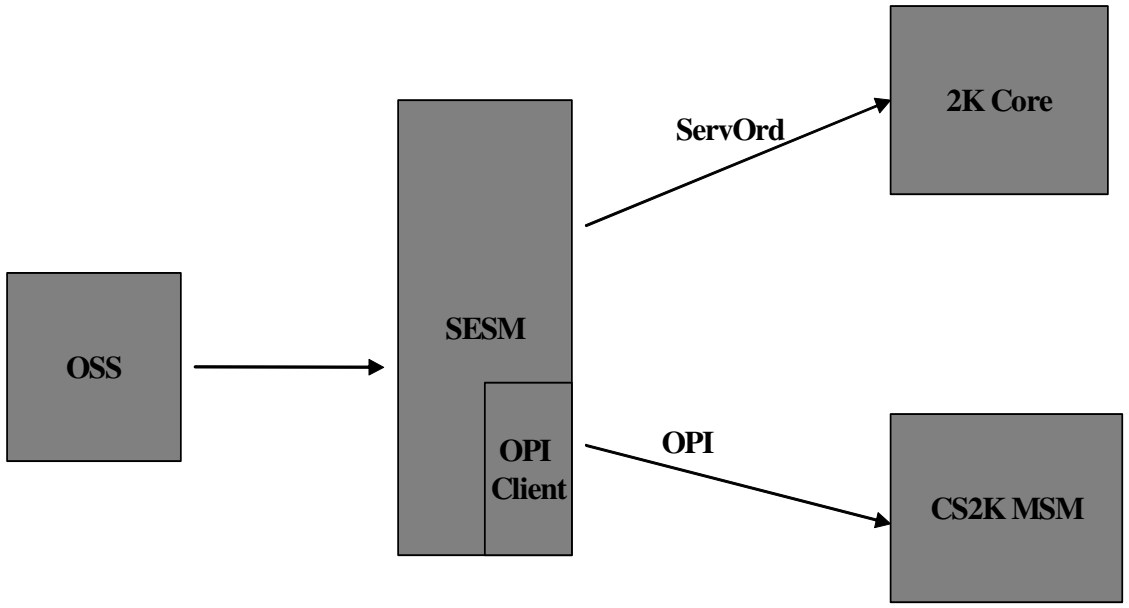


Figure 4 Flow through provisioning from and to CS2K SS in SIP lines

As mentioned above, provisioning of data for the first release of CS2K SS will involve two phases

- **Manual** - Provisioning Client will be used in this phase to provision data which would change rarely once the system is set up. This reduces the number of commands SESM has to carry out to do provisioning on CS2K SS.
- **Flow through** - the SESM using OPI carries out provisioning for adding subscriber and SIP Line specific information in this phase.

The existence of the following data is a pre-requisite for provisioning subscribers in CS2K SS:

- Administrator Role
- Administrator
- Root Domain
- Service Packages
- Locations
- Routability group

Figure 3 gives description of the information which can and needs to be Pre-provisioned before Flow through provisioning can take place.

The above data will be provisioned only once in CS2K SS as it will never be modified. The purpose of this data and other data that needs to be provisioned only once on CS2K SS is described below:

- **Administrator** - This is required for authentication and authorization of OPI calls during flow through provisioning from the SESM.
- **Domain** - This is where all the subscriber and end point information will be grouped under.
- **Service Package** - service packages containing the new CS2000 SIP Line service will be created. This will be assigned to all subscribers created from SESM, hence qualifying them as SIP Line subscribers.
- **Locations** - these are locations where the subscribers reside and are required for provisioning Routability groups for media portal insertion.
- **Routability Group** - This is required for the media portal insertion functionality via the zone information.

The following figure shows the data that will be manually provisioned in the CS2K SS system.

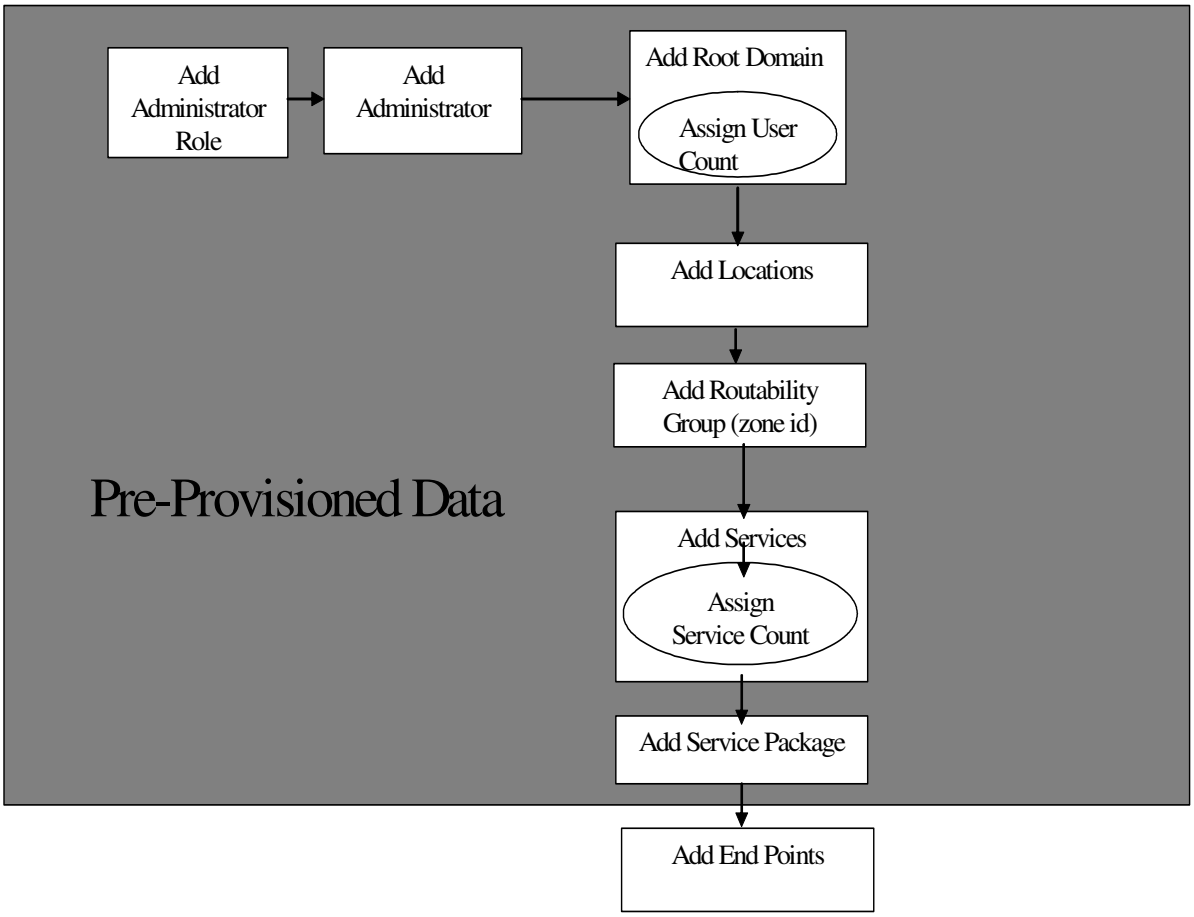


Figure 5 CS2K SS provisioning flow and pre-provisioned data information

Note:

For additional information on the provisioning client and operations please consult the Provisioning Client User Guide.

The next figure shows a sample service package with the CS2000 SIP Line service. Such a service package can be created with a mix of services which are supported on the Session Manager on CS2K SS.

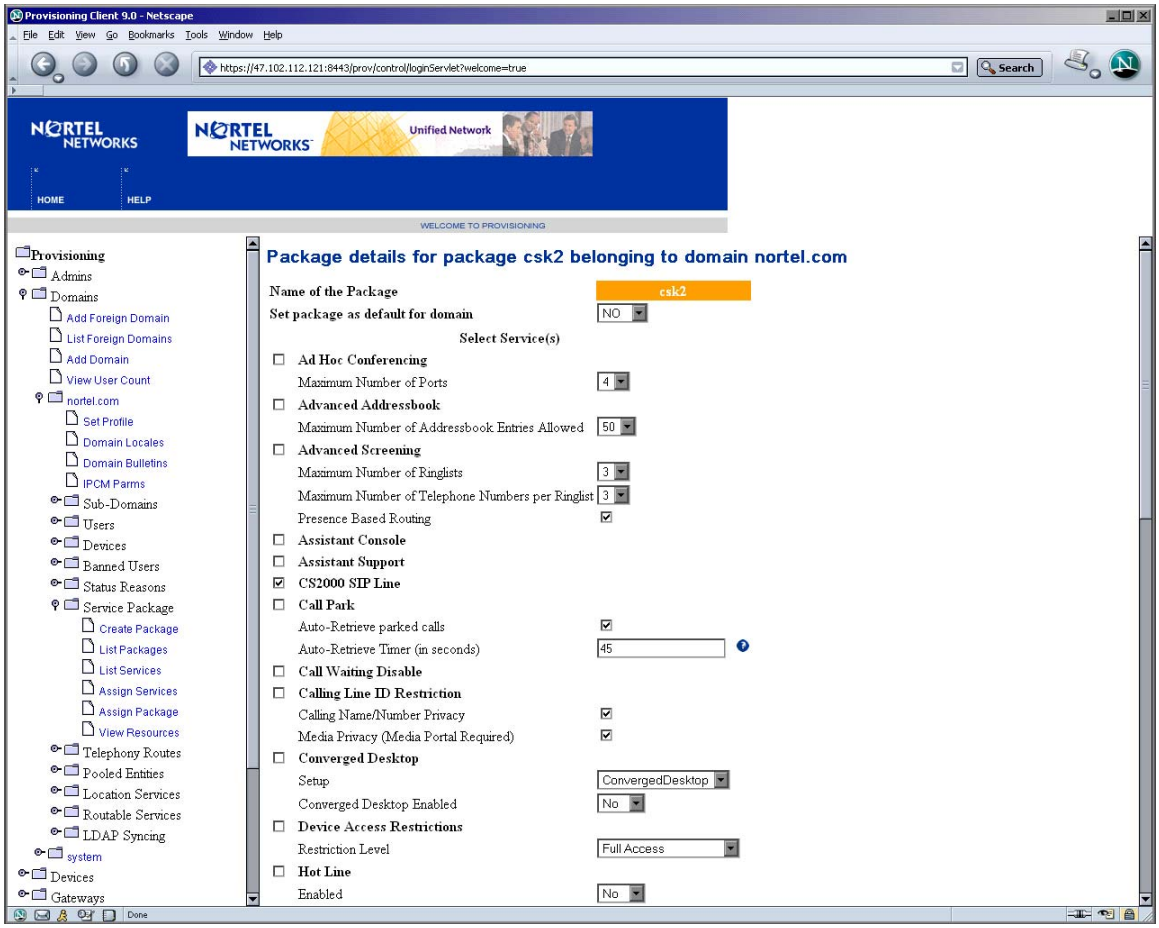


Figure 6 View of service package containing the CS2000 SIP Line service

1.5 Routability Group Information

To determine Media Portal insertion criteria by the Session Manager for services that require media portals for SIP Line calls, a new piece of data named Zone Id will be introduced as a part of the routability group information provisioned as a part of this feature. Following figure shows a view of this field

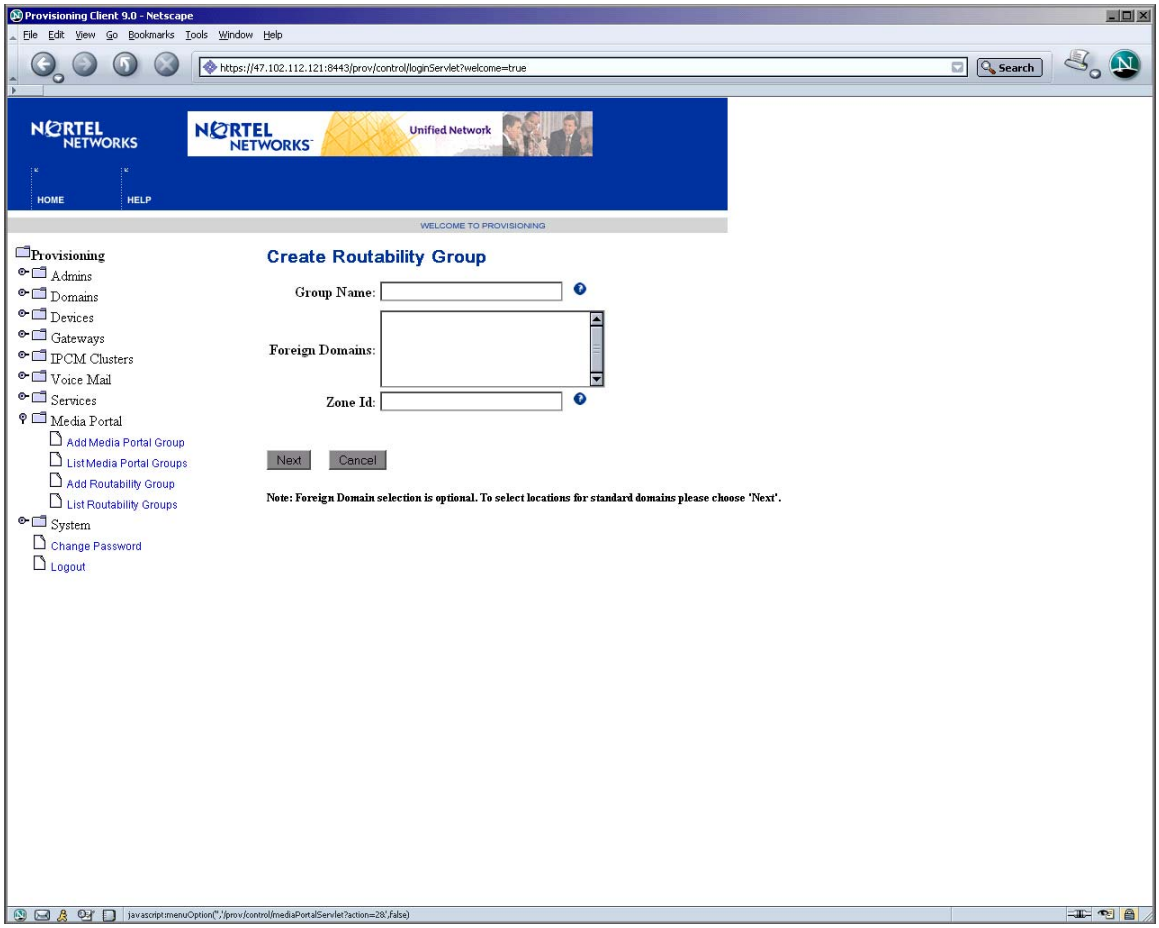


Figure 7 Zone Id information provisioning from Provisioning Client

1.6 SIP Line data provisioning using OPI

SIP Line data can be provisioned onto CS2K SS using both the Provisioning Client or OPI. The methods that are available via OPI for SIP Lines:

- Methods that will be used for user provisioning:

addUser (String domain, User user)
modifyUser (String username, User user)
removeUser (String username)
getUser (String username) : User

- new OPI methods introduced for provisioning SIP Line data

getUserByEndPoint (String endPointID):String
setSIPLineData(String userName, SIPLineData sipLineData)
getSIPLineDataByUserName(String userName):SIPLineData
removeSIPLineData (String userName)
getSIPLineData(String endPointID):SIPLineData
getSIPLineDataByDomain(String domain,int start, int stop):SIPLineData[]
getSIPLineDataByDomainByVMG(String domain, String vmg, int start, int stop):SIPLineData[]
getUserByDN(String dN):String

1.7 Hardware Requirements or Dependencies

The Provisioning Manager configuration in the SIP Lines product is as shown below. SESM will configure the Primary and secondary Provisioning Server Address and Port

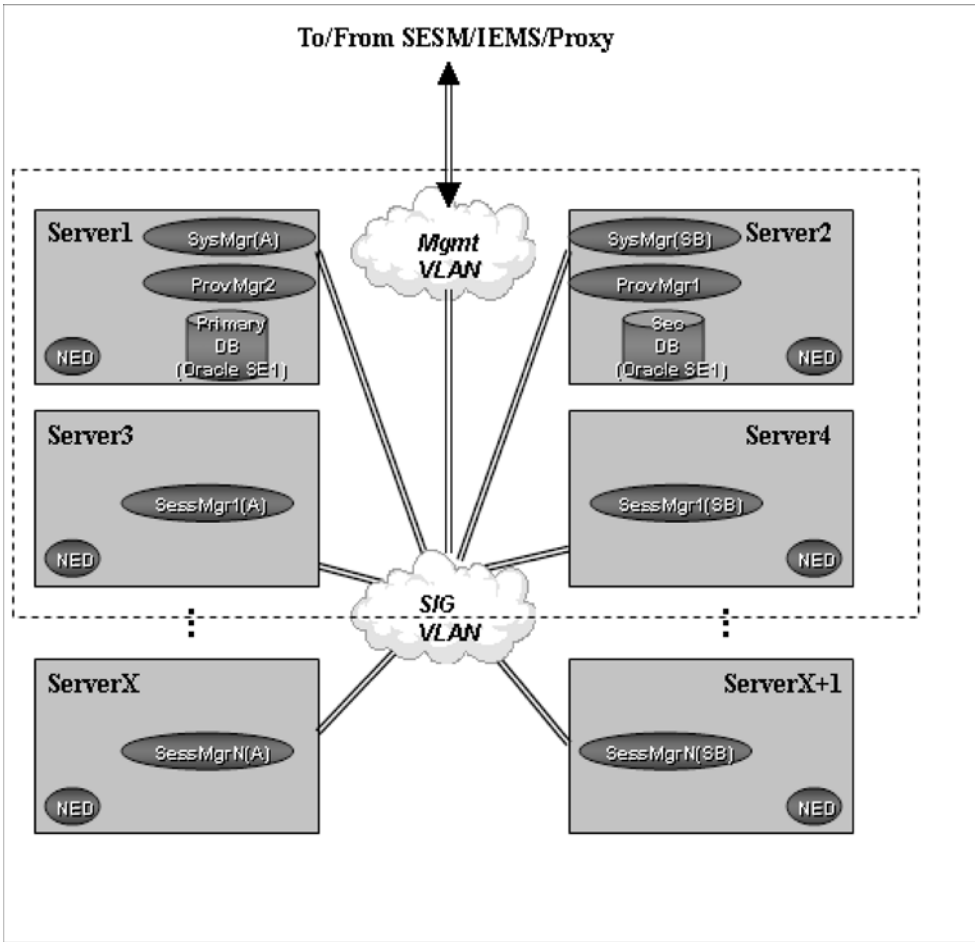


Figure 8 CS2K SS Core server hardware configuration

1.8 Software Requirements or Dependencies

The following software is required for building and using OPI on the SESM and will be delivered as a part of this feature.

- **Axis 1.1 final**: SOAP engine for OPI
- **passwdhash.jar**: contains a utility for hashing the administrator password for security reasons.
- **OPIStubs.jar**: contains the OPI client side stubs along with properties files containing error code and description mapping.
- **truststore**: for HTTPS/SSL based transactions using OPI.

The location of the software will be in the mcp_core_root and mcp_3rdparty vobs and can be accessed by the loadbuild process as needed.

1.9 CS2k SS Service Interaction

The following are services that cannot be provided from CS2K SS for a subscriber who has the CS2000 SIP Line service in the service package:

- Assistant Console
- Assistant Support
- Call Park
- Converged Desktop
- Device Access Restrictions
- Hot Line
- Music On Hold
- Net6 Support on i2004
- Wireless Client
- Voicemail
- Unified Communications
- Calling Line Id Restriction
- Call Waiting Disable
- PCClientSet Control

1.10 OPI Version and Release Information

There will be three new OPI methods introduced which will give current release and version information for OPI and MSM. The methods are:

Method Name	Purpose
getOPIVersion():String	current version of OPI
getOPISupportedVersion():String[]	List of OPI versions supported by the current release
getReleaseName():String	current release for MCP/ CS2K MSM

The information from these method calls can be used for the purpose of software upgrades based on release and OPI version that are compatible.

1.11 License key requirements and miscellaneous changes

The service CS2000 SIP Line at this time is not license keyed, meaning that the number of subscribers that can have this service is not controlled.

Also, as a part of this feature, the lengths of user name and the domain names are being increased to be 64 characters as opposed to the 60 character limit that enforced in earlier releases.

1.12 Glossary

Term	Description
OPI	Open Provisioning Interface
SESM	Succession Element and Sub-Element Manager
HTTP	Hyper Text Transfer Protocol
HTTPS	HTTP over SSL
SSL	Secure Sockets Layer
SIP	Session Initiation Protocol

Product = MCS

A00009045 -- CallP Checkpointing Support

Functional Description

1: Applicable Solution(s)

PT-AAL1, PT-IP, DMS

1.1 Description

This feature adds the following capabilities to the CS2000 Multimedia Session Manager (MSM):

- The ability to checkpoint active calls to the standby instance of an MSM.

  For the purposes of this feature an active stable call is one that has been answered. Answering a SIP call means that the 200 OK response to the initial invite has been received or sent by the active session manager.

  Previously this information would have been lost on failover, but recreated, in part, by the long call audit and/or call clearing.

- The ability to checkpoint subscriptions to the standby instance of an MSM.

  Subscriptions refer to SIP SUBSCRIBE messages for a particular event package.Because if this checkpointing, subscription to service packages like presence , call park.. will be preserved after failover.

  Previously this information would have been lost on failover.

- The ability to checkpoint network call logs to the standby instance of an MSM.

  The call log information is preserved so that a user will be able to get a record of their calls from the Personal Agent even after a failover.

  Prior to this feature if the failover occurred before the call log was written to the DB the call log would have been lost. The database write occurs upon the completion or rejection of the call.

- Enhanced presence processing and recovery of “On the Phone” presence after failover.

  A number of enhancements have been made to presence processing. Additionally, after a failover, the newly active instance of the MSM is able to recover a user’s presence state to an “On the Phone” state if they are active in a call. Prior to this feature the user’s presence state would have been changed to “Connected” after failover.

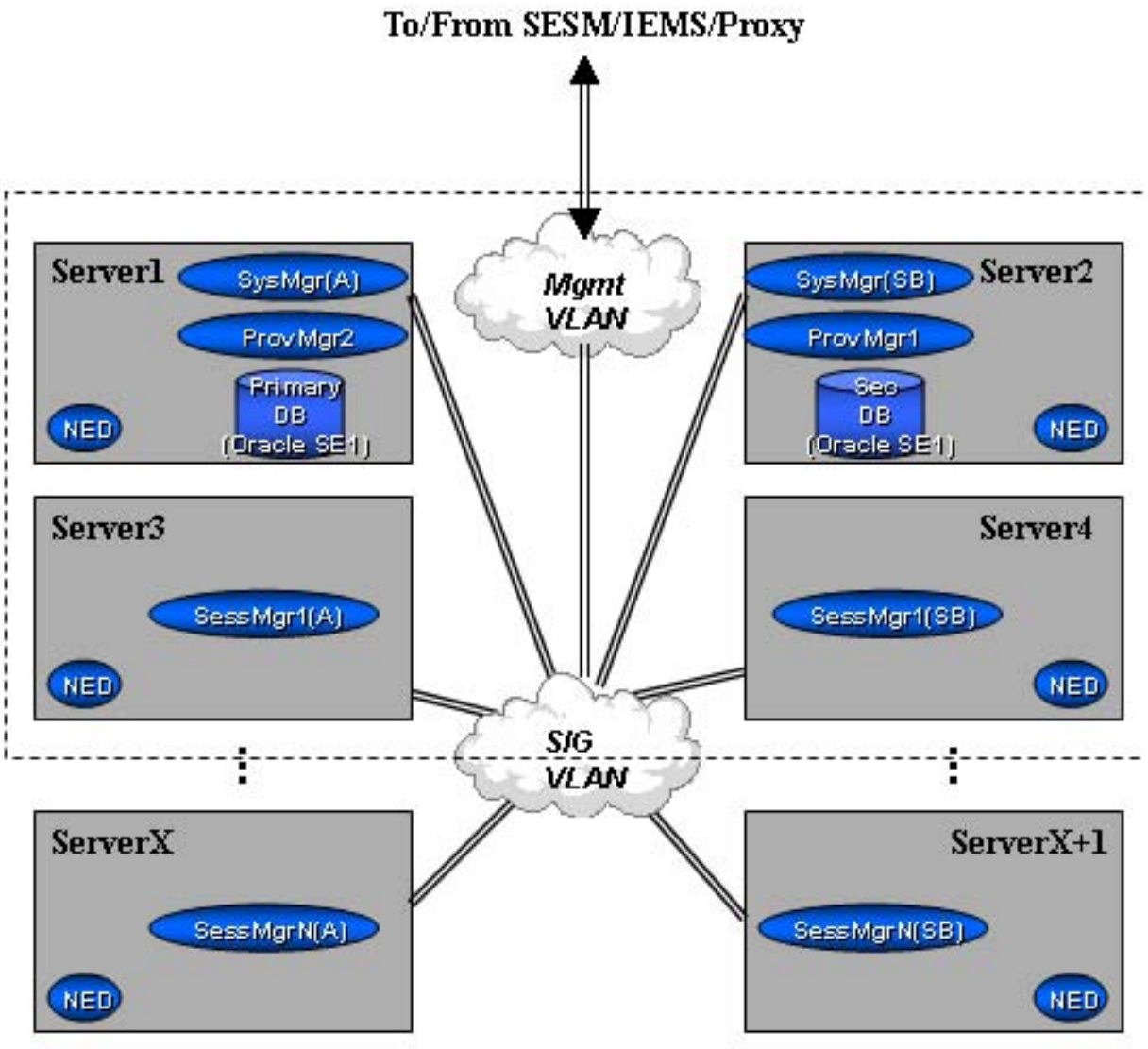
- This features adds 2 additional levels of overload to what was available in 3.0 and 4.0.

  In 3.0 and 4.0, there was only one level of overload, specified by 2 numbers, a "None" number and a "Severe" number. MCS would go into overload when the "Severe" number was exceeded. In the picture below, MCS would go into overload when the Call Queue exceeds 100. When in overload, alarms are raised, and all new sessions are blocked. Sessions that are already in progress would be allowed to continue. When the Call Queue goes below 70, the alarm is cleared, and all sessions are serviced.

1.2 Hardware Requirements or Dependencies

The diagram below represents the MSM configuration for 35000 subscribers. In this diagram, Server 3 and 4 represent an active/standby pair for Session manager instance 1 (SessMgr1). Server 3 is the active instance signified by the (A) and Server 4 represents the standby instance signified by (SB).

Figure 1 35000 Subscriber System



The following diagram represents the configuration for 15000 subscribers. In this diagram, SessMgr1(SB) represents the standby instance for SessMgr1(A), the active instance.

Figure 2 15000 Subscriber System

The diagrams above do not represent the only configuration possible.

1.3 Software Requirements or Dependencies

This feature is part of the MCP 9.0 release.

1.4 Limitations and restrictions

There are limitations in the processing for checkpointing. When a standby instance becomes active due to a failover there are two possible problems, both are due to the case where a Checkpoint is in process at the time the failover occurs. The newly active system can have calls active that were in the process of disconnecting and the checkpoint was not transferred before the failover occurred. In addition calls that were just setup prior to the failover will not appear on the newly active instance.This leads to inconsistent state information between the Sip Line clients, the MSM and the GWC. .

One audit goes active once the standby instance becomes the active instance to correct the inconsistencies. This audit causes the MSM to send a SIP message to all SIP Line clients the MSM thinks is active on a call to verify that they are actually on a call.

Due to the above limitations on checkpointing not all of the calls to a subscriber will be logged. Any entry in the local call log table in the process of being checkpointed at the time of the fail over will be lost. Unfortunately there is no way to mediate this loss of information.

Subscriptions have the same limitations as the call logs in that there is no way to audit them from the Session Manager. However any subscription that is lost will be refreshed by the client within one hour which is the expiration time returned by the session manager upon processing a subscription.

1.4.1 Removed Limitations and restrictions

A number of restrictions and limitations that were previously in effect have been lifted as a result of enhancements to the presence service operation.

Reporting of “On the Phone” presence is no longer limited to Nortel clients. Previously, only the Nortel IP Client Manager, Nortel Multimedia PC Client, and Nortel Multimedia Web Client were capable of reporting that they were “On the Phone” through signalling to the MSM. Now any subscriber that has an answered call going through the MSM will have their “On the Phone” presence tracked at the MSM itself. This allows third-party clients to be shown as on the phone regardless of their client’s capability set.

The MSM now detects dead clients much faster than in previous releases. This affects the scenario of a user’s client crashing or losing network connectivity and is unable to re-register with the MSM. In this case, their presence state will change to “Unavailable Offline” close to the time their last registration expires. In previous releases the interval between their last registration expiring and their presence state being updated was highly non-deterministic due to the auditing mechanism being used and system load. This mechanism has been improved to be less sensitive to system load and more timely than in previous releases.

The auditing mechanism to detect dead clients has also been applied to detecting stale clients that last reported that they are in an “Active Available” state. This is the case where a client reports that the user is actively using the PC. The MSM previously audited clients in this state by asserting that they were no longer in the active state. As a result this prompted the client to re-assert that the PC is actively being used to prevent users being shown as “Active Available” when network connectivity may have posed a challenge to accurately reporting their state. In previous releases the time period between audits was highly variable. The new mechanism reduces the variable lag time between the engineered activity auditing period and the audit being performed.

1.5 Interactions

Advanced services are not guaranteed to work after the fail over of the call. The only service guaranteed to work is the release of the call by either party in the call. Other messages will be sent a 500 service unavailable if the core is not able to process the message. Some of the services not guaranteed to work afte failover are MOH, Call Park, Boss/admin, unstable calls like consultative or blind transfers in progress , CD calls.

The presence service has been better integrated into the system overload controls. As a result, if the MSM is in a minor overload state, presence notifications will not be sent to people watching a particular user. Only the user's own self-subscriptions will be notified of presence state changes. If the MSM is in a major or severe overload state, presence notifications will not be sent to anyone. When the MSM returns to the minor overload state any postponed self-presence notifications are sent out as a background process. When the MSM is no longer in overload notifications return to normal and any postponed notifications are sent out as a background process.

Additionally, the presence service no longer processes presence events using the same processing queue as call processing. This reduces the processing time for registration requests and allows the system to handle presence processing at a different priority from call processing during overload conditions.

1.6 Operational Measurements

New OMs will be introduced with this feature.

1.6.1 Checkpoint OMs

One new OM is introduced relating to checkpointing: CheckpointedCalls.

The CheckpointedCalls OM can be used on the standby instance to monitor the number of calls that would be preserved in a case of a failover.

This OM will be reset in case of extensive connection loss between the active and standby instance, as all calls will be re-checkpointed when the connection is reestablished.

1.6.2 Presence OMs

A new OM group is introduced as part of the presence enhancements: Presence Event Report. This OM group is in addition to the OMs defined for presence in previous releases. This OM group tracks the behavior of the various presence events that are processed by the server.

For each of the rows in the report, which represent the eight presence event types: Activity, End Call, Inactive, Login, Logout, New Call, and Manual there are five columns:

- Created

  The number of events of that type that have been created in the system. This gives the operator an idea of the relative frequency of occurance for that presence event type.

  This OM is a counter register and is reset to zero after each office transfer period.

- Processed

The number of events of that type that have been processed by the presence event processor. Just because a presence event is created, does not mean that it is guaranteed to ever be processed. It may be eliminated from consideration because of an opposing presence event.

This OM is a counter register and is reset to zero after each office transfer period.

- Optimized

  The number of events of that type that have been optimized by the presence event processor. An event is optimized when it an opposing presence event is processed that nullifies the presence event change that would have taken place. For instance, if a new call event is processed, and the presence event processor sees that there is an opposing end call event in the queue or parked, there is no further point in processing either event, they cancel each other out.

  This OM is a counter register and is reset to zero after each office transfer period.

- Queued

  The number of events that are currently in the presence event processor queue waiting to be processed.

  This OM is a usage register. It increments and decrements according to the length of the processing queue and is unaffected by the office transfer.

- Parked

  The number of events that have been initially processed, but must wait for the presence guard timer to expire before being processed. These events are “parked” waiting for the guard timer to expire before being applied. They are frequently candidates for optimization.

  This OM is a usage register. It increments and decrements according to the length of the processing queue and is unaffected by the office transfer.

In addition to the new OM group, the following OMs are added to the existing “Presence” OM group:

- throttleNotifySelfOnly

  This OM is pegged every time the system does not send out a notifications to non-self subscriptions because of a presence state change during minor overload. This is pegged once for the entire state change, and does not reflect the actual number of notify messages that were not sent out.

This OM is a counter register and is reset to zero after each office transfer period.

- throttleNotifyAll

  This OM is pegged every time the system does not send out any notifications, including self-subscriptions because of a presence state change during major or severe overload. This is pegged once for the entire state change, and does not reflect the actual number of notify messages that were not sent out.

  This OM is a counter register and is reset to zero after each office transfer period.

1.7 System Manager Changes

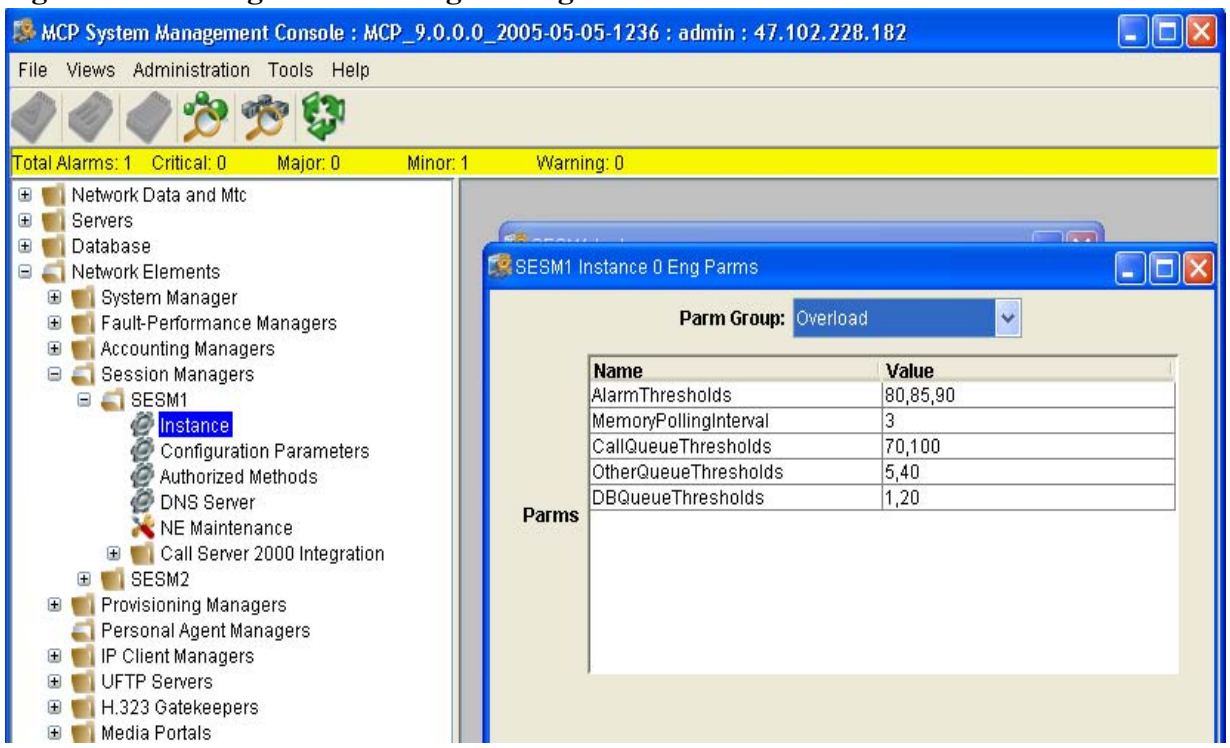
Instead of just having the Severe overload condition, there are 2 other overload conditions. They are:

- Minor -- presence notifications except to self and admins won't be generated.
- Major -- Same as in Minor, additionally, IM will be blocked.
- Severe -- Everything except in-session messages will be blocked.

To specify the additional levels, instead of just having the "None" and "Severe" numbers, the format is to accept 4 numbers: "None", "Minor", "Major", and "Severe".

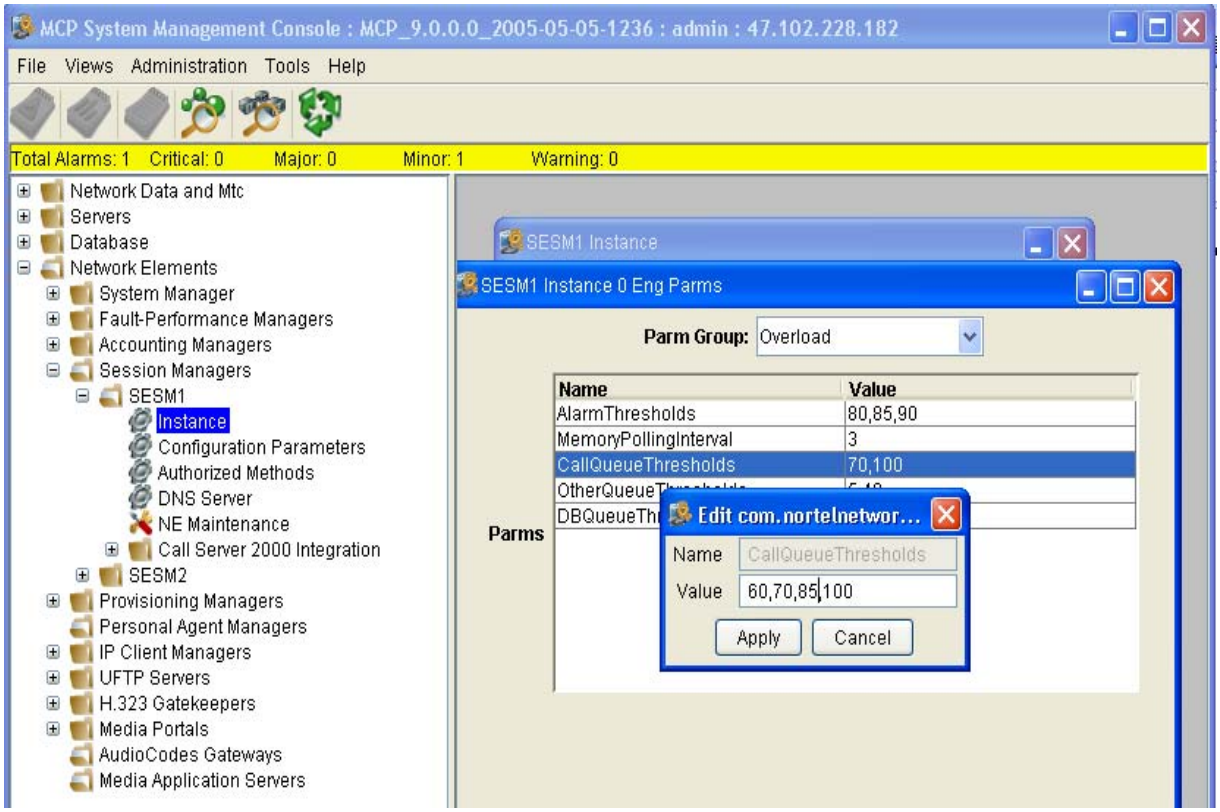
If only 2 levels are specified, such as after an upgrade, then the same behavior as in 3.0 and 4.0 is provided (see Figure 14, “Existing Overload Engineering Parameters,” on page 1719).

Figure 14: Existing Overload Engineering Parameters



When four numbers are provided, the increased overload granularity is enabled. In the example below (Figure 15, “New Overload Engineering Parameters,” on page 1720) if the Call Queue exceeds the Minor number (70), and stays at that level for a few seconds, MCS will stop generating presence notifications. If the Call Queue exceeds the Major number (85), then Instant Messages will be blocked. If the Call Queue exceeds the "Severe" number, then all new sessions will be blocked. For any of the overload conditions, the same alarm is raised, but different severities are assigned to those alarms.

Figure 15: New Overload Engineering Parameters



1.8 Glossary

Term	Description
Info Ping	A SIP INFO message sent without a message body. The proper response is a 200 Ok if the INFO is within a call and a 481 if outside of a call. Defined in RFC 2976
MSM	Multimedia session Manager
SIP	Session Initiation Protocol

Product = MCS

A00009092 -- CS2K MSM SIP Lines Cisco 7960 Client Integration

Functional Description

1: Applicable Solution(s)

MCS

1.1 Description

This feature covers the integration of the Cisco 7960 SIP-enabled IP Phone with the CS2000 MSM SIP Lines program. This document details the functional requirements for the phone and CS2000 MSM 1.0 compliancy to the requirements.

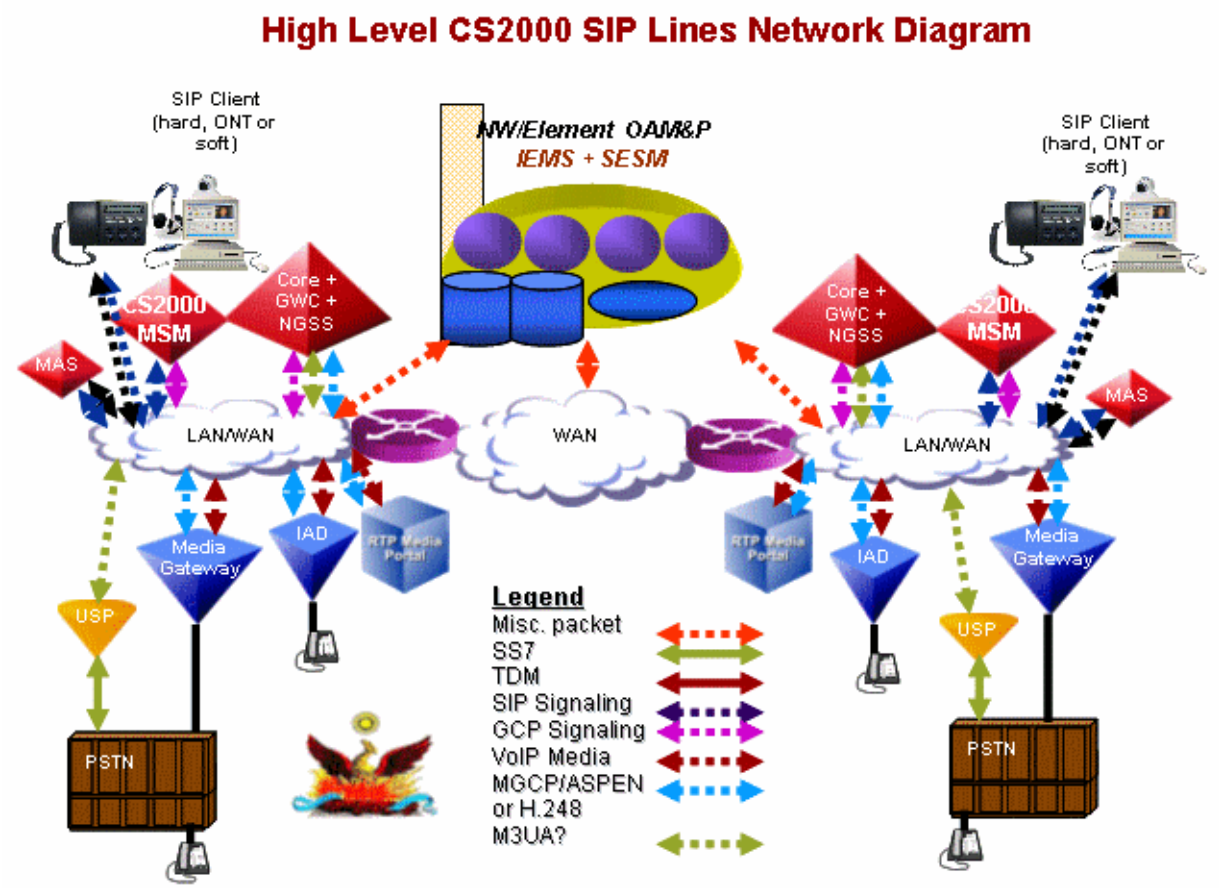
The Cisco 7960 requirements are broken into 3 categories:

1) Call Processing Services and Functionality

2) Software Download and configuration

3) NAT traversal

1.1.1 Hardware Requirements or Dependencies



1.1.2 Software Requirements or Dependencies

This feature is part of the MCP 9.0 Release. The Cisco Firmware release is POS3-07-4-00.sb2 (version 7.4)

The following requirements compliancy matrix lists both the feature requirements for the phone and which features are supported for CS2000 SS 1.0 in SN09.

Note: An asterisk (*) in the “Supported” column indicates the requirement is supported by the phone but requires development work on the CS2000 SS.

Feature/Capability	Supported on the Cisco 7960	Additional Notes
911	SN09	Routing provided by the core
Address book (personal)	No	

AIN services	n/a	
Analog signaling	n/a	
Answering Machine	n/a	
Assistant Console (Boss/Admin)	n/a	
Audible voice identity delivery	n/a	
Basic inbound call delivery	SN09	
Bridged lines	n/a	
Bulletins	No	
Busy line verification	n/a	
Call back to busy line (ACBAR)	SN10	Done via feature activation on the core
Call forward locally on 7960	SN09	Programmed locally via softkeys on the phone
Call Forward via Personal Agent	SN09	
Call Forward via CS2000 Core	SN09* (if via FAC)	Handled by the core
Call Park	No	Not supported in SIP functionality on the phone – not available in standalone solution
Call rejection	n/a	
Call return	SN09 * (if via FAC)	Handled at the core
Call subjects	No	
Call tracing	SN09 * (if via FAC)	Handled at the core
Call waiting	SN09	User configurable on the phone
Call waiting disable	SN09	User configurable on the phone
Caller ID	SN09	User configurable on the phone
Click to call	n/a	Not initiated from the phone
Clipboard	n/a	
CODEC - G711	SN09	
CODEC - G729	SN09	
Conference (Ad hoc; 3-way calling only)	SN09	Phone provides the audio mixing at G.711 only – max 3-way call
6-way Adhoc conference	n/a	Not supported; max 3-way mixing
Converged Desktop	SN10	
Decline	n/a	Not supported by the phone
Device restrictions	n/a	
Direct connect	No	
Directory (global address via LDAP)	No	
Distinctive ringing	No	

Do Not Disturb	SN09	User configurable on the phone
File exchange	n/a	
Firewall support	SN09 *	Support for non-symmetric firewalls
Friends online	No	
Group alerting	n/a	
Hold (automatic hold)	SN09	Basic hold/retrieve performed on the phone
Hotline	n/a	
Ignore	n/a	
Import Outlook contacts	n/a	
Inbound call delivery to a group of lines	n/a	
Inbox	SN09	Phone has “Received Calls” and “Missed Calls” directories
Instant Message (IM)	No	Not supported by the phone
Lawful intercept (via Core)	SN09	Done by the core
Meet me Audio Conferencing	SN09 *	
Message Waiting Indicator (MWI)	SN09	
Multiple Lines/Users supported	SN09	Supports multiple users logged into the same device
Outbound call dialing	SN09	
Outbound call routing	SN09	
Outbound call screening	SN10	
Outbox	SN09	Phone has a “Placed Calls” directory
Outlook integration	n/a	
Picture ID	No	
Presence	n/a	SIP Presence not supported by the phone. “On the Phone” presence available via the SS
Profile manager	n/a	
Protocol - TCP	No	
Protocol - TLS	No	
Protocol - UDP	SN09	
Quality of Service (QoS) Reporting	n/a	
QoS Type Of Service (ToS) Marking	SN09	
Recursive calling (party line)	n/a	
Redirect	n/a	
Reject reasons	No	

Screening and routing (follow me, sequential ringing)	n/a	
Search options (address books)	No	
Server selection	SN09	Admin can provision a single Session Manager Address at the outbound proxy
Sharing	n/a	
Speed dialing	SN10	
Telemetry	n/a	
Transfer – Blind	SN09	Transfer failure cannot be retrieved
Transfer – Consult	SN09	Transfer failure cannot be retrieved
User configurable settings – requires user knowledge of phone configuration password	SN09 (See Section 2.5 below)	
User controlled codec selection – requires user knowledge of phone configuration password	SN09	
Video (video on demand)	n/a	
Voice mail	SN09	
Web push and co-browsing	n/a	
Whiteboard	n/a	

1.2 Limitations and restrictions

Certain call processing limitations of the 7960 result in the following services limitations:

- Calling Name/Number Blocking must be done via star-code activation on the core. The 7960 SIP implementation of this feature is not compatible with the CS2000 SS.
- Call Transfer is accomplished using the SIP REFER method. Transfers that fail cannot be retrieved due to the implementation on the 7960.
- Ad-hoc conferencing is accomplished as a 3-way call. The Cisco 7960 provides the audio mixing at the device itself. The 7960 only mixes G.711 packets, thus any existing legs negotiated to G.729 will attempt to be renegotiated to G.711. If a device does not support the G.711 codec then it cannot be included in a 3-way conference on the phone. The maximum ad-hoc conference size is 3. 6-way conferencing must be done via an external conferencing server.
- Presence is not supported from the phone. Therefore, all presence indications or updates must be derived from the active call state or registration state. By default, the CS2000 SS will support a presence state

of “connected” for a registered user, “unavailable offline” for a user who is not registered, and “On the Phone” for a user who is in an active call. Any additional presence states must be derived as if this device were a “Non SIP Lines device” by the core.

In addition, CS2000 SS SIP Lines will not support initiating a remote reset of the Cisco 7960 phone (via NOTIFY) for this release. Since reset remote is not supported, the phones cannot initiate a firmware upgrade without manual intervention. All firmware upgrades must be done manually via editing the configuration files located on the TFTP server and resetting the phone. Once the phone is reset, it will compare the current firmware load in flash with the load specified on the TFTP Server configuration file and initiate a download of the new firmware if the loads do not match. The network administrator is responsible for scheduling and initiating the reset of the phones for firmware upgrade. In addition, the TFTP server will not be integrated with the CS2000 SS solution, but rather a separate server from any other CS2000 SS component.

Note: Currently, there is no security mechanism in place to authenticate a remote reboot request via NOTIFY.

Likewise, provisioning of a CS2000 SS SIP Lines user will not automatically generate a phone specific configuration file on the TFTP server. The admin is responsible for creating and maintaining all the configuration files on the TFTP server for each phone in the network.

The Cisco phone does not provide a NAT traversal mechanism to indicate in SIP signaling the presence of a firewall between the client and the CS2000 SS. To compensate for this, the CS2000 SS will compare the UDP packet source IP address against the SIP Via Header IP address to determine whether or not to treat this client as a firewalled client and replace the contact IP address appropriately. The mechanism for keeping the firewall binding active will be a combination of the periodic maintenance audit via the OPTIONS message and a reduced registration expiry timer. However, if a NAT device dynamically re-binds a new IP and port to the Cisco 7960 after the phone is initially registered, a period of time will exist when calls can no longer terminate to the Cisco phone due to the stale NAT binding. This period of time can be up to the configured registration expiry timer. This firewall detection algorithm will not work for “symmetric” firewall solutions, where the IP address on both sides of the NAT device remain the same and only the port changes. Thus, symmetric firewall solutions are not supported for the first release.

1.3 Interactions

Where applicable, services initiated from the Cisco phone will use existing SIP service implementation to accomplish the desired feature. However, due to the

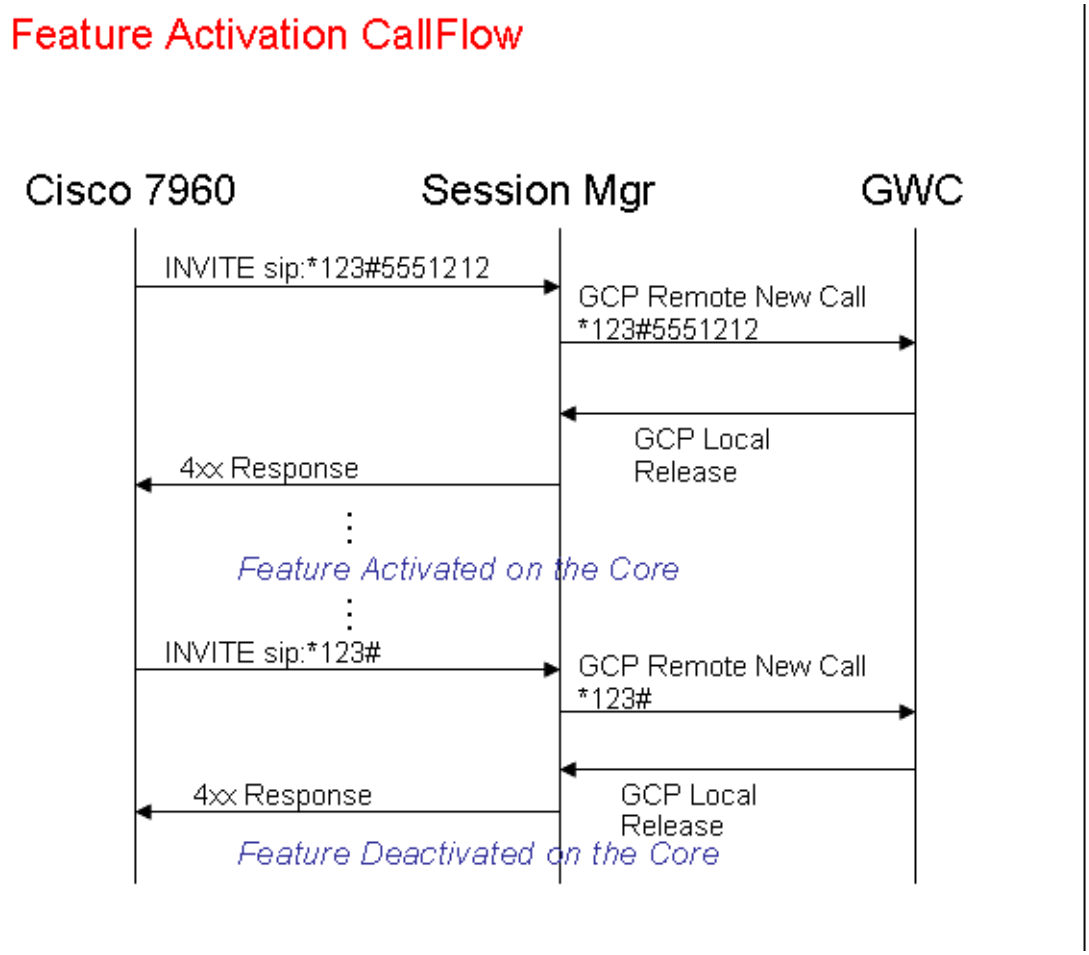
complex suite of services available to SIP Lines on the CS2000 Core, some feature activation will be done via star-code feature activation codes (FACs).

These services can be activated or deactivated by the phone via the configuration menu system:

- Do Not Disturb
- Auto-Completion of numbers
- Call Waiting
- Call Hold Ringback
- Stutter Message Waiting
- Auto-Answer (Intercom)
- Speed Dial (up to 5 numbers)
- Call Forward Unconditional

The services below will be permanently disabled on the phone and only available thru FACs. See the proposed call flow below for an indication of how the digits will be presented to the core.

- Caller ID Blocking
- Anonymous Call Reject



Call Forward is available on the phone (CFU) and also via FACs at the core.

1.4 Recommended Configuration

The following recommended settings should be used to assure interoperability between the 7960 and the CS2000 SS. The files reside in the root directory of an available TFTP server that all the 7960 phones are configured to use.

1.4.1 Common SIP Parameters

The SIPDefault.cnf file contains the common sip parameters needed by all the 7960 devices. These parameters control the default behavior of the phone and provide the phone the Session Server address and domain name that should be used. If these default parameters are not applicable to all 7960 phones in the network, then multiple TFTP servers should be used or duplicate parameters included in the phone-specific configuration file detailed in section 2.7.2. The file should be of this general format with only the domain name and IP Addresses highlighted in blue changed:

```
# SIP Default Generic Configuration File


# Image Version
image_version: P0S3-07-4-00

# Proxy Server
proxy1_address: "nortel.com" ; Can be dotted IP or FQDN
proxy2_address: ""           ; Can be dotted IP or FQDN
proxy3_address: ""           ; Can be dotted IP or FQDN
proxy4_address: ""           ; Can be dotted IP or FQDN
proxy5_address: ""           ; Can be dotted IP or FQDN
proxy6_address: ""           ; Can be dotted IP or FQDN

# Proxy Server Port (default - 5060)
proxy1_port: 5060
proxy2_port: 5060
proxy3_port: 5060
proxy4_port: 5060
proxy5_port: 5060
proxy6_port: 5060

# Proxy Registration (0-disable (default), 1-enable)
proxy_register: 1

# Phone Registration Expiration [1-3932100 sec] (Default - 3600)
timer_register_expires: 3600

# Codec for media stream (g711ulaw (default), g711alaw, g729a)
preferred_codec: g711ulaw

# TOS bits in media stream [0-5] (Default - 5)
tos_media: 5

# Inband DTMF Settings (0-disable, 1-enable (default))
dtmf_inband: 1

# Out of band DTMF Settings (none-disable, avt-avt enable (default), avt_always -
always avt )
dtmf_outofband: avt

# DTMF dB Level Settings (1-6dB down, 2-3db down, 3-nominal (default), 4-3db up, 5-6dB
up)
dtmf_db_level: 3

# SIP Timers
timer_t1: 500                ; Default 500 msec
```

```
timer_t2: 4000                ; Default 4 sec
sip_retx: 10                  ; Default 10
sip_invite_retx: 6            ; Default 6
timer_invite_expires: 180     ; Default 180 sec

####### New Parameters added in Release 2.0 #######

# Dialplan template (.xml format file relative to the TFTP root directory)
dial_template: dialplan

# TFTP Phone Specific Configuration File Directory
tftp_cfg_dir: ""; Example:  ./sip_phone/

# Time Server (There are multiple values and configurations refer to Admin Guide for
Specifics)
sntp_server: ""               ; SNTP Server IP Address
sntp_mode: directedbroadcast ; unicast, multicast, anycast, or directedbroadcast
(default)
time_zone: EST                ; Time Zone Phone is in
dst_offset: 1                 ; Offset from Phone's time when DST is in effect
dst_start_month: April        ; Month in which DST starts
dst_start_day: ""             ; Day of month in which DST starts
dst_start_day_of_week: Sun    ; Day of week in which DST starts
dst_start_week_of_month: 1    ; Week of month in which DST starts
dst_start_time: 02            ; Time of day in which DST starts
dst_stop_month: Oct           ; Month in which DST stops
dst_stop_day: ""              ; Day of month in which DST stops
dst_stop_day_of_week: Sunday ; Day of week in which DST stops
dst_stop_week_of_month: 8     ; Week of month in which DST stops 8=last week of month
dst_stop_time: 2              ; Time of day in which DST stops
dst_auto_adjust: 1            ; Enable(1-Default)/Disable(0) DST automatic adjustment
time_format_24hr: 1           ; Enable(1 - 24Hr Default)/Disable(0 - 12Hr)

# Do Not Disturb Control (0-off, 1-on, 2-off with no user control, 3-on with no user
control)
dnd_control: 0                ; Default 0 (Do Not Disturb feature is off)

# Caller ID Blocking (0-disbaled, 1-enabled, 2-disabled no user control, 3-enabled no
user control)
callerid_blocking: 2              ; Default 0 (Disable sending all calls as anonymous)

# Anonymous Call Blocking (0-disabled, 1-enabled, 2-disabled no user control, 3-enabled
no user control)
anonymous_call_block: 2           ; Default 0 (Disable blocking of anonymous calls)

# DTMF AVT Payload (Dynamic payload range for AVT tones - 96-127)
dtmf_avt_payload: 96              ; Default 101
```

```
# Sync value of the phone used for remote reset
sync: 1                         ; Default 1

####### New Parameters added in Release 2.1 #######

# Backup Proxy Support
proxy_backup: ""                ; Dotted IP of Backup Proxy
#proxy_backup_port: 5060        ; Backup Proxy port (default is 5060)

# Emergency Proxy Support
proxy_emergency: ""             ; Dotted IP of Emergency Proxy
#proxy_emergency_port: 5060     ; Emergency Proxy port (default is 5060)

# Configurable VAD option
enable_vad: 0                   ; VAD setting 0-disable (Default), 1-enable

####### New Parameters added in Release 2.2 ######

# NAT/Firewall Traversal
nat_enable: 1                   ; 0-Disabled (default), 1-Enabled
#nat_address: ""                ; WAN IP address of NAT box (dotted IP or DNS A record
only)
voip_control_port: 5060         ; UDP port used for SIP messages (default - 5060)
start_media_port: 16384         ; Start RTP range for media (default - 16384)
end_media_port: 32766           ; End RTP range for media (default - 32766)
#nat_received_processing: 0     ; 0-Disabled (default), 1-Enabled

# Outbound Proxy Support
outbound_proxy: "47.104.26.178" ; restricted to dotted IP or DNS A record only
outbound_proxy_port: 5060       ; default is 5060

####### New Parameter added in Release 3.0 #######

# Allow for the bridge on a 3way call to join remaining parties upon hangup
cnf_join_enable : 0             ; 0-Disabled, 1-Enabled (default)

####### New Parameters added in Release 3.1 #######

# Allow Transfer to be completed while target phone is still ringing
semi_attended_transfer: 0       ; 0-Disabled, 1-Enabled (default)

# Telnet Level (enable or disable the ability to telnet into the phone)
telnet_level: 2                 ; 0-Disabled (default), 1-Enabled, 2-Privileged

####### New Parameters added in Release 4.0 #######

# XML URLs
```

```
services_url: ""                ; URL for external Phone Services
directory_url: ""               ; URL for external Directory location
logo_url: ""                    ; URL for branding logo to be used on phone display

# HTTP Proxy Support
http_proxy_addr: ""             ; Address of HTTP Proxy server
http_proxy_port: 80             ; Port of HTTP Proxy Server (80-default)

# Dynamic DNS/TFTP Support
dyn_dns_addr_1: ""              ; restricted to dotted IP
dyn_dns_addr_2: ""              ; restricted to dotted IP
dyn_tftp_addr: ""               ; restricted to dotted IP

# Remote Party ID
remote_party_id: 0              ; 0-Disabled (default), 1-Enabled
```

1.4.2 Device Specific Parameters

The device-specific file of the filename format SIP<MACAddress>.cnf is used to specify parameters that apply only to a specific 7960 phone. In addition, parameters included in this file will take precedence over duplicate parameters in the SIPDefault.cnf file. The file should be of this general format with the each user-field matching what is provisioned:

```
# SIP Configuration Generic File

# Line 1 appearance
line1_name: user10

# Line 1 short name
line1_shortname: user10

# Line 1 Registration Authentication
line1_authname: "user10"

# Line 1 Registration Password
line1_password: "1234"

# Line 2 appearance
line2_name: user3

# Line 2 Registration Authentication
line2_authname: "user3"

# Line 2 Registration Password
line2_password: "1234"
```

```
####### New Parameters added in Release 2.0 #######

# All user_parameters have been removed

# Phone Label (Text desired to be displayed in upper right corner)
phone_label: "Phoenix SIP Lines         "; Has no effect on SIP messaging

# Line 1 Display Name (Display name to use for SIP messaging)
line1_displayname: "user10"

# Line 2 Display Name (Display name to use for SIP messaging)
line2_displayname: "user3"


####### New Parameters added in Release 3.0 ######

# Phone Prompt (The prompt that will be displayed on console and telnet)
phone_prompt:   "SIP Phone"      ; Limited to 15 characters (Default - SIP Phone)

# Phone Password (Password to be used for console or telnet login)
phone_password: "cisco" ; Limited to 31 characters (Default - cisco)

# User classifcation used when Registering [ none(default), phone, ip ]
user_info: none
```

1.4.3 Dialplan Definition

Finally, the dialplan.xml file should have the following entry to allow the proper handling of FAC star-code processing:

```
<DIALTEMPLATE>
    <TEMPLATE MATCH="\*.*#,*" Timeout="5"/>      <!-- Anything else -->
</DIALTEMPLATE>
```

1.5 Glossary

Term	Description
FAC	Feature Activation Code
NAT	Network Address Translation
TFTP	Trivial File Transfer Protocol
SS	Session Server

Product = MCS

A00009241-- NCAS and QSIP Development on CS2K SS

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

The Non-call associated signalling (NCAS) Link on Communication Server 2000 (CS2K) Session Server (SS) platform with query SIP line data (QSIP) application feature provides a light-weight switching control point (SCP) like functionality (SCPLite). The NCAS link provides a non-call associated link between the CS2K SS and the core. At present the NCAS link is only used by the SIP Lines program for QSIP command interface (CI) command in the core to get the static and dynamic data snap shot from the CS2K SS platform related to the SIP line.

The display of the static and dynamic data is provided by QSIP CI command at CI increment.

1.2 Hardware Requirements or Dependencies

The development is on CS2K SS platform.

This activity does not require any new hardware.

1.3 Software Requirements or Dependencies

This activity uses SCTP library (SCTP.DE) developed in Germany for SCTP communication with the Core. The SCTP.DE is a generic SCTP library available from the web and it is not a NORTEL product.

The activity depends on the following two activities:

- QSIP CI Command development in the core under actid A00008556.
- OAM and GUI development in the CS2K SS platform under actid A00009028.

1.4 Limitations and restrictions

- Only one NCAS link is allowed for QSIP Application. When the link is active for QSIP application, subsequent QSIP application request to create another NCAS link will be ignored.

- QSIP application has lowest priority. Therefore, in case of high traffic and/or abnormal conditions, QSIP application will not response with the data within the timeout period.
- During failover cases, the NCAS link is disconnected with the core and re-established from the active side. All outstanding QSIP request prior to failover complete will be discarded and no response will be provided.

1.5 Interactions

The QSIP command from the core is a stand alone command. In the core, the QSIP CI increment send a request to CS2K SS platform. The software developed under this activity gathers the static and dynamic data associated with the specific SIP line, and sends an asynchronious response to QSIP CI in the core.

The QSIP request, data collection and sending response are independent from other activities/actions/events in the CS2K SS platform. Therefore, no specific interaction anticipated by this activity.

1.6 Glossary

Term	Description
CI	Command Interface
CS2K	Communication Server 2000
GUI	Graphical User Interface
NCAS	Non-Call Associated Signalling
OAM	Operation, Administration and Maintenance
QSIP	Query SIP Line data
SCP	Switching control point
SCPLite	SCP like functionality
SCTP	Steam Control Transport Protocol
SIP	Session Initiation Protocol
SS	Session Server

Product = MCS

A00009651 -- Meet Me Web Collaboration Multilingual Support

Functional Description

1: Applicable Solution(s)

MCS

1.1 Description

1.1.1 Background

Meet Me Web Collaboration was introduced as a Fast Feature in the MCS 3.0 release and only supported English on the collaboration web pages presented to users. This activity incorporates the FTR 424 Fast Feature into the 9.0 release and enhances it by adding multilingual support for the collaboration web pages.

1.1.2 Overview

Web Collaboration allows people in different locations to view a PC generated presentation over the IP based network. The initial release of Web Collaboration did not include support for multiple languages. It is expected to provide the same languages supported within other portions of MCS.

In prior releases, MCS users have had the ability to select language preferences both as personal preferences for their PA, and by dialing Meet Me alias numbers that are associated with a specific language. This feature extends the language choice indicated by the Meet Me alias dialed, to the Web Collaboration GUI (tool tips and dialog boxes, and user help). As a result, the audio prompts of the conference and the display on the collaboration web pages will be in the same language. It is not intended to translate the presenter's presentation.

Below is the list of languages supported in MCS 09. Meet Me Web Collaboration supports the same set of languages as the other MCS network components

1. English
2. Parisan French
3. Latin America Spanish
4. German
5. Japanese
6. Traditional Chinese
7. Simplified Chinese
8. Korean

1.2 Feature Description

1.2.1 Operator Configuration and Provisioning

This section presents Meet Me Web Collaboration configuration and provisioning information needed by operators and installers of the MCS solution.

1.2.1.1 Installation

Each Web Collaboration server must be configured with the required collaboration software. The major applications which will be installed are listed below.

- Microsoft Server 2000: Operating System (custom OS image is included on the hardware when ordered).
- Web Collaboration Application: Server side Web Collaboration software
- Provider Supplied:
  - Microsoft Office 2003: Office productivity Application suite required for collaborative document presentation (Word, PowerPoint and Excel)
  - MSDE 2000: Database required for run time collaboration data storage
  - IIS: Web Server
  - MS Internet Explorer 6.0
  - SSL 128 Certificates for HTTPS

1.2.2 Administrator Configuration and Provisioning

This section presents configuration and provisioning information needed by the system administrators for daily service and end-user support.

No new configuration or provisioning tasks are added.

1.2.3 Feature Provisioning

There are no new Meet Me Web Collaboration configuration options available to the end-user. However, all the existing Meet Me options a user has in their Personal Agent also apply to Meet Me Web Collaboration sessions. The user's language selection for their Meet Me Conference and Collaboration session is determined by the ALIAS dialed. The available Alias's are listed for a user in there PA under their Meet Me Preferences (language specific Meet Me aliases are not a new feature).

1.2.4 Feature Behavior

1.2.4.1 Overview

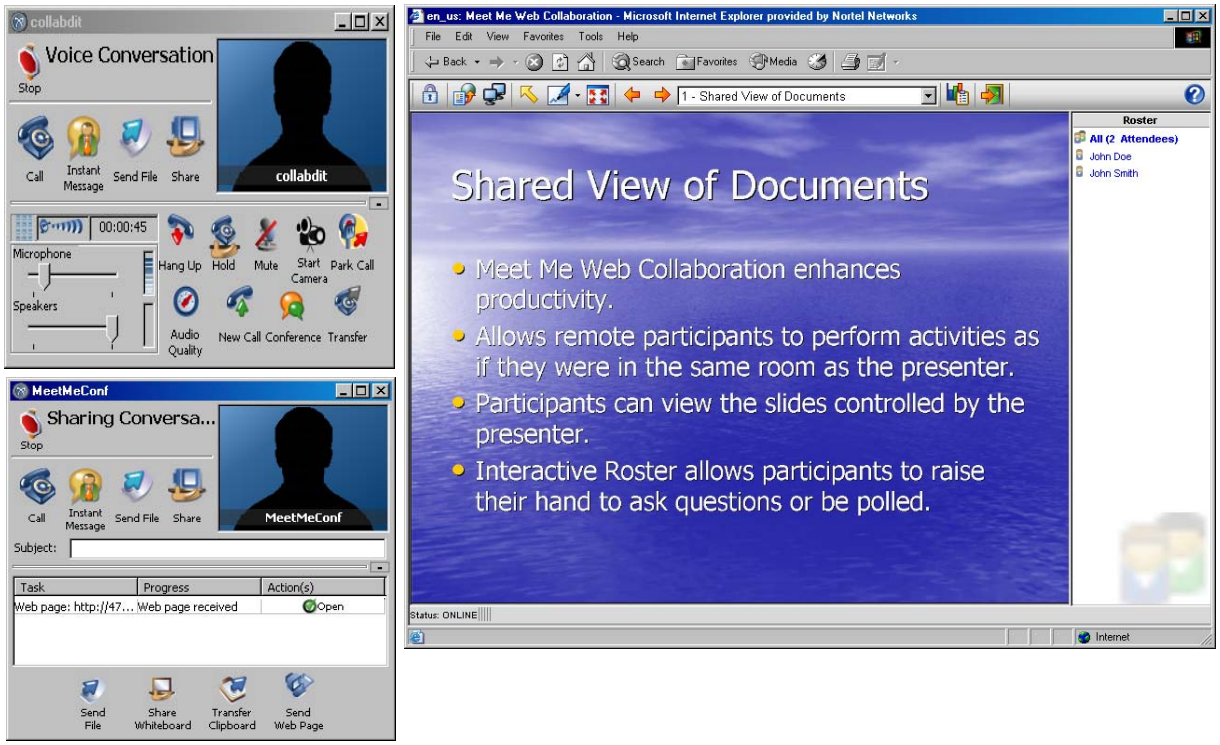
Language selection and use in the collaboration session is based upon Meet me Conference **alias a user dials**. The available aliases are listed for a user in their PA under their Meet Me Preferences (language specific Meet Me aliases are not a new feature). Prior to the Multilingual Support for Web Collaboration, only the audio prompts reflected the language indicated by a dialed alias. N**ow**

the Collaboration session will also reflect the language indicated by the dialed alias.

In addition to multilingual support, a few other enhancements are introduced. as outlined in this section.

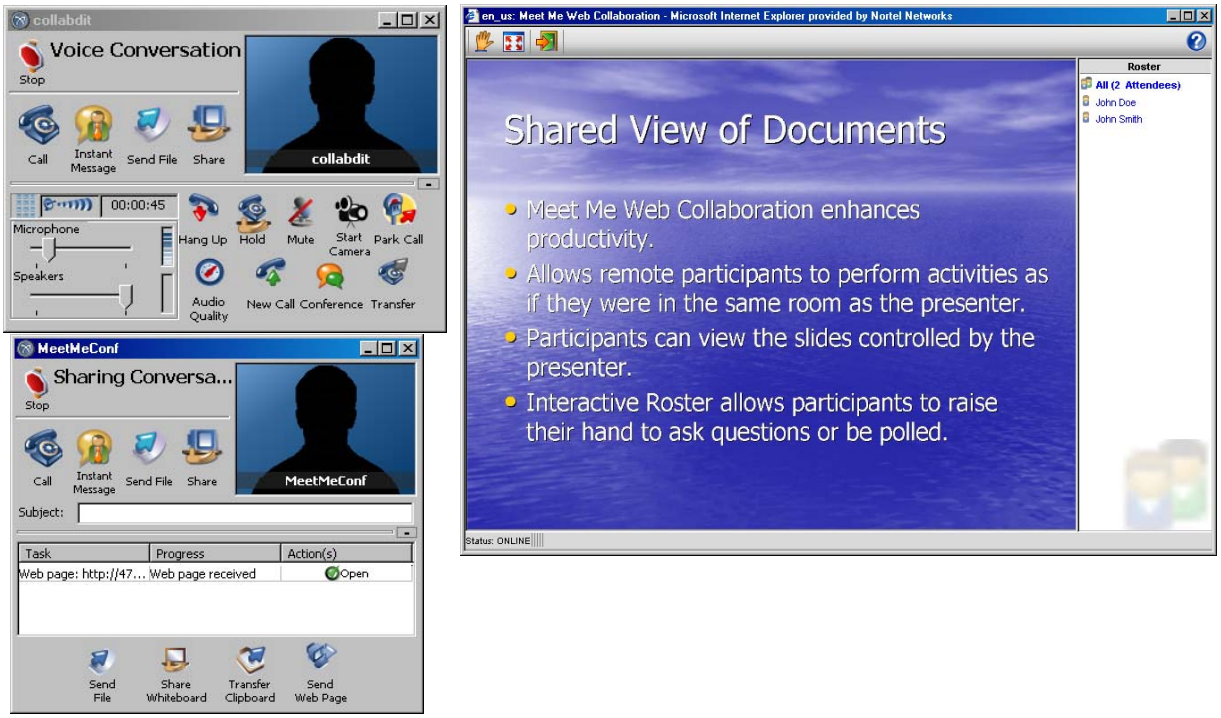
There have been some minor graphical updates to the displays as shown in the following figures.

Figure 1: Presenter's Client Call Control Window and View of Published Material



The participants now have a roster showing other participants. The main difference between the presenter and participant windows is the options available on the tool bars.

Figure 2: Participant's Client Call Control Window and View of Published Material



The publish interface has been changed and enhanced. There is a new window for publishing and the presenter (chairperson) may now login early and prepublish 1-30 documents. A presenter can then quickly jump between documents with out waiting for the uploading and conversion process of publishing. (All the documents are deleted when the Collaboration session is ended.).

To publish a document:

1 From the Presenter toolbar, click the Publish Documents icon . The "Publish Documents window is displayed.

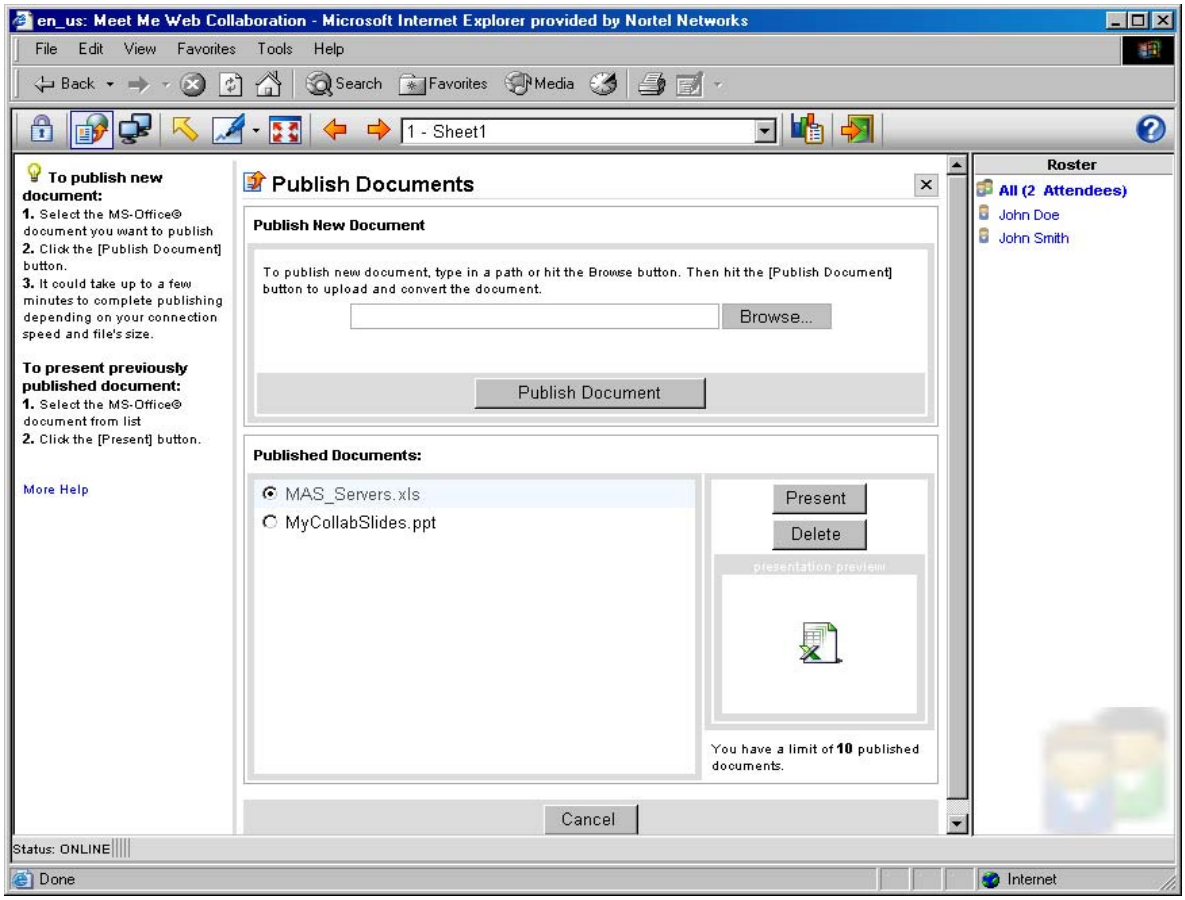
2 Click Browse, navigate to the directory containing the document to publish, and select the document.

3 Click Open.
The user is returned to the "Publish Documents" window and the full path to the document is displayed.

4 Click Publish Document.
The document is displayed in the main window. Note that uploading a document can take several minutes, depending on the speed of the network connection and the size of the document.

When the presenter is finished with one document, they may click the Publish Documents icon to return to the Publish New Document window to publish or present other documents.

Figure 3: Presenter Publishes Content



The presenter uses the above window to publish and manage published documents during a collaboration session. Office documents are published by using the Browse… button, selecting a file and then pressing the Publish Document button. Once this is done, the "Published Documents:" panel shows all the documents ready to present. A radio button allows selection of a particular document. The buttons Present and Delete perform the corresponding action on the selected document. All documents are deleted when the collaboration session ends.

The collaboration tool bars have been internationalized. The English labels under each button have been removed and replaced with hover help text which displays in the users language. The tool bar buttons also have a new graphic look and are defined below.

The Web Collaboration presenter's window has a tool bar with controls for the presentation. The following functionality is available to the presenter on the Presenter's Tool bar:

	Publish	Allows the presenter to specify the file to be published. After selecting the desired file the document is converted to a web publishable HTML format.
	Share	Allows the presenter to graphically share the view of any running program on their computer with participants.
	Point	Provides the presenter with an active mouse controlled pointer for the published document.
	Marker	Provides mouse annotation tool for the published document. All participants can see the resulting mark-ups.
	Full Screen	Toggles Full-Screen mode. When the presenter uses this button, the presenter's and all participants' collaboration screens switch to full screen mode. If the present toggle Full Screen Mode off, only his screen is normalized.
	Previous	Navigation to the previously displayed document page.
	Next	Navigation to the next document page.
	Content Selector	The Content Selector displays slide numbers and titles in a selectable drop down list providing the ability to quickly jump between slides.
	Poll	Launches a polling mechanism which allows the presenter to enter a question and multiple choice answers and get instant tabulated results.
	Exit	Ends the collaboration Session
	Help	Online user help.
	Lock	Locks the web portion of the collaboration session so that no new users may join. Does not impact the audio portion of the conference.

The Web Collaboration participant's window contains a toolbar with the following functionality:

	Raise Hand	Allows the participants to toggle “raising their hand.” The presenter’s roster shows a raised hand icon next to the participant’s name.
	Full Screen	Allows a participant to enter/exit the full screen collaboration mode (only for their own screen). Note: The presenter can force all participants to full screen, but then the participants may individually normalize their screens as desired.
	Exit	Removes participant from the collaboration session. The Meet Me Audio conference connection is unaffected.
	Help	Online user help.

1.3 Dependencies

1.3.1 Hardware Dependencies

IBM X335 or X336 eServers and the IBM Blade Center and Blade Center-T hardware may be used for the Web Collaboration Servers. Previous to this feature only the X335 eServer was supported.

1.3.2 Software Dependencies

1.3.2.1 Nortel Networks Software Dependencies

Not Applicable

1.3.2.2 Non-Nortel Networks Software Dependencies

Clients

Joining Conferences

The personal computers of people joining the collaboration session must meet the following minimum requirements to view published pages:

- 56kbps or higher connection speed is recommended
- Microsoft Windows 98/NT/ME/2000/XP/Server2003 with Internet

Explorer 5.5 or higher (preferred), Netscape 7.1 or higher.

- Cookies, Pop-Ups and Scripting Enabled in web browsers.

Application & Desktop Sharing

For application and desktop sharing, the sharing system must meet the following additional requirements:

- Microsoft Windows 98/NT/ME/2000/XP/Server2003 System with Internet Explorer 5.5 or higher
- Ability to run ActiveX sharing controls or pre-install sharing components
- 128kbps or higher connection speed is recommended
- The Microsoft or Sun JVM maybe used. A Java Virtual Machine 1.5 or higher is required to view or control shared screens (Windows NT systems should use Microsoft or Sun JVM 1.4.2_03). The latest service pack and patches should be applied to all Windows operating systems.

Servers

Table 2: External Software Dependencies

Component	External Dependency	Description
Media Application Server	Microsoft Windows Server 2000	Operating System
Collaboration Server	Microsoft Windows Server 2000	Operating System
Collaboration Server	Microsoft Office 2003 (All components except Access and Outlook)	Office productivity Application suite
Collaboration Server	Microsoft MSDE 2000	Database
Collaboration Server	Microsoft IIS	Web Server
Collaboration Server	Microsoft Internet Expoler 6.0	Web Browser

1.3.3 Network Component Dependencies

1.3.3.1 Nortel Networks Components

Interactions remain as described in FTR 424 Meet Me Web Collaboration.

1.3.3.2 Non-Nortel Networks Components

Not Applicable

1.4 Fault Management for A00009651

1.4.1 Fault Management strategy

No changes to Fault Management

1.4.2 Logs and alarms

No new logs or alarms

1.5 Performance Management for A00009651

There are no changes to the MAS based Meet Me conferencing performance management strategy. The Web Collaboration Servers, introduced by this feature, are monitored using a web based administrator tool.

1.5.1 Performance management tools and utilities

The web based administrator tool on the Web Collaboration Servers is used to monitor system behavior and health. For security the administrators must log in to the tool.

The tool presents both historical and current real-time collaboration session information. This functionality remains the same as in MCS 3.0 as described in FTR424.

1.5.2 Performance Measurements (PM), Operational Measurements (OM) and Stats

No new MCP measurements are added

1.6 Network Engineering

Not applicable

1.6.1 Network configuration

No changes are introduced to the Web Collaboration configuration

1.6.2 Hardware configuration

No changes are introduced to the MAS and the Web Collaboration server configurations.

1.6.3 Network Engineering Rules

Rules remain as described in FTR 424 Meet Me Web Collaboration.

1.6.4 Engineering Variables

Not Applicable

1.7 Upgrade

1.7.1 Upgrade from Previous Release or Current Release

Follow standard upgrade procedures for Web Collaboration. No special actions required.

When upgrading the Nortel Networks Web Collaboration Server must be uninstalled using Add/Remove Programs from the Control Panel, a reboot performed, and then the new install shield can be run.

1.7.2 Upgrade Problems and Rollbacks

The following procedure is to be followed when rolling back to 3.0 Web Collaboration Server after already installing a 9.0 Web Collaboration Server.

The procedure should also be used when any type of installation problems or problems after installatiom are encountered: It performs a complete uninstall of all the related software.

1. Via *Control Panel > Add/Remove Programs* remove *Nortel Networks Web Collaboration Server*
2. Via *Control Panel > Add/Remove Programs* remove *WebInterpoint Server*
3. From a cmd prompt, run `C:\Program Files\Nortel Networks\MAS\tools\uninstallData.bat`
4. Via *Control Panel > Add/Remove Programs* remove *Microsoft SQL Server Desktop Engine*
5. Via *Administrator Tools > Data Sources (ODBC) System DSN* tab remove "localPC" data source.
6. Via *Control Panel > Add/Remove Programs > Add Remove Windows Components* uncheck *IIS* and select *Next* to remove.
7. From a cmd prompt, run `C:\Program Files\Nortel Networks\MAS\tools\cleanFolders.bat`
8. Reboot Server

The software is now completely removed. Follow installation procedure as outlined in the Web Collaboration Service Guide.

1.8 Software Delivery Packaging

Not Applicable

1.9 Command interface changes

Not accplicable.

1.10 Security

No changes to the existing security.

1.11 Restrictions and Limitations

The language used for Meet Me Audio prompts and for the Collaboration Web pages is based on the Meet Me Alias dialed, as opposed to the language selected in the settings of a user's Personal Agent on the MCS.

Restrictions from FTR 424 that are still applicable:

- Collaboration Servers may not be clustered or pooled in this release.
- No participant summary or collaboration session logs are available to the chairperson in release MCP 9.0.

- Web pushes for the presenter are sent to the chairperson's userid. As a result, Meet Me Web Collab accounts cannot be shared by using another userid to start the conference: That user will not get the web push.
- When the Presenter deletes a user form the web collaboration session, they are not removed from the audio conference.
- PSTN Clients cannot chat.
- All web communications with participant web browsers may be encrypted using SSL (Secure Socket Layer) through the HTTPS protocol. The connection between the MAS and the Collaboration server uses HTTP.
- If a user ends a collaboration session prior to the point where the chairperson can publish a document then the session will properly end, a Pop-Up warning window may appear. This warning can be ignored.
- If a participant hangs up the collaboration web session is ended. If they re-open the web page the can rejoin the collab session with out being involved with the Meet Me conference. The Presenter will see the user re-enter on the roster.
- One default brand is provided with the system.
- There is no MCS keycoding incorporated into the Web Collaboration server in this release.
- Participants of a Meet Me Web Collaboration conference which are joined in to the conference via an Ad Hoc conference are not provided automatic web pushes. User must be direct participants of the Meet Me conference to receive web pushes.
- If a participant leaves the Meet Me Web Collaboration conference they loose their web collaboration session. Examples include consultative transfer and transfer.
- When a participant of a Meet Me call, who is also a member of a foreign domain, parks their leg, the retrieved call will not receive the web push required for web collaboration. This is a limitation between client contact information and call park. It is noted as a limitation with in the call park feature.
- Microsoft provides a password protection feature for Office documents which is not supported. If a user attempts to publish a password-protected document they will receive a failure notice. To resolve this problem, open the document using Office, save the document without a password, and then try publishing it again.
- Microsoft Excel documents containing macros or "scenarios" are not supported.

1.12 Glossary

Term	Definition
MAS	Media Application Server
MCS	Multimedia Communications Server
PA	Personal Agent

Product = MCS

A00009655 -- BladeCenter-T RTP Media Portal

Functional Description

1: Applicable Solution(s)

MCS

1.1 Background

The RTP Media Portal has been a part of the Multimedia Communications Portfolio (MCP) since its inception. The RTP Media Portal was a pooled resource that provides a variety of media-plane functions to MCP solutions including:

- Firewall and NAPT (FW/NAPT) Traversal for obscured endpoints.
- Media-Plane Firewall to protect sensitive components in the service network.
- Media Anchor/Pivot capabilities that enable media-stream manipulation without the involvement of a participating endpoint.
- Replication of media streams for CALEA.

The introductory version of the RTP Media Portal was delivered as a distributed set of subcomponents that ran on the carrier-grade Motorola CPX8216T hardware chassis. The Motorola CPX8216T chassis is a compact PCI (cPCI) architecture that provided the environmental requirements for the processing blades on which the distributed RTP Media Portal subcomponents executed. The Motorola CPX8216T chassis was partitioned into two separate PCI control domains that enabled two RTP Media Portals to reside in a single chassis. Each of these PCI control domains support the hardware components that constitute a RTP Media Portal:

- A CPV5370 Intel processor board (the Host card) with 1 GB memory, a SCSI input/output (IO) daughter board, and rear Transition Module.
- One (or more) Motorola MCPN765 Power PC processor board (the Media Blade), with 64 MB RAM and associated Rear Transition Module.
- The Hot Swap Controller and Bridge (HSC) modules.
- SCSI CD-ROM drive.
- SCSI hard drive.
- Floppy drive.

From one perspective the introductory version of the RTP Media Portal had a software architecture that closely matched the hardware architecture.

However, it was also designed to be portable so that it would be platform-agnostic and poised to benefit from the advances provided by Moore's Law.

Since its first introduction, the RTP Media Portal has fared well and proven itself to be a stable component of the MCP solution. Unfortunately, the maturation of the Voice-Over-IP (VoIP) market has begun to stress some of the first generation RTP Media Portal's limitations:

- Need for higher density (more media flows per unit of rack space).
- Need for more media bandwidth than can be provided by the dual 10/100 Mbps Ethernet links on the MCPN765 Media Blade.
- Need for improved supportability (PPC Linux).
- Need for improved reliability strategy.

The demands of the market, the benefits being reaped by other MCP components that were migrating onto the IBM BladeCenter-T platform, and the synergies that could be realized by being able to deliver all MCS components on the same platform, came together in the program to evolve the RTP Media Portal and migrate it to the IBM BladeCenter-T platform. Migration to the IBM BladeCenter-T platform provides many benefits:

- Component simplification.
- Increased capacity.
- Decreased footprint.
- Decreased cost-per-port.
- Commonality with other components (e.g. MAS, and MCS Linux Port).

1.2 Overview

The evolution to the second generation Media Portal involves the following activities:

- Migration to the IBM BladeCenter-T platform.
- Rearchitecture of the RTP Media Portal software.
- Introduction an N+1 (N-active and 1-standby) fault tolerance strategy.

1.2.1 Migration to the IBM BladeCenter-T Platform

The IBM BladeCenter-T (Type 8720 – DC Power) unit is based on proven off-the-shelf IBM Enterprise X-Architecture technologies.

The BladeCenter-T unit is a rack-mounted, high-density, high-performance blade- server system developed for NEBS telecommunications network applications and other applications requiring additional physical robustness.

The BladeCenter-T unit uses Blade Servers, switches, and other components that are common to the IBM BladeCenter product line. This common component strategy makes it ideal for applications in telecommunications networks that need high levels of computing power and access to common off-the-shelf middleware packages that are used in IT data centers.

The BladeCenter-T unit supports up to eight Blade Servers, making it ideally suited for networking environments that require a large number of high-performance servers in a small amount of space.

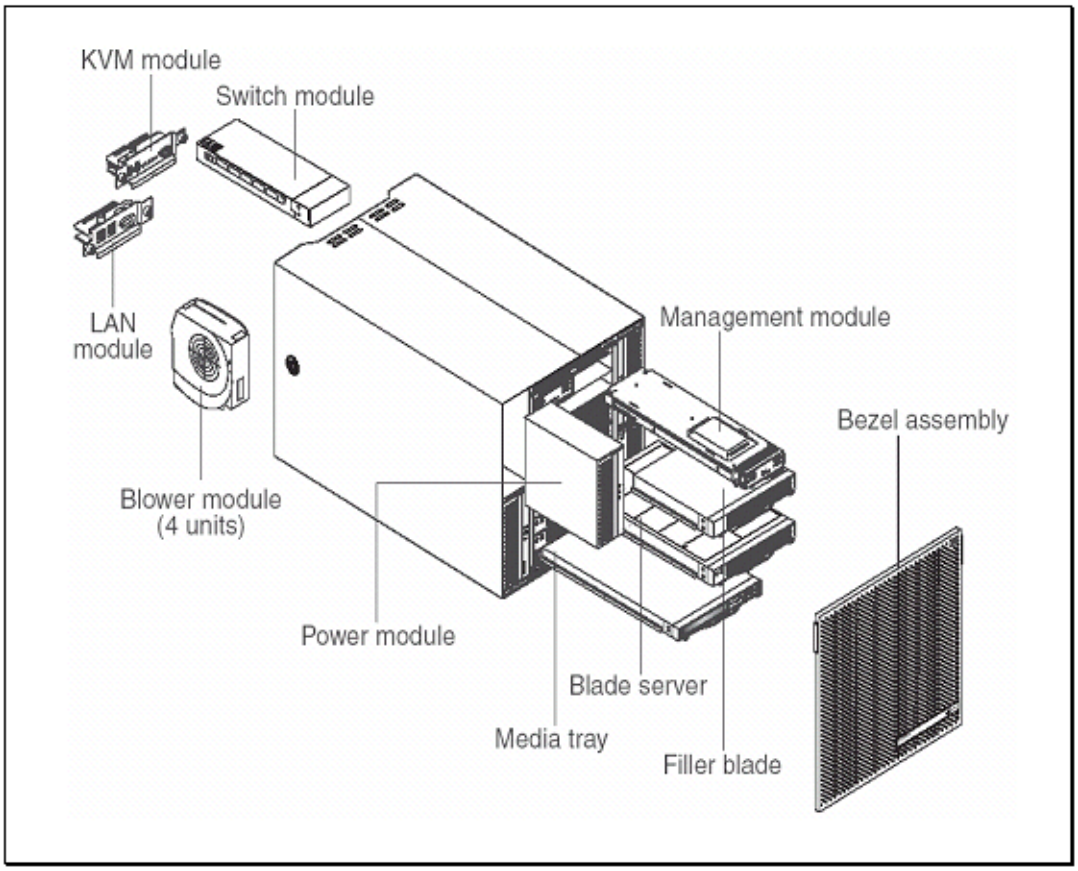
The BladeCenter-T unit provides common resources that are shared by the Blade Servers, such as power, cooling, system management, network connections, backplane, and IO (CD-ROM drive and connectors for USB, keyboard, video, mouse, and network interfaces). Refer to Figure 1 on the following page.

Performance, ease of use, reliability (NEBS/ETSI compliance), and expansion capabilities were key considerations in the design of the BladeCenter-T unit. These design features make it possible for you to customize the system hardware to meet your needs today, while providing flexible expansion capabilities for the future.

This feature activity ports the MCP RTP Media Portal component on to these Blade Servers - expanding the commonality of the IBM BladeCenter-T in MCP technology. In another move towards technology consolidation this feature also up-versions the Operating System upon which the RTP Media Portal runs to Red Hat Linux Advanced Server 3 (AS3). This is the Operating System utilized by other MCP components and its adoption by the RTP Media Portal contributes to further simplification of the overall solution.

You can obtain up-to-date information about the BladeCenter-T Type 8720 product at http://www.ibm.com/eserver/xseries/.

Figure 1: IBM BladeCenter-T Chassis (8720 – DC Version) Exploded View



1.2.2 Rearchitecture of the TRP Media Portal Software

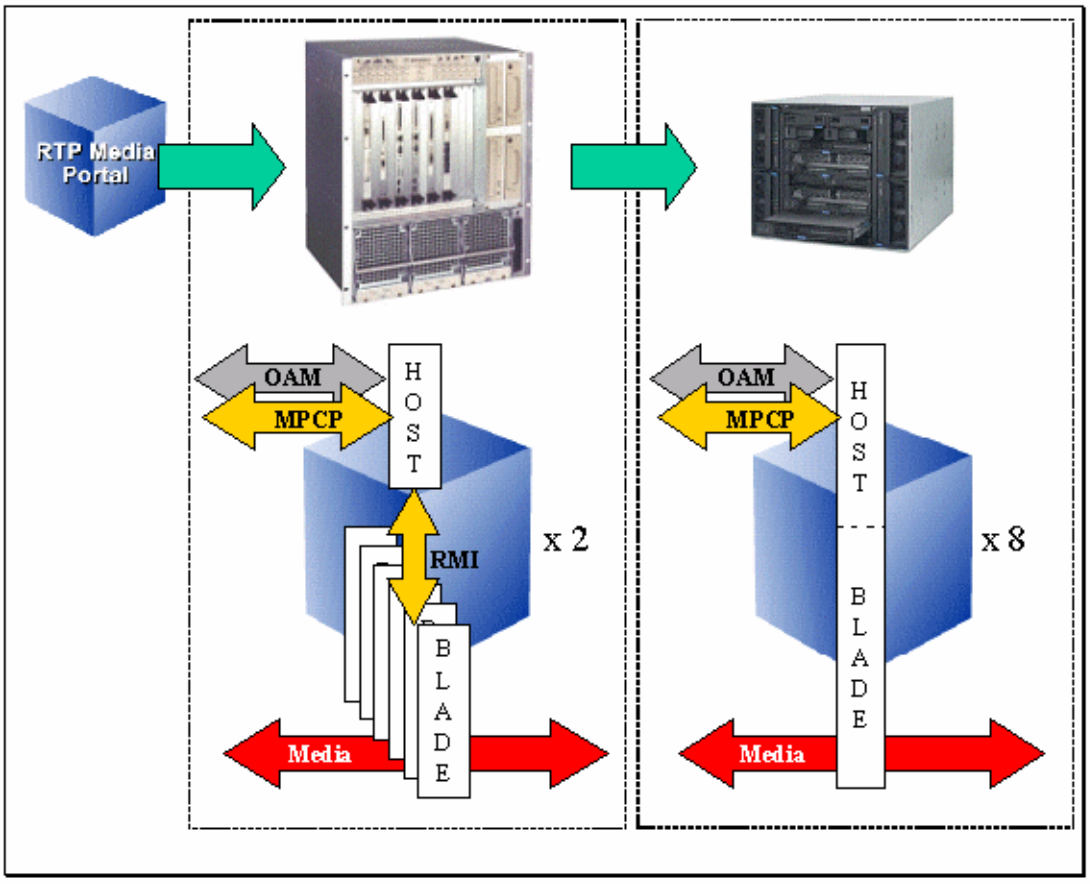
The migration from a distributed hardware architecture to a new hardware architecture that consolidates all service functionality onto a single hardware component necessitated a re-architecture of the internal software that comprises the RTP Media Portal and the services it provides.

The RTP Media Portal software was originally architected to operate in a distributed system (with a single Host communicating over the network to one or more Media Blades). This architecture has been enhanced so that the software will properly configure itself to conform with the operating environment of the target platform: it will either initialize as a distributed collection of networked sub-components (i.e. a Host communicating to one or more Media Blades), or as a consolidated amalgamation of Host and Media Blade functions into a single entity. Refer to the following figure.

The consolidation of Host and Media Blade functionality into a single entity also results in simplification through the elimination of the internal

complexities involved with coordinating service delivery amongst many distributed elements.

Figure 2: RTP Media Portal Platform Migration: Overview of Software Architectures



1.2.3 Introduction of N+1 Fault Tolerance Strategy

The original RTP Media Portal reliability strategy was to treat the RTP Media Portal as a pooled resource. Each RTP Media Portal was configured to advertise its availability to provide service to a set of Call Servers. The Call Servers would place each available RTP Media Portal into a media resource pool that would be used to serve-up available media resources during call processing.

In this manner traffic was distributed over many RTP Media Portals which lessened the impact of a failure. While lessening the impact of most failure conditions, this strategy did not preserve media sessions that existed on a piece of failed hardware. As a result, there are failure scenarios for the original RTP Media Portal that could result in loss of active calls (in the case of a Media Blade failure this could mean the loss of 400 calls, in the case of a single

chassis domain failure 2400 calls could be lost, and in the case of a full chassis failure there could be up to 4800 calls lost).

Simplification of the software architecture afforded an opportunity to take a quantum leap forward in terms of the fault tolerance attributes of the RTP Media Portal when it executes on the IBM BladeCenter-T platform. The consolidation of both Host and Media Blade functions into a single entity greatly reduced the complexity of providing the N+1 fault tolerance capabilities delivered by this feature.

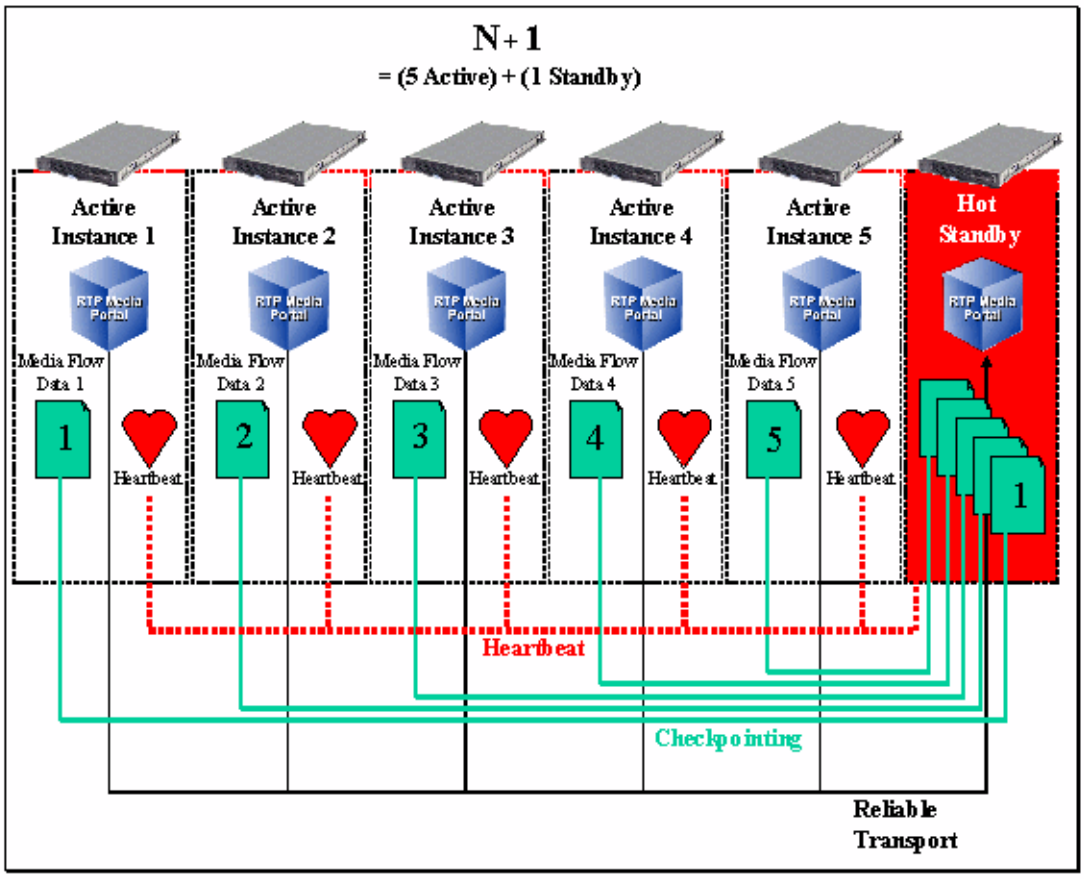
The N+1 fault tolerant RTP Media Portal is achieved through the creation of fault tolerant service clusters that define a set of RTP Media Portal instances (the “N” logical service instances) and that identifies the target servers that host the instances (“N” servers to run the active service instances and an additional server that runs a standby service instance). In this way a fault tolerant RTP Media Portal is provided that is able to have active media sessions survive the catastrophic failure of a single instance of the service by having a “standby” instance that is ready-and-able to takeover all media sessions that were hosted on the failed instance. Refer to Figure 3 on the next page.

The N+1 fault tolerant capabilities of the RTP Media Portal are built upon a reliable messaging framework that ensures connectivity between cluster members. The operating context of the cluster members is established through an election protocol that runs over the reliable messaging framework to dynamically determine which servers will be running active instances of the RTP Media Portal – and which server will be running the standby instance. This operating context is maintained through use of a heartbeat mechanism that continuously validates the state of members in the cluster. Once the cluster is formed, all state data for each active media stream (on each active instance of the RTP Media Portal in the cluster) is checkpointed to the standby RTP Media Portal instance. In this way, the standby instance remains synchronized with all active instances and is thereby ready to takeover processing of the sessions for any of those instances should a failure occur.

The N+1 takeover process is transparent to the endpoints that are originating and terminating the media streams relayed through the failed instance. This is because the standby instance begins receiving and relaying those same media streams as soon as the failure is detected and takeover is affected.

Initially, N+1 fault tolerance capabilities are restricted to the confines of a single IBM BladeCenter-T chassis. This enables configuration of fault tolerant clusters as small as 1+1 (“1-active-instance” + “1-standby-instance”) and up to as large as 7+1 (“7-active-instances” + “1-standby-instance”).

Figure 3: RTP Media Portal N+1 Fault Tolerant Service Cluster (example 5 active +1 standby configuration)

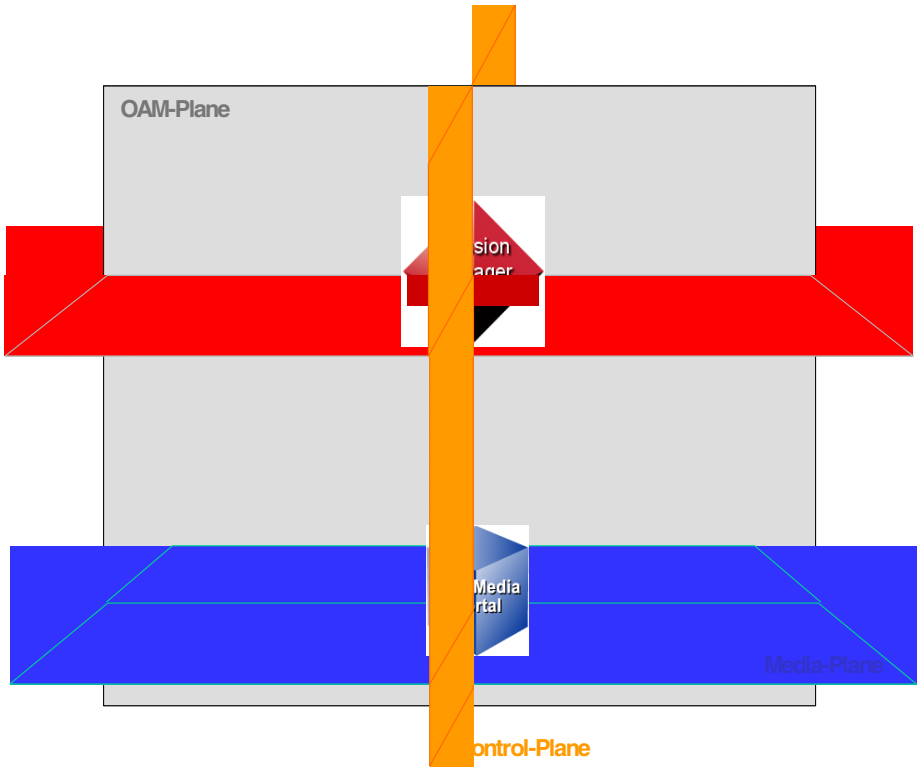


2: Functional Description

2.1 Overview

The RTP Media Portal has always existed in the Control-plane, the Management-plane, and the Media Plane. Refer to the following figure.

Figure 4 Legacy RTP Media Portal Presence in Service-planes

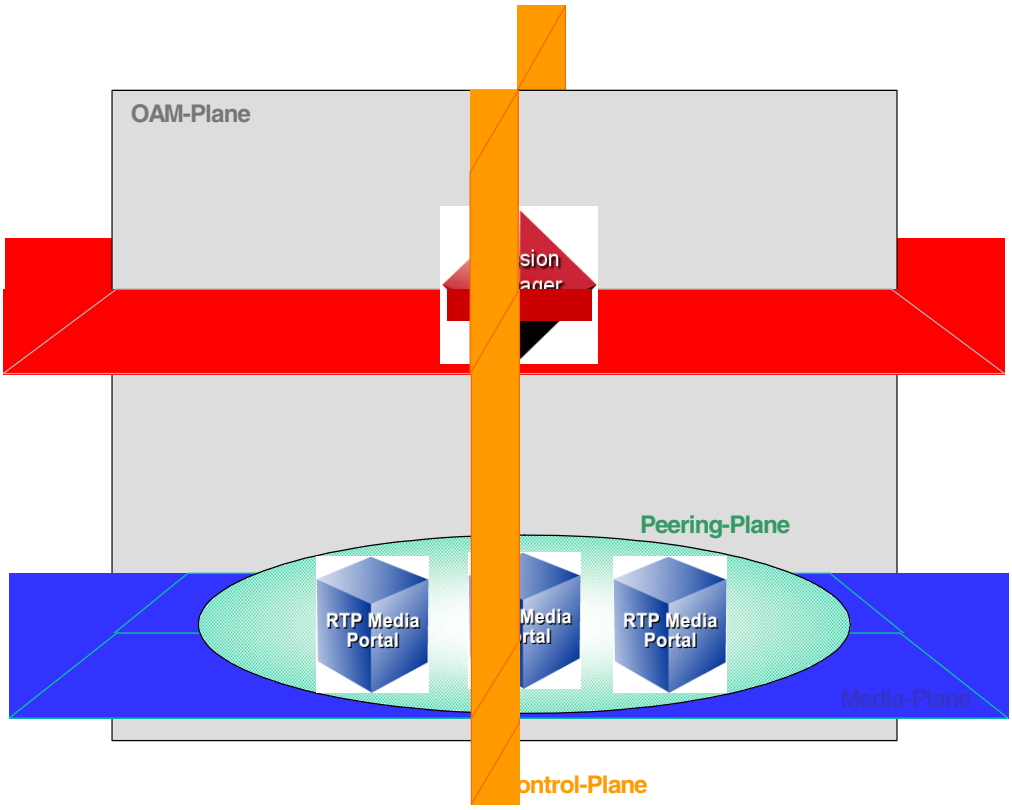


The BladeCenter-T RTP Media Portal continues to have presence in the Control, Management, and Media service-planes thus appearing (from a macro-level) to be the same as established legacy deployments to the outside world. Refer to the figure that follows. While appearing the same to the outside world, the BladeCenter-T RTP Media Portal does introduce some change as to how it is present in each of the service-planes at a sub-atomic level (not visible to the outside world):

- The BladeCenter-T RTP Media Portal has abstracted the RTP Media Portal Service from the platform. So, in fact the BladeCenter-T RTP Media Portal consists of an RTP Media Portal Service (which resides in the Control-plane and the Media-Plane), and a separate BladeCenter-T Platform (which resides in the Management-plane). This architectural change enables the BladeCenter-T RTP Media Portal to have separate and distinct points of presence in the Control-plane (the Controlipaddr), the Management-plane (the Blade Server's physical IP address), and the Media-plane (Net1MediaIP and Net2MediaIP). Previously, the RTP Media Portal was a tight coupling of hardware and software configuration that constituted a single point (the Host IP address – which was also the Server's physical IP address) through which the RTP Media Portal participated in the service-planes.

- The introduction of N+1 Fault Tolerance with the BladeCenter-T RTP Media Portal has created a new service-plane (orthogonal to all others) to support Intra-Cluster Service Communications as part of the N+1 Fault Tolerance Framework. This new service-plane is called the Peering-plane.

Figure 5 BladeCenter-T RTP Media PortalPresence in Service-planes



By retaining presence in the service-planes, and making changes that are not visible to the outside world, the BladeCenter-T RTP Media Portal maintains compatability with legacy configurations:

- The BladeCenter-T RTP Media Portal appears identical from the perspective of the MCS Management Server as viewed in the Management-plane. This is accomplished transparently as the BladeCenter-T RTP Media Portal utilizes the pre-existing RTP Portal Network Element as its point of attachment to the Management-plane:
  - the BladeCenter-T RTP Media Portal is deployed using the RTP Portal Network Element,
  - the BladeCenter-T RTP Media Portal conveys telemetry (Logs, Alarms, and Operational Measurements) through the RTP Portal Network element,

- and the BladeCenter-T RTP Media Portal is managed (Start, Stop, Kill) through the RTP Portal Network Element.

- The BladeCenter-T RTP Media Portal appears identical from the perspective of the controlling Call Server as viewed in the Control-plane because it supports the same version of the Media Portal Control Protocol (MPCP) that is supported by legacy systems.
- The BladeCenter-T RTP Media Portal also provides the same media-layer functions as provided in legacy systems and so appears identical in terms of Media-plane capabilities.

Note: There is a new RTCP CNAME screening capability introduced into the Media-plane as part of this feature activity. This new capability was implemented as part of the Media Packet Engine – and so is common to both legacy and BladeCenter-T RTP Media Portals. Thus compatability, and equivalence is maintained across platforms.

2.2 BladeCenter-T RTP Media Portal Service Instantiation

2.2.1 Overview

The following activities must be performed in order to deploy the RTP Media Portal to actively provide service in the network:

1. Installation and Commissioning of the base hardware (IBM BladeCenter-T) and software (Red Hat Advanced Server 3) platforms. This ensures proper cabling, network connectivity, and IP address assignments. Refer to “The BladeCenter-T RTP Media Portal Installation and Commissioning Guide”[1] for detailed information on the installation and commissioning procedure.
2. Configuration of the Service. (Refer to the "Configuration” section of this feature.)
3. Deploy the Service software to distribute the service logic to each of the Blade Servers participating in the Service Cluster.
4. (Finally) The Service Instance must be started (the START command must be issued from the Management Console) in order for instatiation to occur and service to be provided.

The Deploy and Start activities are described in more detail in the following sections.

Note: Deploy and Start are very similar for Stand-Alone and Service Cluster configurations, but each will be described separately for completeness.

2.2.2 Stand-Alone RTP Media Portal Instance

2.2.2.1 Stand-Alone Instantiation

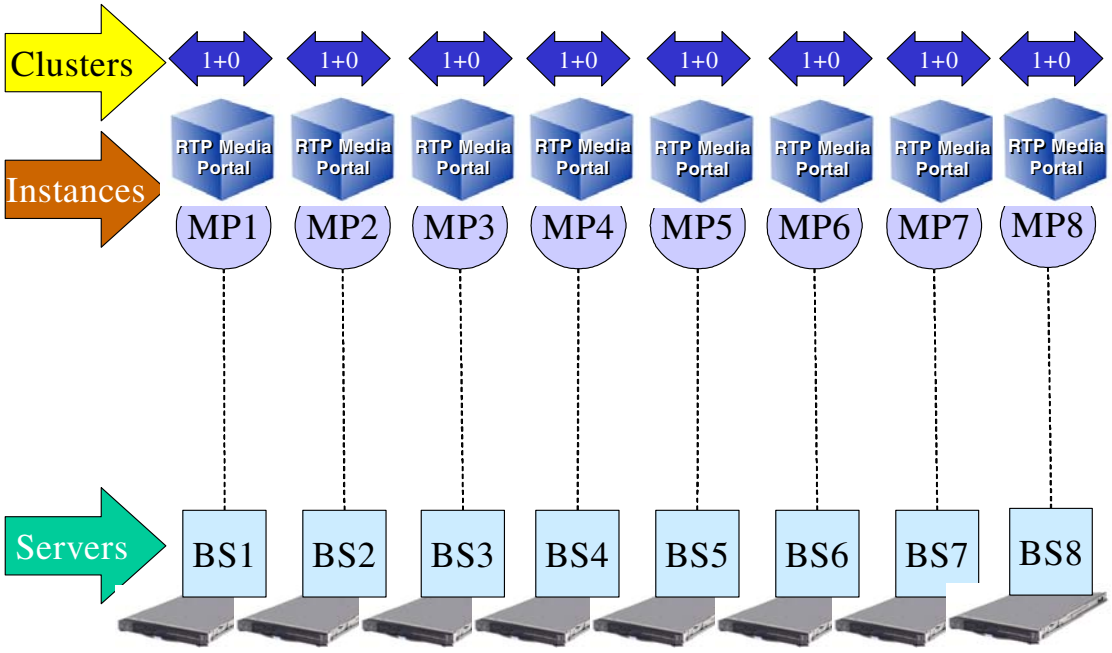
This section describes the deployment of Service software and the start-up of the RTP Media Portal service for a Stand-Alone RTP Media Portal Service Instance. The deployment phase places the Service software on the target Blade Server, and the start phase causes the instantiation of run-time structures so that the Stand-Alone RTP Media Portal Service Instance can become active and begin providing service.

The Stand-Alone RTP Media Portal Service is a single non-redundant instance of the service that runs independently of all other instances. Even though the Stand-Alone RTP Media Portal Instance is operationally different from the RTP Media Portal Service Cluster in a number of ways, it is configured as if it were a “1+0” Cluster – that is one (1) active service instance and zero (0) standby instances.

One characteristic that distinguishes a Stand-Alone RTP Media Portal Instance from an RTP Media Portal Service Cluster is that the stand-Alone Instance is only configured with one element of Service Instance Data (in Network Data => Clusters). When instantiated this effectively creates as one-to-one association of the Stand-Alone RTP Media Portal Service Instance with the target Blade Server.

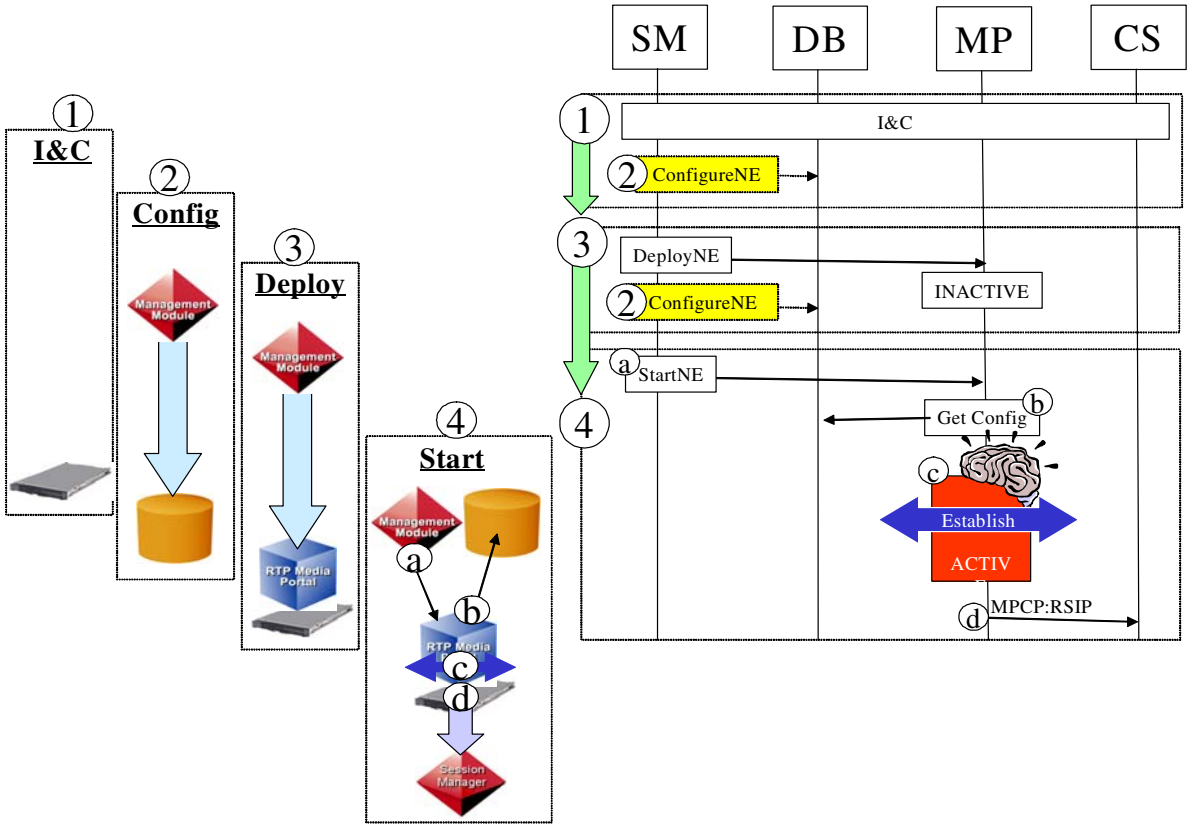
A single BladeCenter-T chassis can host up to eight (8) Stand-Alone RTP Media Portal Instances (refer to the following figure).

Figure 6 Stand-Alone RTP Media Portal Service Instances (Logical View)

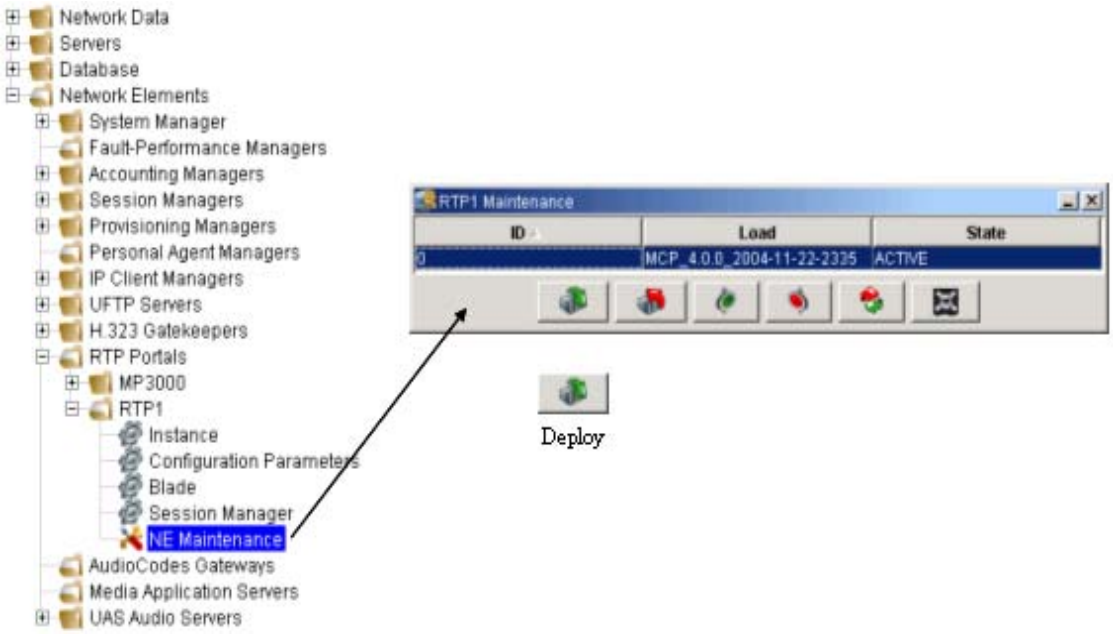


The following figure is provided as reference for the activities to be discussed that are performed in in the course of introducing a new Stand-Alone RTP Media Portal Service Instance into a site.

Figure 7 RTP Media Portal Service Deploy

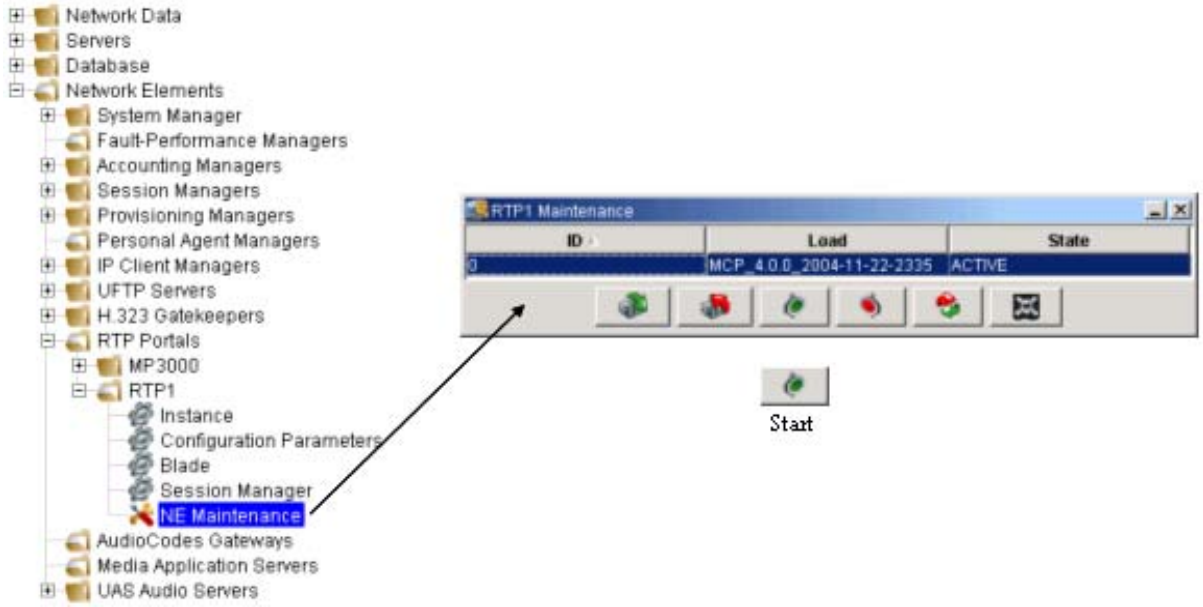


1. Installation and Commissioning of the base hardware and software platforms. Refer to “The BladeCenter-T RTP Media Portal Installation and Commissioning Guide”[1] for detailed information on the installation and commissioning procedure.
2. Configuration of the Service. The RTP Media Portal Service configuration can be changed at any time but (for the most part) is only picked up by the service on start-up. Refer to section “Service Configuration.”
3. Navigate the Management Console to the RTP Portal Network Element representing the Blade Server participating in this “1+0” Service Cluster (this will be the only RTP Portal NE that has been configured to participate in this Cluster – making it a Stand-Alone). Open the NE Maintenance window and click the Deploy button to dispatch all Service software to the Blade Server:



4. Once successfully deployed the Service Instance must be started so that instantiation of the run-time structures occurs and the service can be offered:

   a. Once again, navigate the Management Console to the RTP Portal Network Element representing the Blade Server participating in this "1+0" Service Cluster. Open the NE Maintenance window and click the Start button to start-up a RTP Media Portal Service Instance on this Blade Server:



b. As the RTP Media Portal Service Instance on the target Blade Server begins to come into service it retrieves its configuration data from the MCS Database Server. The RTP Media Portal Service Instance determines that it is configured to participate in a Cluster and then locates the specific Cluster configuration in the Network Data. Instantiation then proceeds using the Cluster Network Data to configure the service.

c. Some of the first processes started by the RTP Media Portal Service Instance are those that support the N+1 Fault Tolerant Framework (i.e. they allocate the configured multicast address and port, start the reliable messaging framework to open the intra-cluster communications channel, etc.). As the N+1 Fault Tolerant Framework Processes come up they establish the Cluster in run-time. Since this is the first RTP Media Portal Service Instance in the Cluster it is determined to be an active instance.

d. Once a RTP Media Portal Service Instance is set to active state, it issues MPCP RSIP messages to all of its configured Call Controllers (as configured in the Cluster Network Data) in order to advertise its ability to provide service. After this point the RTP Media Portal Service Instance will be called upon to service calls.

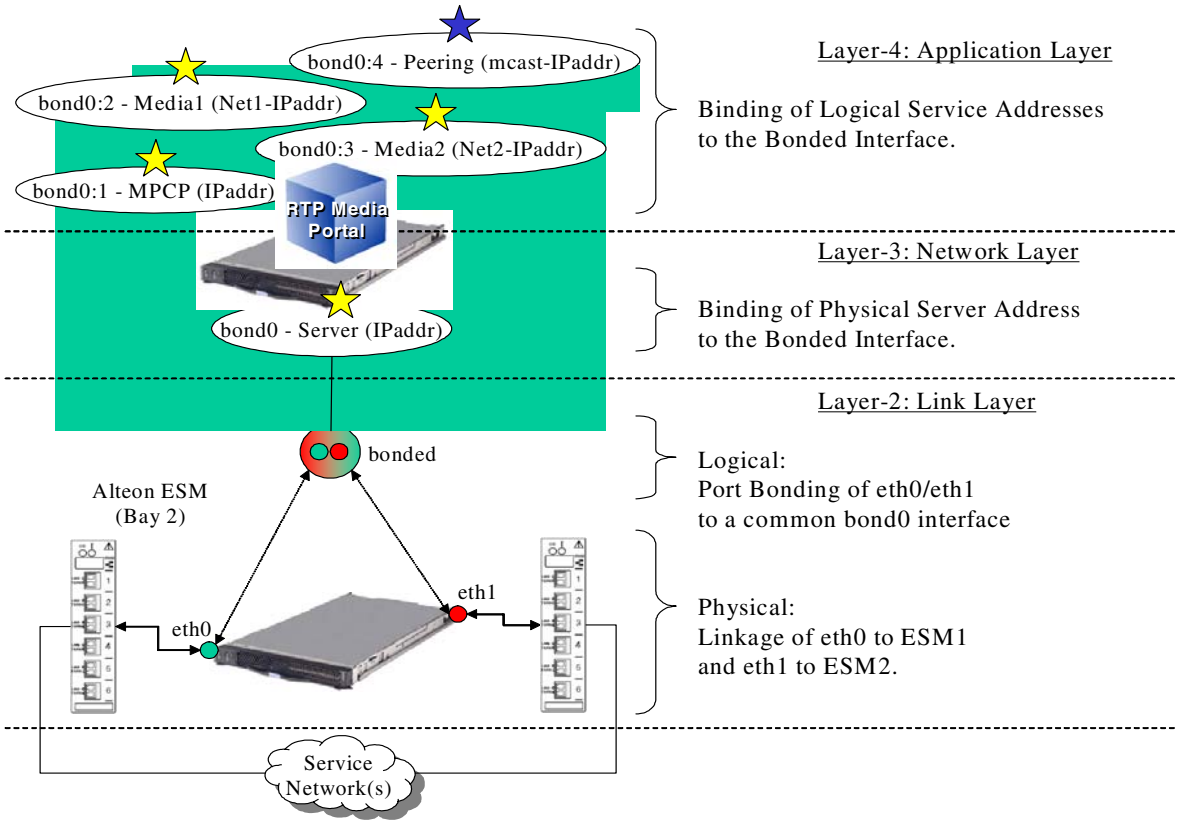
2.2.2.2 Stand-Alone Run-Time

Once instantiated the Stand-Alone RTP Media Portal Service Instance consists of the following run-time characteristics: (refer to the following figure.)

- A single physical Server IP address (bond0) that is connected to the Service Network(s) through redundant (Active/Standby Network Interface Teaming) Layer-2 connections. This physical Server IP address establishes the RTP Media Portal Service Instance's presence in the Management-plane through which the service can be managed.
- A single logical MPCP Control IP address (bond0:1) that is associated with bond0 – and so benefits from the configured Active/Standby Network Interface Teaming. This logical MPCP Control IP address represents this RTP Media Portal Service Instance in the Control-plane establishing a point from which the service can advertise its availability – and from which to process service requests.
- One, or two, logical Media IP addresses (bond0:2 and bond0:3) that are also associated with bond0 (and its redundant Layer-2 network connectivity). The Media IP addresses provide points of presence in the Media-plane to which endpoints can direct their media streams for handling by the RTP Media Portal Service Instance.
- A single logical multicast IP address (bond0:4) associated with bond0 and its inherent benefits. The multicast IP address (and port) uniquely identify a Cluster to its members. This multicast IP address represents the Cluster in the Peering-plane and is used by all Cluster members as the

communications channel through which they participate in the Cluster. In the case of a "1+0" Cluster there is only one member active on this channel and so that lone member is effectively operating in a Stand-Alone configuration.

Figure 8 RTP Media Portal Service Instance: Stand-Alone Run-Time

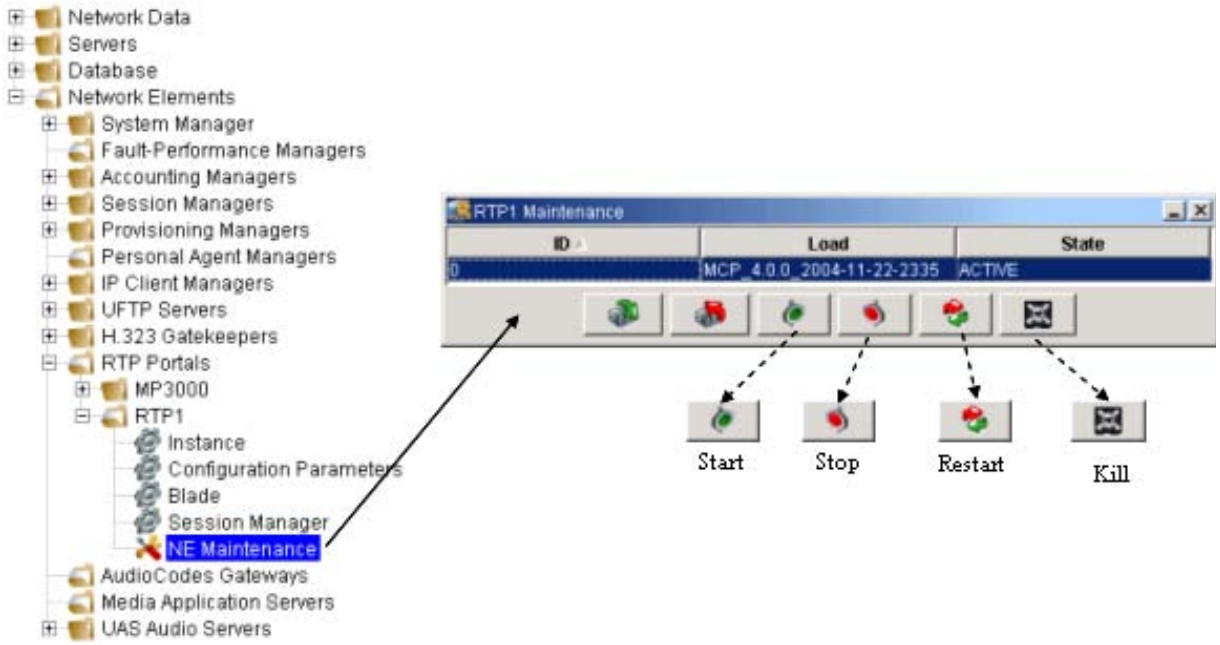


2.2.2.3 Stand-Alone RTP Media Port Management

The Stand-Alone BladeCenter-T RTP Media Portal is managed (telemetry monitoring and state changed) in exactly the same manner used to manage the stand-alone RTP Media Portal components that existed in all previous releases – that is the MCP System Management Console.

Logs, Alarms, and Operational Measurements are viewed in their respective areas of the Management Console.

Likewise, State Management (Start, Stop, Kill commands) continues to be performed through the RTP Portal NE's Instance window:



2.2.3 RTP Media Portal Service Cluster

2.2.3.1 Service Cluster Instantiation

This section describes the deployment of Service software and the start-up of the RTP Media Portal service for an RTP Media Portal Service Cluster. The deployment phase places the Service software on the target Blade Servers, and the start phase causes the instantiation of run-time structures so that the RTP Media Portal Service Cluster forms and begins to actively provide service.

The RTP Media Portal Service Cluster is an N+1 redundant collection of RTP Media Portal Service Instances. Each instance of the RTP Media Portal Service that runs in the Cluster coordinates its activities with the other member instances. Service coordination takes place over the intra-Cluster communications channel (the Reliable Messaging Framework) that is used to form (using the Election Protocol) and maintain the Cluster (using the Checkpointing functions).

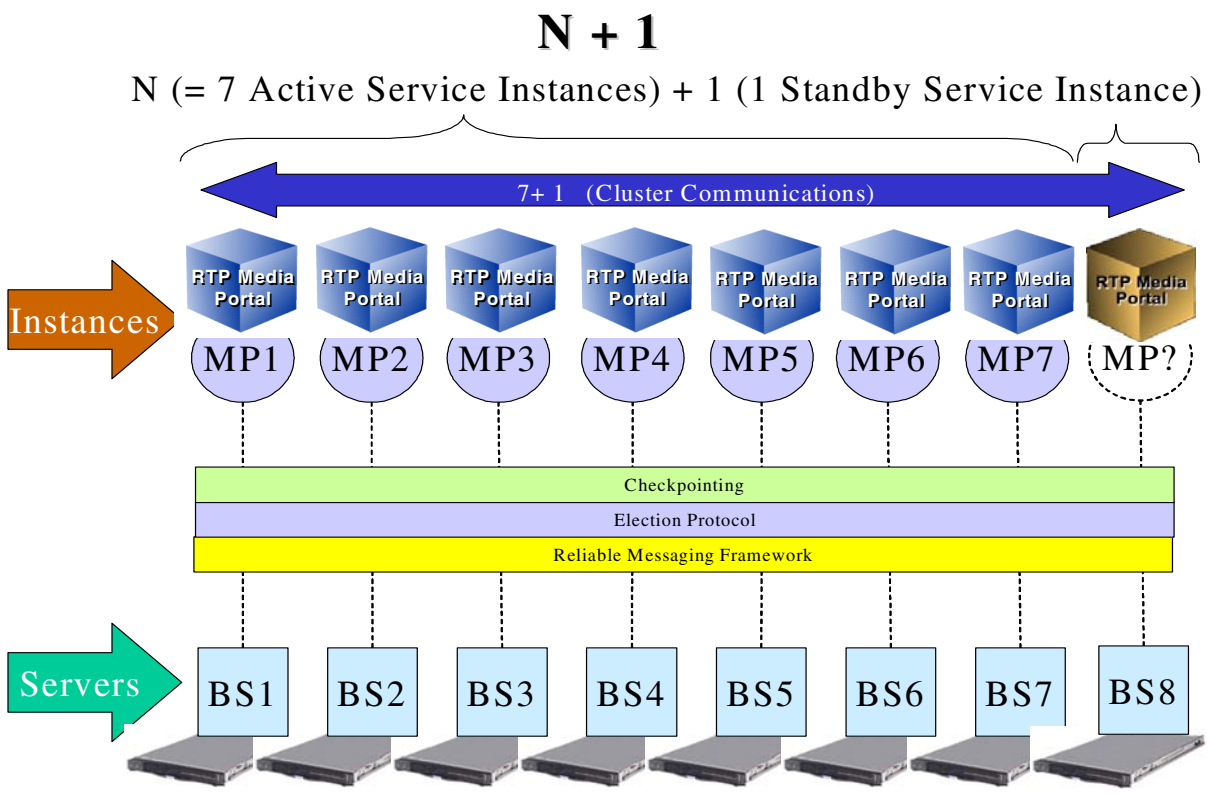
When forming an N+1 Cluster (“N” active instances and “1” standby instance), the lastinstance to join the Cluster becomes the standby instance. This ensures that that a Cluster reaches optimal operational capacity as quickly as possible before electing a standby instance.

The characteristic that distinguishes the configuration of an RTP Media Portal Service Cluster from a Stand-Alone RTP Media Portal Instance is that the Service Cluster is configured with multiple of Service Instance Data elements (in Network Data => Clusters). Once instantiated, any of the RTP Media Portal

Service Instances in the Cluster can be running on any of the Blade Servers participating in the Cluster – ther is NOT a one-to-one relationship..

A single BladeCenter-T chassis can host an RTP Media Portal Service Cluster of up to “7+1”: seven (7) active RTP Media Portal Service Instances and one (1) standby RTP Media Portal Service Instance (refer to the following figure).

Figure 9 RTP Media Portal Service Cluster (Logical View)



The following figures are provided as a reference when performing the next set of numbered steps.

Figure 10 RTP Media Portal Service Cluster Deploy (1 of 2)

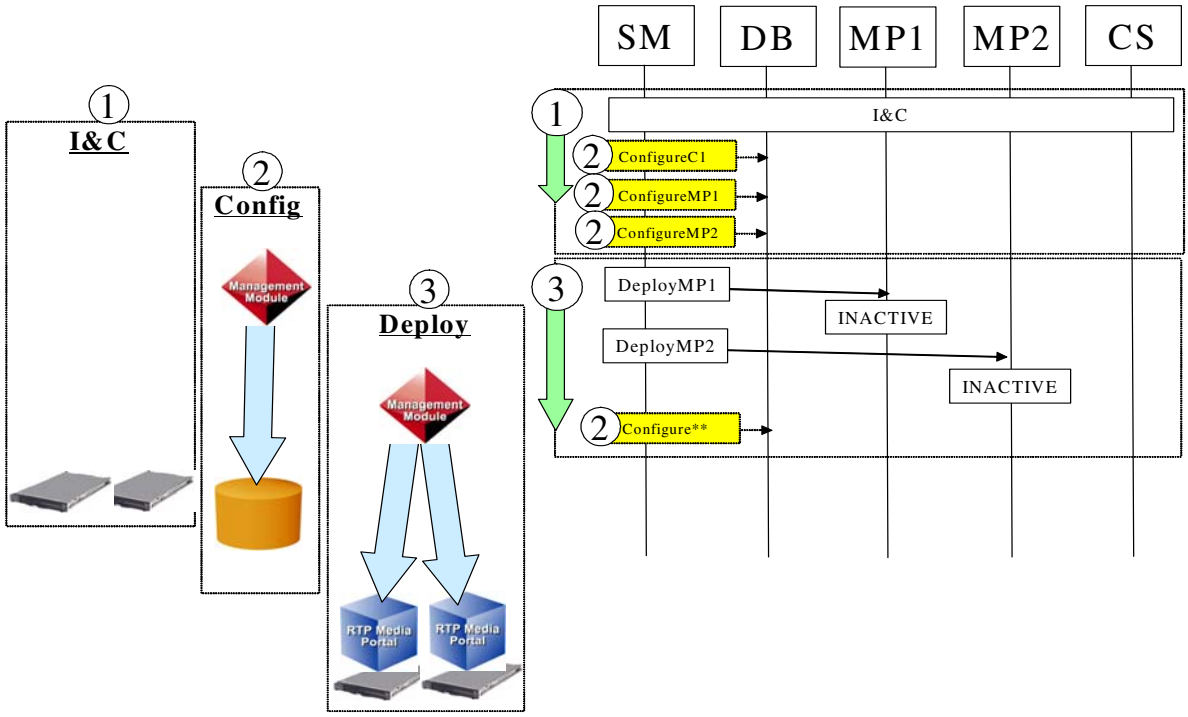
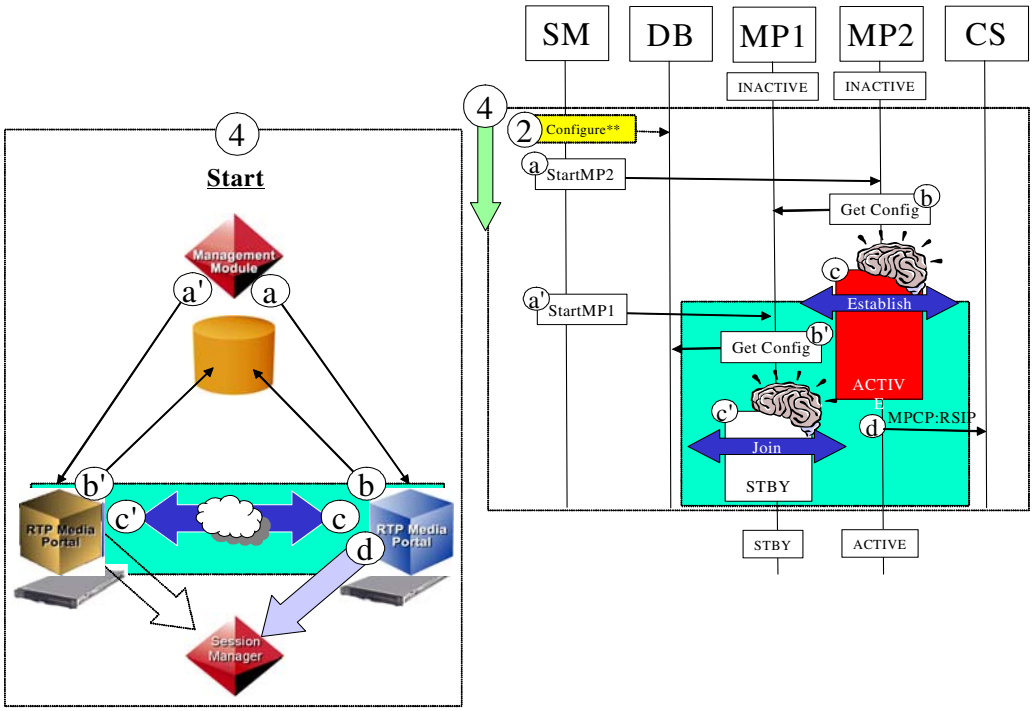
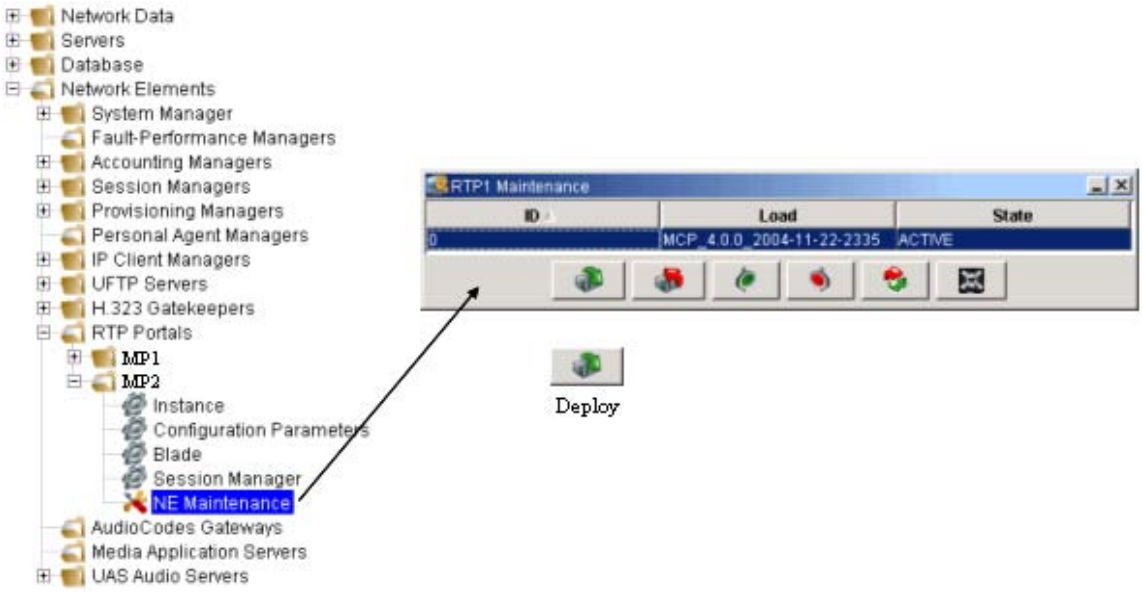


Figure 11 RTP Media Portal Service Cluster Deploy (1 of 2)

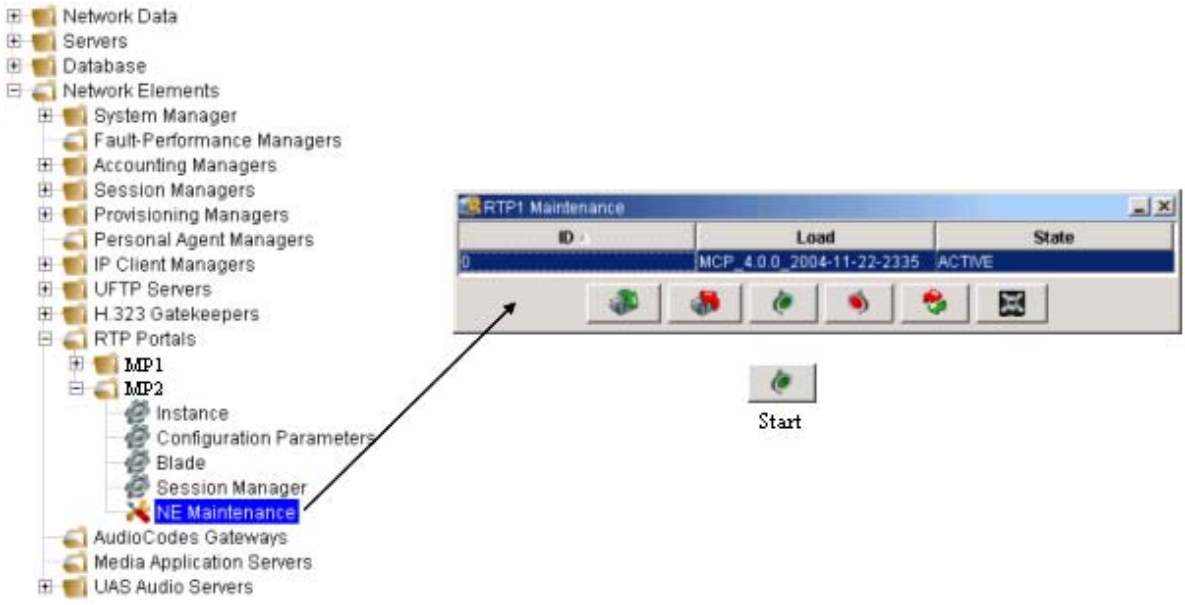


The following activities are performed in the course of introducing a new RTP Media Portal Service Cluster into a site:

1. Installation and Commissioning of the base hardware and software platforms for each of the Blade Servers intended to participate in the Cluster. Refer to “The BladeCenter-T RTP Media Portal Installation and Commissioning Guide”?[1] for detailed information on the installation and commissioning procedure.
2. Configuration of the Service. The RTP Media Portal Service configuration can be changed at any time but (for the most part) is only picked up by the service on start-up. Refer to the “Service Configuration” section of this feature.
3. Navigate the Management Console to the RTP Portal Network Elements representing each of the Blade Servers that will participate in this (“1+1”) Service Cluster. For each of these RTP Portal NEs: open the NE Maintenance window and click the Deploy button to dispatch all Service software to the associated Blade Server:



4. Once successfully deployed the member Service Instances must be started so that instantiation of the run-time structures occurs, the Cluster forms, and the service can be offered. Start-up of the individual Service Instances can occur any time after the service software is deployed to the BladeServers participating in the Cluster. This process is repeated for each of the RTP Portal NEs representing a member of the Cluster:
    a. Once again, navigate the Management Console to the RTP Portal Network Element representing a Blade Server participating in this “1+1” Service Cluster. Open the NE Maintenance window and click the Start button to start-up a RTP Media Portal Service Instance on this Blade Server:



(a' – Issuing Start command to the RTP Portal NE representing the next Cluster participant occurs in a similar fashion)

b. As the RTP Media Portal Service Instance on the target Blade Server begins to come into service it retrieves its configuration data from the MCS Database Server. The RTP Media Portal Service Instance determines that it is configured to participate in a Cluster and then locates the specific Cluster configuration in the Network Data. Instantiation then proceeds using the Cluster Network Data to configure the service.

   (b' – The next RTP Media Portal Service Instance starts-up in a similar fashion)

c. Some of the first processes started by the RTP Media Portal Service Instance are those that support the N+1 Fault Tolerant Framework (i.e. they allocate the configured multicast address and port, start the reliable messaging framework to open the intra-cluster communications channel, etc.). As the N+1 Fault Tolerant Framework Processes come up they establish the Cluster in run-time. Since this is the first RTP Media Portal Service Instance in the "1+1" Cluster it is determined by the N+1 Fault Tolerant Framework to be an active instance.

   (c' – As the second RTP Media Portal Instance starts-up and joins the Cluster, the N+1 Fault Tolerant Framework determines that, since this is configured as a "1+1" Cluster, this instance must be the Standby. The second RTP Media Portal Instance operates in Standby mode –

checkpointing all service data from the active Service Instance and monitoring its status – waiting for the opportunity to assume activity in the event that the active Service Instance encounters a fault)

d. Once a RTP Media Portal Service Instance is set to active state, it issues MPCP RSIP messages to all of its configured Call Controllers (as configured in the Cluster Network Data) in order to advertise its ability to provide service. After this point the Cluster has come into service (not yet at full capacity, but able to provide service) and this RTP Media Portal Service Instance will be called upon to service calls. In the course of processing its service requests, all active RTP Media Portal Service Instances communicate inside the Cluster to checkpoint service data and convey status so that the Cluster remains synchronized and able to survive the failure of one of its members.

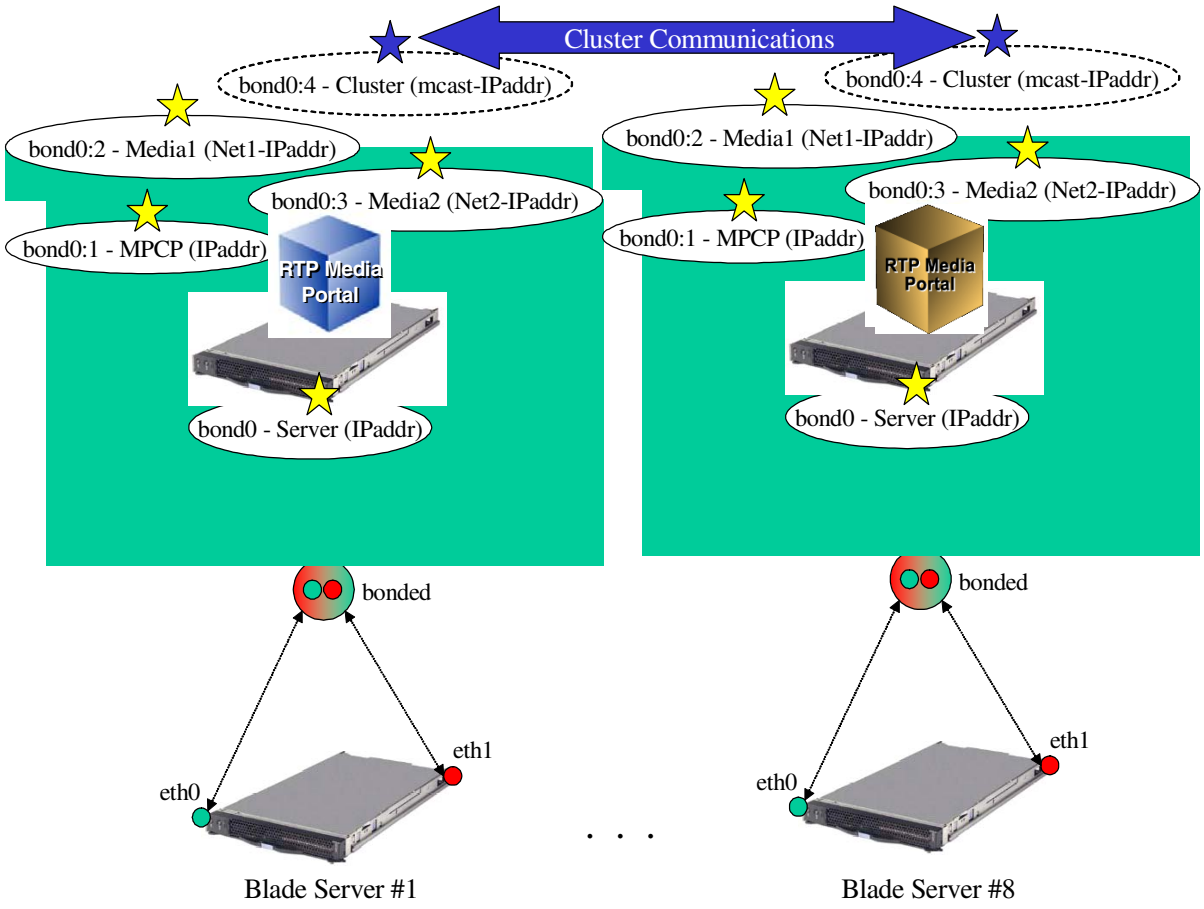
2.2.3.2 Service Cluster Run-Time

Once instantiated, an RTP Media Portal Service Cluster exists as a collection of individual RTP Media Portal Service Instances that communicate with each other (within the Cluster) to checkpoint service data and convey status information. As such the run-time characteristics of the RTP Media Portal Service Cluster is comprised of the run-time characteristics of the member Service Instances. These characteristics are very similar to the Stand-Alone RTP Media Portal Service Instance with the exception of the activity in the Peering-plane: (refer to the figure that follows).

- Each member Service Instance has a single physical Server IP address (bond0) that is connected to the Service Network(s) through redundant (Active/Standby Network Interface Teaming) Layer-2 connections. This physical Server IP address establishes this member RTP Media Portal Service Instance's presence in the Management-plane through which the service can be managed.
- Each member Service Instance has a single logical MPCP Control IP address (bond0:1) that is associated with bond0 – and so benefits from the configured Active/Standby Network Interface Teaming. This logical MPCP Control IP address represents this member RTP Media Portal Service Instance in the Control-plane establishing a point from which the service can advertise its availability – and from which to process service requests.
- Each member Service Instance has one, or two, logical Media IP addresses (bond0:2 and bond0:3) that are also associated with bond0 (and its redundant Layer-2 network connectivity). The Media IP addresses provide points of presence in the Media-plane to which endpoints can direct their media streams for handling by this member RTP Media Portal Service Instance.
- Each member Service Instance in a Service Cluster shares a logical multicast IP address (bond0:4) associated with bond0 and its inherent

benefits. The multicast IP address (and port) uniquely identifies a Cluster to its members. This multicast IP address represents the Cluster in the Peering-plane and is used by all Cluster members as the communications channel through which they participate in the Cluster. In the case of a "1+1" Cluster there is one active RTP Media Portal Service Instance on this channel and and one standby RTP Media Portal Service Instance on this channel. Generally, active Service Instances provide service and convey their service data over the Cluster communications channel to the standby Instance. The standby RTP Media Portal Service Instance checkpoints the service data received from all active Service Instances so that it can effect a transparent take-over of activity for any of the active Service Instances (should the need arise). The standby RTP Media Portal Service Instance also monitors the health of the active Service Instances so that it can take-over activity if a fault is detected on any one of the active Service Instances.

Figure 12 RTP Media Portal Service Cluster Run-Time



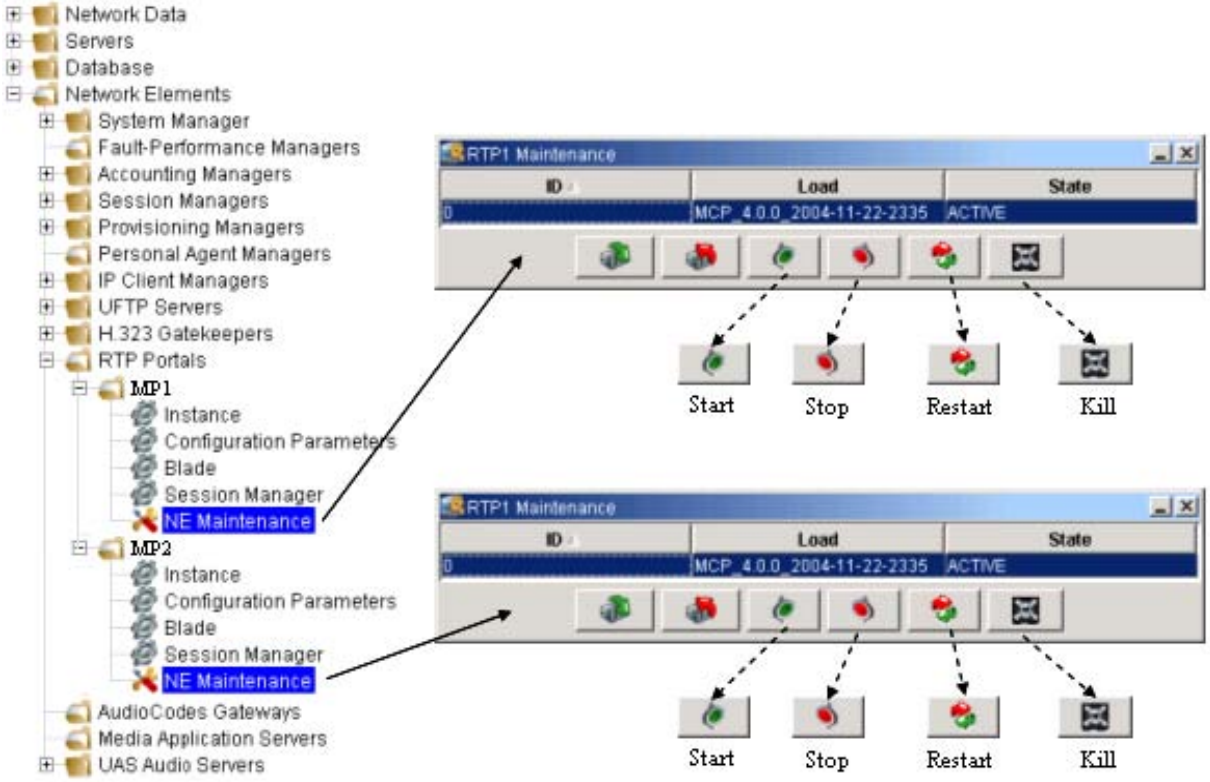
2.2.3.3 RTP Media Portal Service Cluster Management

Unfortunately, there is no capability provided to manage at the Cluster-level. As a result the BladeCenter-T RTP Media Portal Service Cluster is managed (telemetry monitoring and state changed) through administrative coordination of the management of each individual RTP portal NE.

This effectively reduces the management of the RTP Media Portal Service Cluster to the coordinated management of the collection of member RTP Portal NEs through the MCP System Management Console.

Logs, Alarms, and Operational Measurements are available for each member RTP Portal NE and are viewable in their respective areas of the Management Console.

Likewise, State Management (Start, Stop, Kill commands) must be performed in a coordinated fashion on the member RTP Portal NEs in order to achieve the desired operational result. Each member RTP Portal NE is managed using the RTP Portal NE's Instance window:



2.3 Hardware Dependencies

This feature requires IBM BladeCenter-T hardware:

- Chassis.
- DC Power Modules.
- Media Tray.
- Management Modules.
- Blower Modules.
- KVM Module.
- LAN Module.
- IO Modules.
- Blade Servers.

2.4 Software Dependencies

This feature requires Red Hat Linux Advanced Server 3 Linux Operating System.

2.4.1 Network Component Dependencies

This feature requires the collaboration of the following components:

- Management Server (and Management Console): to enable configuration and management through the MCP OAM Framework.
- Database Server: to enable persistence of configuration data and to integrate into the MCP OAM Framework.

2.4.1.1 Nortel Networks Components

Management Server (and Management Console)

The Management Server and the Management Console provide a graphical interface from which to configure and manage the BladeCenter-T RTP Media Portal. In addition to pre-existing functions, the Management Console provides access to the following new structures:

- The new Clusters are created in the Network Data.
- The new Cluster field introduced into the RTP Portal NE Instance Data.

Database Server

The Database Server provides persistent storage and centralized distribution for the newly introduced configuration information related to the BladeCenter-T RTP media Portal:

- Clusters Table (new table)
- RTP Portal Network Entity Table (new Cluster field)

2.4.1.2 Non Nortel Networks Components

Not Applicable.

2.5 Accounting

Pre-existing MCS functionality captured the following information in the accounting stream to identify which RTP Media Portal resources were selected to facilitate a call:

- mediaPortalHost: the RTP Media Portal Host IP address used to facilitate the media path of the call
- origMPConnAddr: The RTP Media Portal Media Blade IP address that replaced the Originator's media connection IP address in the SDP.
- origMPPort: RTP Media Portal Media Blade Port that replaces the Originator's media connection Port in the SDP.
- termMPConnAddr: RTP Media Portal Media Blade connection IP address that replaces the Terminator's media connection IP address in the SDP.
- termMPPort: RTP Media Portal Media Blade Port that replaces the Terminator's media connection Port in the SDP.

This information is still conveyed in the accounting stream but, as a result of this feature, some of the relationships previously implied by this information may no longer exist. Specifically, in previous releases this data not only identified service information – it also uniquely identified a piece of hardware. With the introduction of the RTP Media Portal Service Cluster the service information has been abstracted from the hardware information (a set of Service Instances can be executing on any of the hardware platforms participating in the Cluster at any given point in time) and so there is no longer a precise correlation between service information and hardware information.

3: Fault Management for A00009655

All pre-existing RTP Media Portal fault reporting is unaffected by this feature. However; the BladeCenter-T RTP Media Portal does introduce some new in-band fault reports (within the MCP OAM Framework) as well as out-of-band fault reports (in SYSLOG).

3.1 Fault Management strategy

Fault Management for the BladeCenter-T RTP Media Portal is primarily accomplished through the MCP OAM Framework through which logs, alarms, statistics, and control events flow.

Additional Fault Mangement facilities exist for managing the BladeCenter-T hardware including:

- BladeCenter-T Management Module administrative functions.
- Blade Server administrative functions.

- Alteon ESM administrative functions.

4: Configuration for A00009655

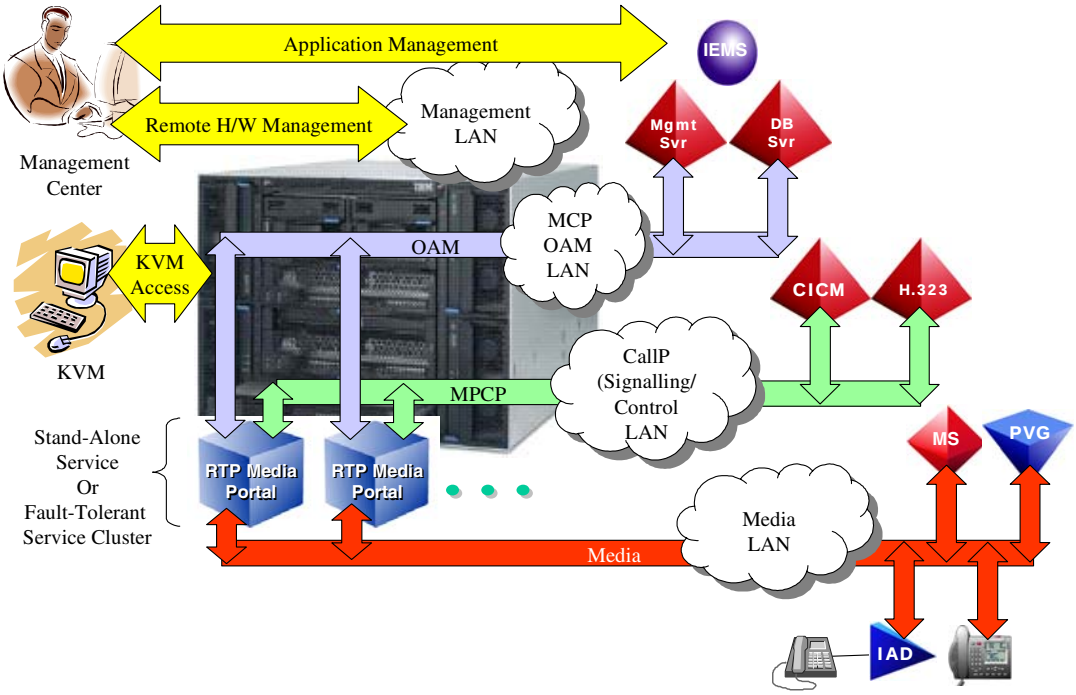
4.1 Overview

The introduction of the BladeCenter-T RTP Media Portal introduces: new hardware components, a new software architecture with new capabilities (Fault Tolerant Service Clusters), and new network connectivity configurables that enable management of the platform and execution of the service (refer to the following figure).

As a result the new BladeCenter-T RTP Media Portal introduces configuration requirements in the following areas:

- Hardware Configuration: (beyond the scope of this document.)
- Network Configuration: describes the network connectivity – this is used to define connectivity of the BladeCenter-T RTP Media Portal into the broader solution (and connections into Service Provider network[s]). The BladeCenter-T RTP MP can connect to a myriad of networks that provide: management access to the hardware components, OAM access to the product, control channel service capabilities, and access to the media streams upon which the service operates. Configuring the BladeCenter-T RTP Media Portal for connection in to a network is executed as part of the initial installation and commissioning procedures – and as part of maintenance/repair activities – that are described in detail in the appropriate methods and procedures.
- Service Configuration: describes the configuration of the stand-alone RTP Media Portal service instance, and the N+1 Fault Tolerant RTP Media Portal service cluster. Service configuration is established and can be easily modified as required to adapt to usage patterns, meet new needs, etc.

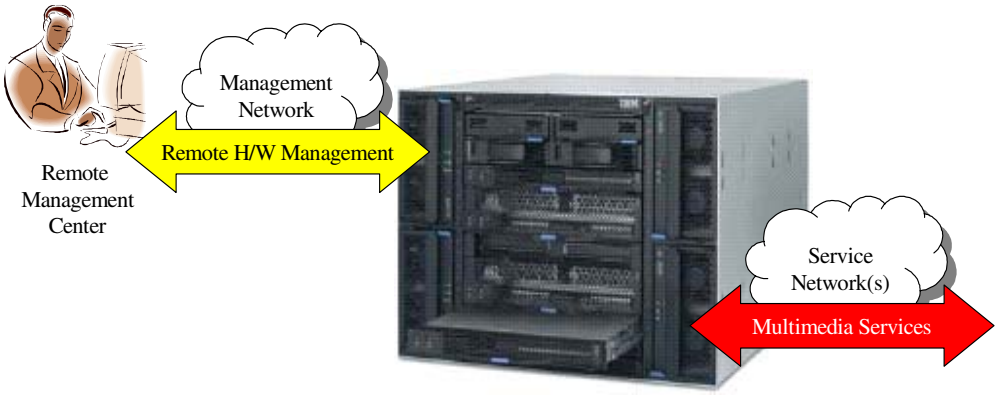
Figure 13 BladeCenter-T RTP Media Portal Configuration Overview



4.2 Network Configuration

The BladeCenter-T RTP Media Portal network configuration is partitioned between two network-spaces: one for management operations (a Management Network), and one for service execution (one or more Service Networks). Refer to the following figure. Certain subcomponents of the BladeCenter-T RTP Media Portal reside in the dedicated Management Network and others reside in the Service Network(s). Subcomponents with presence in the Management Network enable administrative access to the BladeCenter-T platform. Those subcomponents that reside in the Service Network(s) participate in the following aspects of the RTP Media Portal service: Operations/Administration/Maintenance (OAM), service control (MPCP), and execution of media processing functions.

Figure 14 BladeCenter-T RTP Media Portal Network Spaces



The Management Module and the Ethernet Switch Module are configured with IP addresses to provide them presence in the Management Network. The Management Network provides remote administrative and maintenance access to the BladeCenter-T platform.

The Blade Servers are configured with presence (an IP address) in the Service Network(s). The RTP Media Portal service instance that resides on the Blade Servers is also configured with presence in the Service Network(s). This positions both the BladeCenter-T platform and the RTP Media Portal in the service-space – where they can execute the RTP Media Portal service.

This distribution of subcomponents across different network-spaces enables the BladeCenter-T Management Modules reside on a secure management subnet, while the Blade Servers reside on a generally accessible service network in which they can participate in multimedia service delivery. That is, the management functions of the BladeCenter-T chassis are not accessible from outside the Management Network.

The following assumptions apply to the recommended network configuration of this product:

- •The BladeCenter-T Management Module (MM) and Alteon Ethernet Switch Modules (ESMs) must reside on the same subnet. The actual IP addresses and subnet mask are subnet-specific and are outside the scope of this document.
- •The Blade Servers and RTP Media Portal service instances reside on a different subnet from the BladeCenter-T Management Modules. The actual IP addresses and subnet mask for the Blade Servers are subnet-specific and are outside the scope of this document.

- Prior to network configuration of the BladeCenter-T, a sufficient number of IP addresses must be available. The IP address requirements for the various BladeCenter-T subcomponents are listed below):

  Total IPaddrs =

  [(2xIPaddr)] {for Management Module internal/external ports}

  + [(1xIPaddr) x (Number_of_ESM)]

  + (1xIPaddr) {Multicast IPaddr for Fault Tolerant Service Cluster}

  + [(4xIPaddr) x (Number_of_Blade Servers)]

Table 5: BladeCenter-T RTP Media Portal: Overall IP Address Requirements

Network	Subcomponent	IPaddr Requirements	IPaddr Count
Management Network	Management Module (only one set required)	1xIPaddr (external)	3-4
		1xIPaddr (internal)	
	Ethernet Switch Module 1	1xIPaddr (internal)	
	Ethernet Switch Module 2	1xIPaddr (internal)	
Service Network (per Blade Server)	Blade Server (OAM)	1xIPaddr (external)	4-33
(per Service Instance)	MPCP (Control)	1xIPaddr (external)	
	Media1 (Net1)	1xIPaddr (external)	
	Media2 (Net2)	1xIPaddr (external)	
(per Service Cluster)	Fault Tolerant Service Cluster (for Service Clusters only)	1xIPaddr (multicast)	
		Total	**Up to 37 IPaddrs**

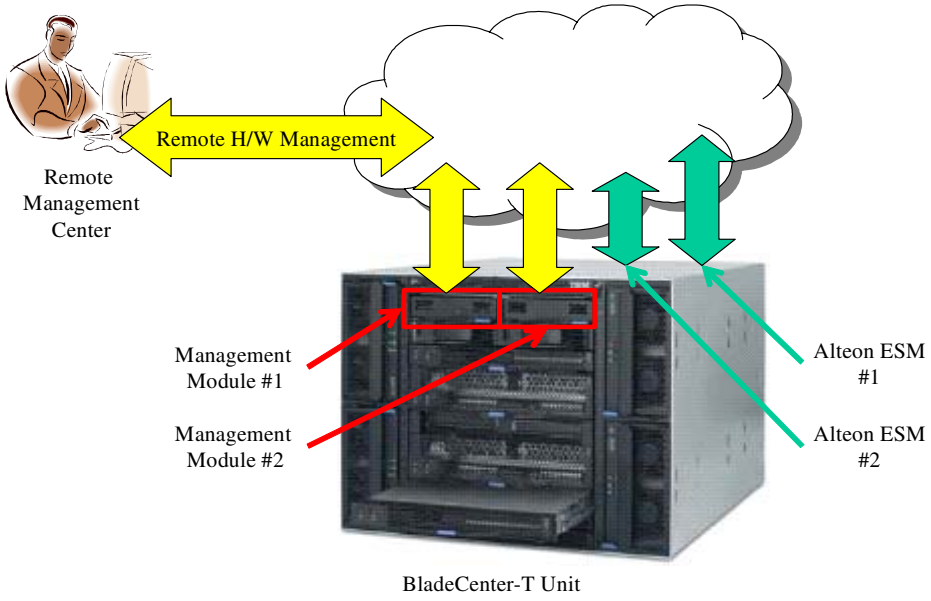
4.2.1 Management Network

4.2.1.1 Overview

The BladeCenter-T RTP Media Portal requires IP Addresses in the Managed Network. In order to provide ubiquitous remote management capabilities, the remote management client IP addresses, the Management Module IP

addresses, and the Alteon ESM management IP addresses all reside in the same subnet. Refer to the following figure.

Figure 15 BladeCenter-T RTP Media Portal: Management Network Overview



The physical relationship of these IP address assignments to the Management Module and the Alteon ESM are represented in the following figure. The actual network topology created by these IP Address assignments is described in the subsequent figure.

Figure 16 Management Network Connections: Physical View (Layer-2 and Layer-3)

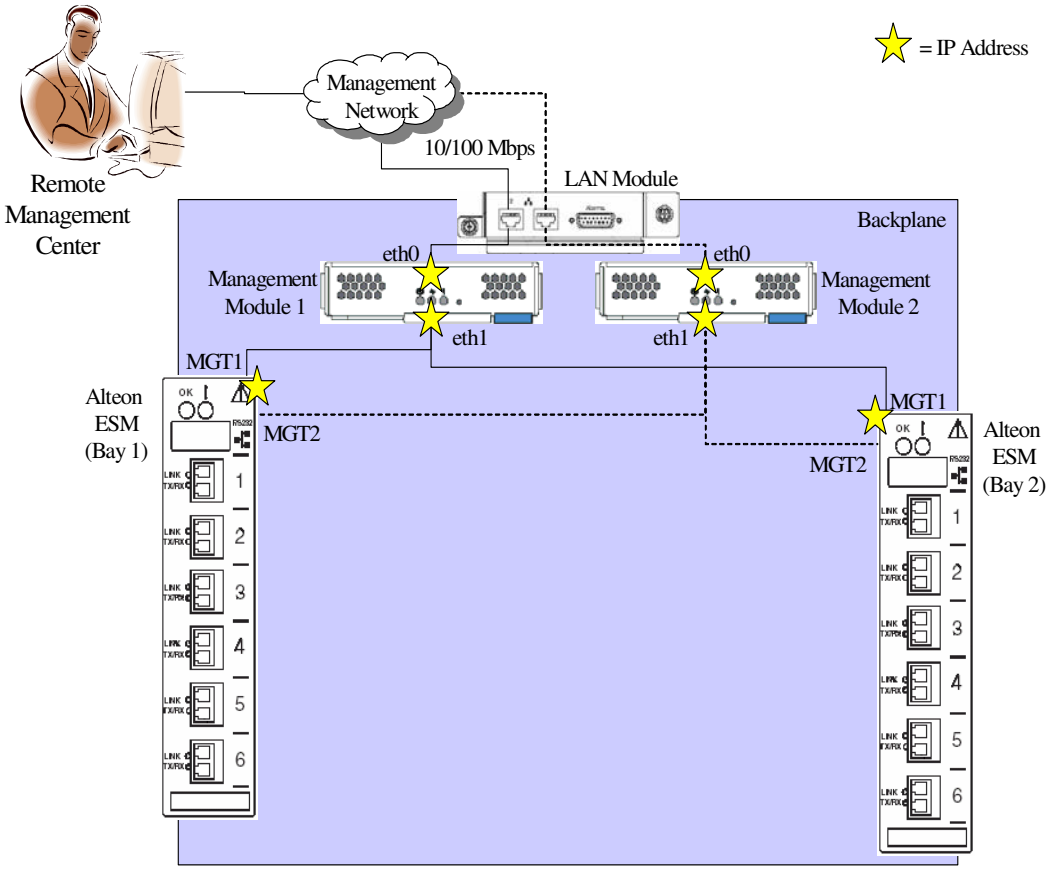
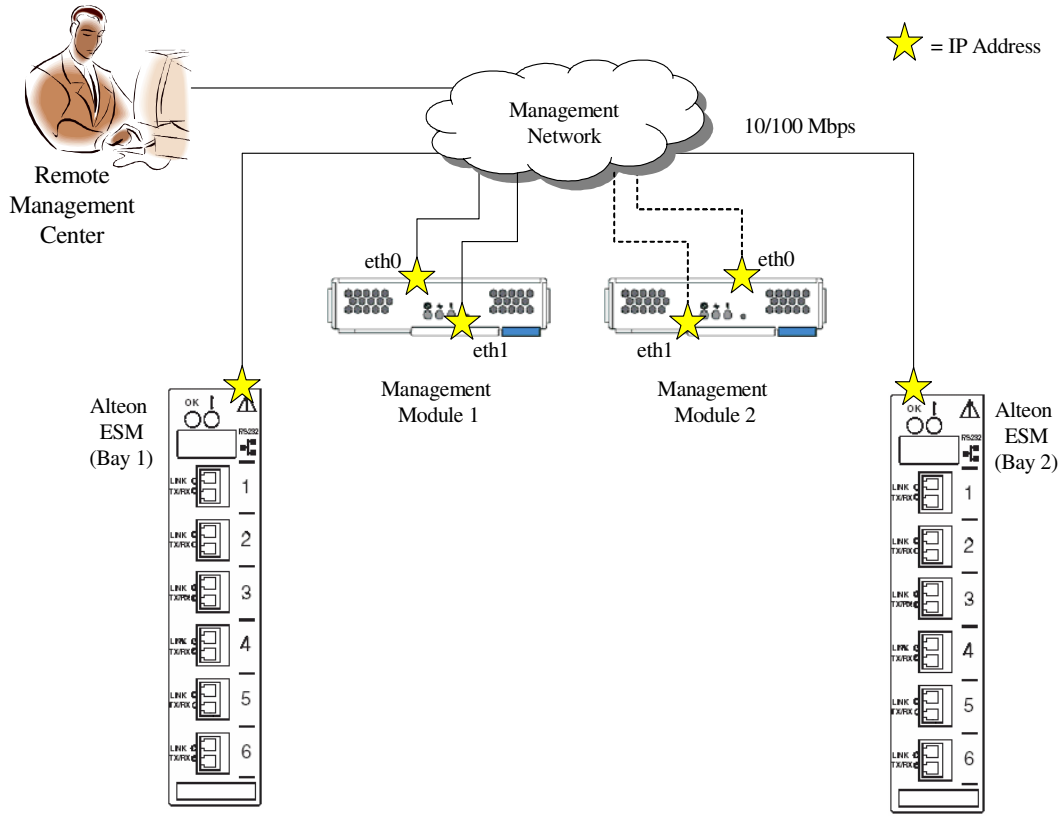


Figure 17 Management Network Connections: Logical View (Layer-3)



4.2.1.2 Configuration of the BCT Management Module

The Management Module provides access to the maintenance and control functions of the IBM BladeCenter-T chassis and its sub-components. Access to these functions is facilitated over the Management Network which connects the remote management center to the Management Modules (via Ethernet connections to the LAN Module which then connect over the back-plane to the Management Modules external interface – eth0).

The LAN Module bridges the external physical Ethernet connection to the Management Network over the backplane to the Management Module (eth0). It is through this path that the Management Module (through eth0), the Alteon Ethernet Switch Modules (accessed through relay between Management Module eth0 and eth1), and other chassis subcomponents can be reached for administrative activities.

There are two new IP Addresses required on the Management Network in order to configure the Management Modules for a given BladeCenter-T (the Management Modules run active/standby so the same settings are shared). These new Management Network IP Addresses overwrite the default factory

settings for each of the Management Modules interfaces (refer to the following table).

Note: It is only necessary to configure the primary Management Module (with IP addresses, etc.); the secondary Management Module does not need to be explicitly configured. In the event that the primary Management Module fails, the secondary Management Module will automatically inherit the settings from the primary Management Module. It is only necessary that both Management Modules be connected to the same network subnet.

Table 6: Management Module: Default IP Addresses.

Interface	Default IP address
eth0	192.168.70.125 / 255.255.255.0
eth1	192.168.70.126 / 255.255.255.0

4.2.1.3 Configuration of the Alteon Ethernet Switch Module (ESM)

The Alteon ESM is configured so that it is only manageable through the BladeCenter-T Management Module. In order to establish this capability the default IP address configured on the Alteon ESM (refer to on page) must be overwritten with a valid IP address on the Management Network.

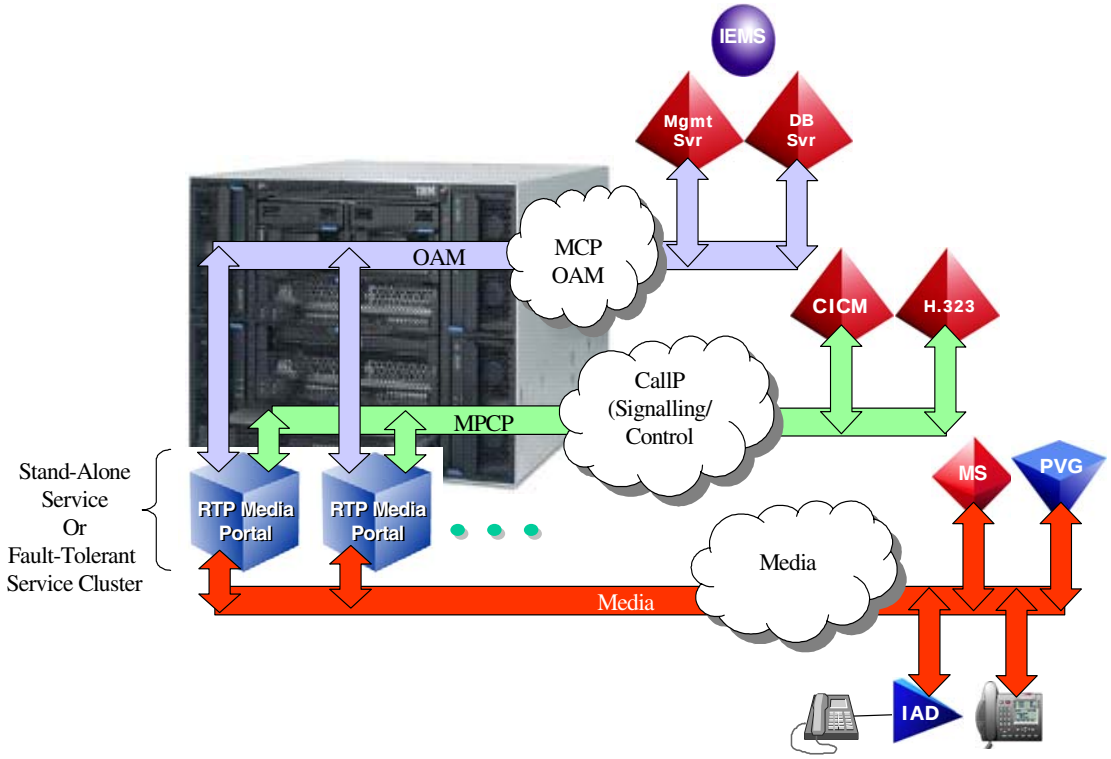
Table 7: Alteon ESM: Default IP Addresses.

Interface	Default IP address
1	10.90.90.91

4.2.2 Service Network

The Service Network is the network-space within which the services are provided and consumed. In fact, this network-space may exist as multiple Service Networks (as depicted in the following figure).
In order to provide the RTP Media Portal service, both the hosting BladeServer and the resident service instance must have presence in the Service Network(s) in order to connect: Service OAM, Service control (MPCP), and Service access (media). Refer to the following figure.

Figure 18 BladeCenter-T RTP Media Portal: Service Network Overview



The physical relationship of these IP address assignments to the Management Module and the Alteon ESM are represented in the following figure. The actual network topology created by these IP Address assignments is described in the subsequent figure.

Figure 19 Service Network Connections: Physical View (Layer-2 and Layer-3)

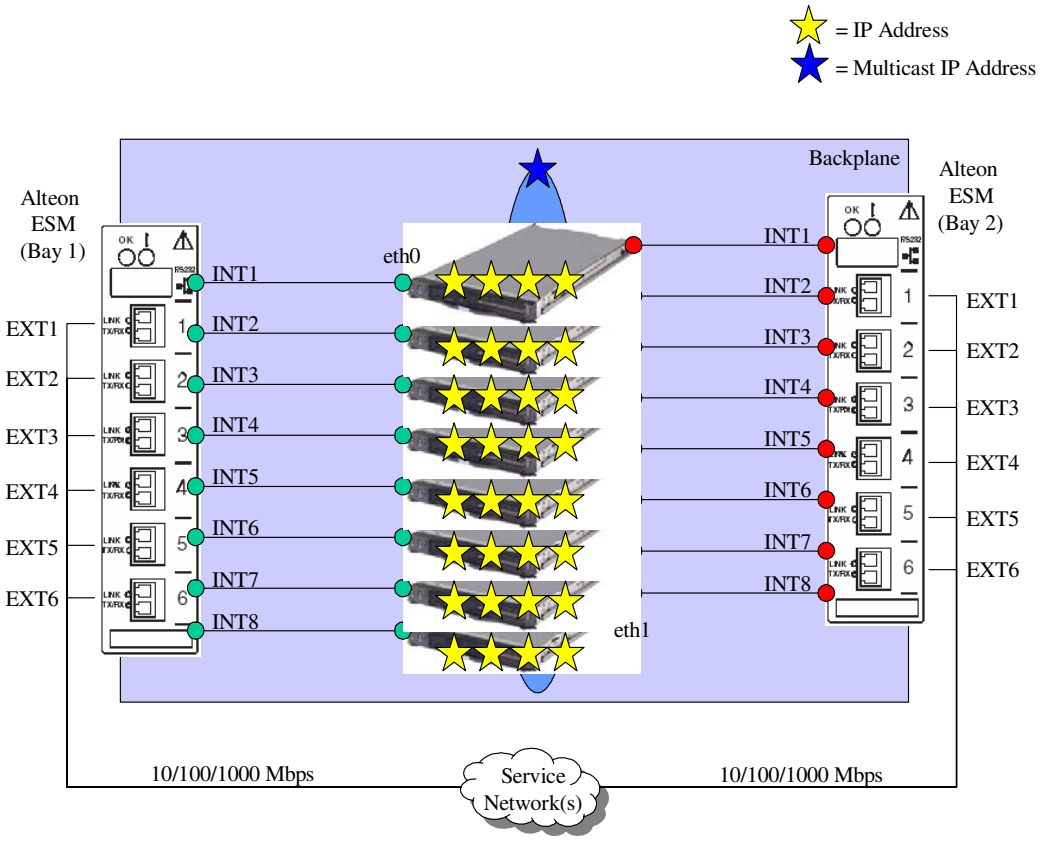
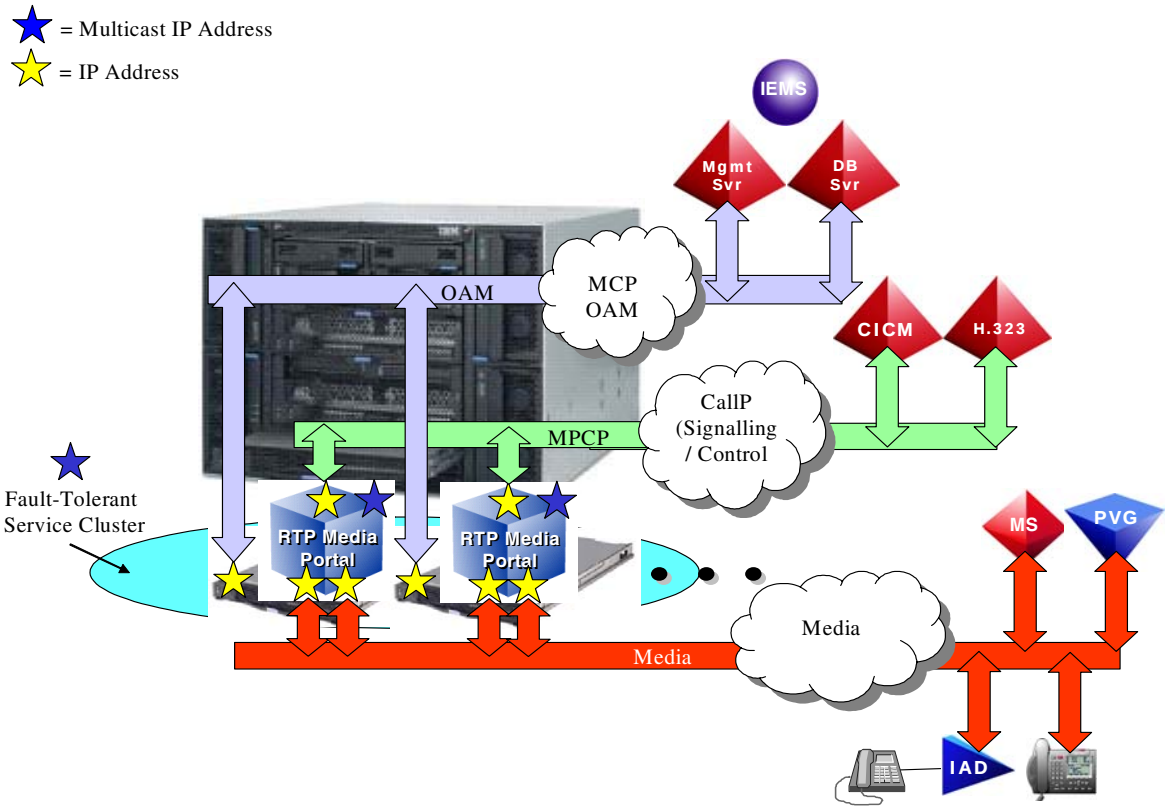


Figure 20 Service Network Connections: Logical View (Layer-3)



4.3 Service Configuration

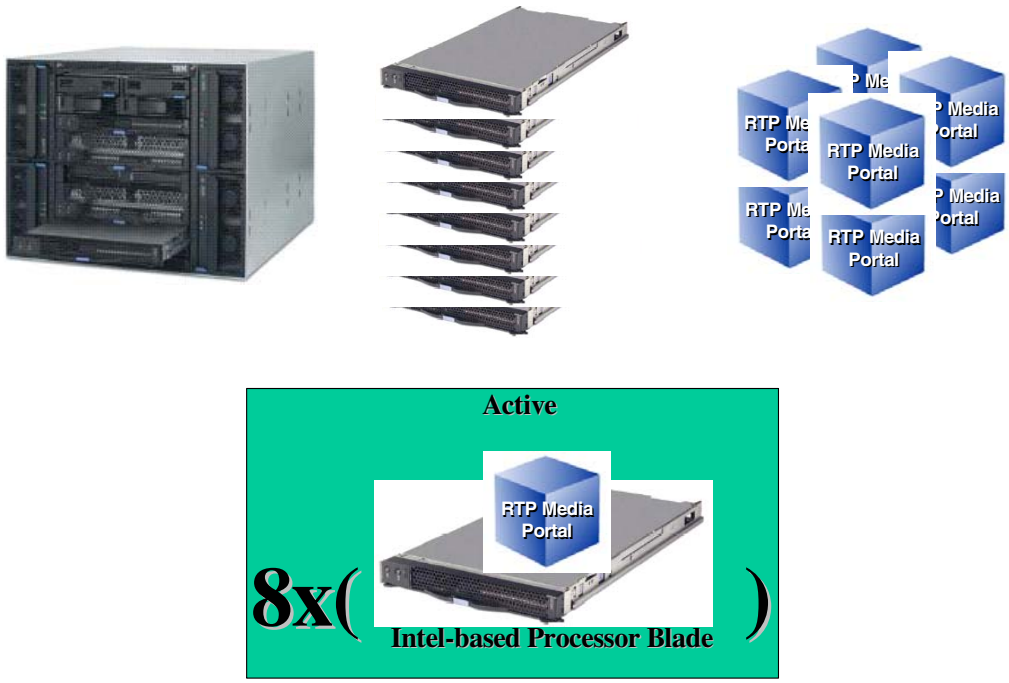
4.3.1 Overview

The introduction of the BladeCenter-T RTP Media Portal represents a major change in how the RTP Media Portal is viewed. The software re-architecture required by the BladeCenter-T RTP Media Portal essentially abstracted the functionality provided by the RTP Media Portal from the underlying platform – effectively establishing the RTP Media Portal as a service that is independent of a fixed relationship with its supporting hardware. Further, the introduction of the N+1 fault tolerance framework adds yet another dimension to the RTP Media Portal. As a result, this feature introduces more than a new hardware platform into the product, it introduces a major new configuration of the RTP Media Portal Service.

The BladeCenter-T RTP Media Portal can be configured to operate as either a collection of independent service instances (“Stand-Alone”), or as an N+1 fault tolerant service cluster (“Clustered”).

When configured as a collection of stand-alone service instances, the BladeCenter-T can support the execution of up to eight (8) independent non-redundant instances of the RTP Media Portal Service (refer to the following figure).

Figure 21 Stand-Alone RTP Media Portal Service Instances (Chassis View)



When configured as a redundant N+1 fault-tolerant service cluster, the BladeCenter-T can support the execution of up to seven (7) active instances of the RTP Media Portal Service and one (1) hot standby instance that is ready to assume the active sessions for any of the active instances (refer to the figure that follows on the next page).

These advances required adaptations to RTP Media Portal configuration to accommodate the new paradigms: RTP Media Portal as a service, and the N+1 fault tolerant RTP Media Portal Service Cluster. Adaptations were performed within the constraints of the capabilities and limitations of the MCP Management System. The resulting changes provide:

- The ability to configure the BladeCenter-T RTP Media Portal as a Stand-Alone Service Instance.

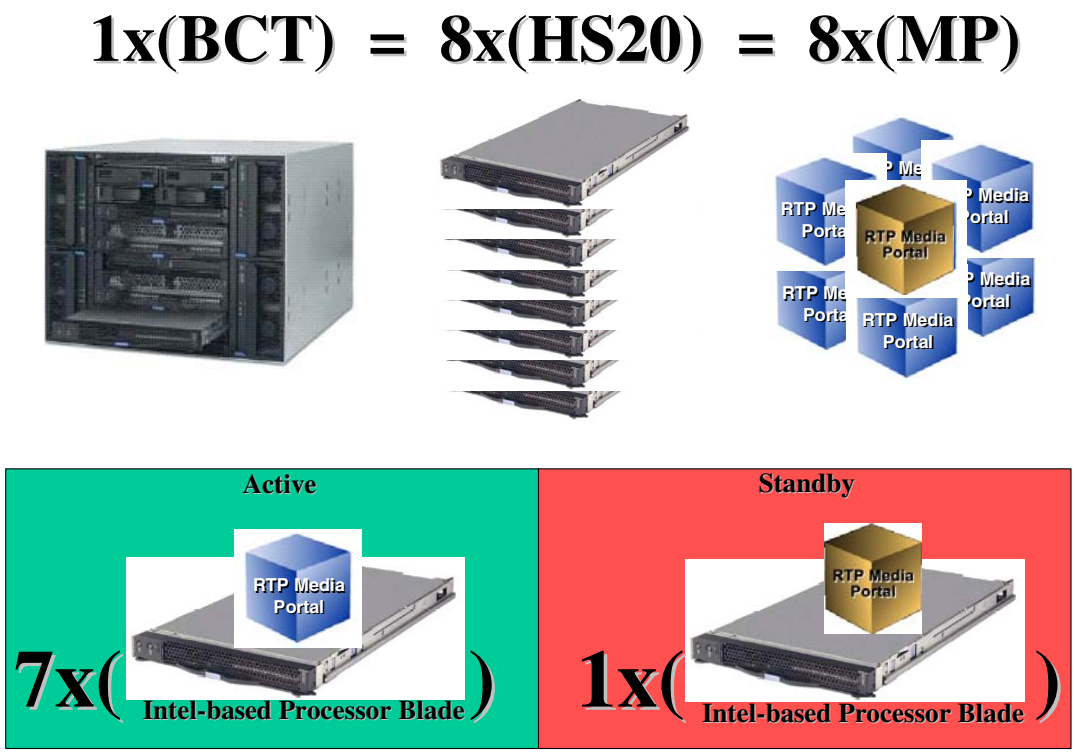
- The ability to configure the BladeCenter-T RTP Media Portal as an N+1 Fault Tolerant Service Cluster.
- The ability to manage the BladeCenter-T RTP Media Portal as a set of distinct network elements (unfortunately there are no Cluster-level management capabilities – management of the Cluster is achieved through the coordinated management of the individual Cluster members).

Fortunately, the configuration adaptations appear as minor changes to the configuration data as presented in the Management Console and so a consistent interface can be be presented for all varieties (the Motorola CPX8216-T introductory platform, and the new IBM BladeCenter-T platform) and configurations (Stand-alone, and Clustered) of the RTP Media Portal. In fact the configuration of the original Motorola CPX8216-T-based RTP Media Portals is unchanged (there is one new configuration parameter added to the RTP Portal Network Element, but for legacy CPX8216-T sites it is left set to its default value of “null”), while the new BladeCenter-T RTP Media Portal utilizes both pre-existing configuration structures (e.g. the RTP Portals Network Element for the conveyance of Engineering Parameters) and the adaptations made to configuration structures (e.g. the new “Clusters” entity in Network Data.

Additionally, both Stand-Alone and Clustered configurations of the BladeCenter-T RTP Media Portal are configured exactly the same – the differentiation being that the Stand-Alone is configured as a “1+0” (1 active instance, and no standby instances) Service Cluster. The real differences between the Stand-Alone and Clustered configurations is in their run-time characteristics and reaction to faults.

All of this is discussed in more detail in the following sections.

Figure 22 N+1 Fault Tolerant RTP Media Portal Service Cluster (Chassis View)



4.4 BladeCenter-T RTP Media Portal Configuration

4.4.1 Overview

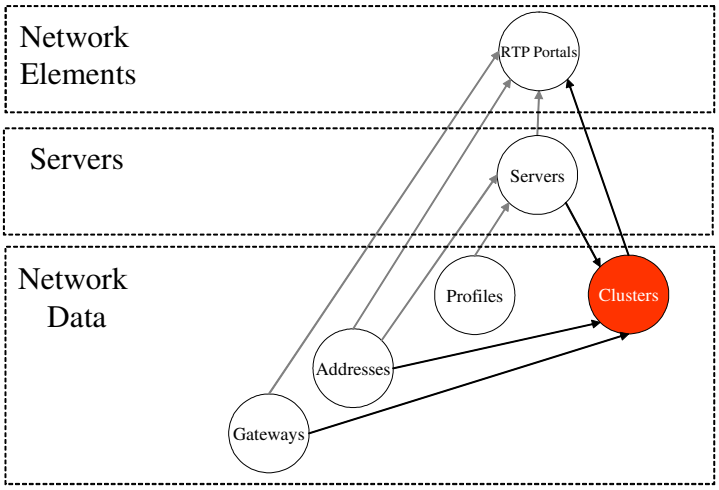
Pre-existing RTP Media Portal configuration structures remain intact for continued support of legacy Motorola CPX8216-T RTP Media Portal deployments. These pre-existing structures consisted of Network Data (specifically “Addresses”, “Gateways”, and “Profiles”), Servers, and Network Elements (where all data constituting an RTP Media Portal was combined together in the RTP Portal Network Element).

The BladeCenter-T RTP Media Portal builds on top of pre-existing configuration structures as follows (refer to the following figure):

- Network Data: the new “Clusters” entity is created in Network Data. The new “Clusters” entity contains all of the information required to configure a RTP Media Portal Service Cluster. As Network Data, “Clusters” is delivered over the MCP OAM Framework to all BladeCenter-T RTP Media Portal nodes.
- Servers: unaffected.
- Network Elements: The “RTP Portal” Network Element is enhanced with the addition of a new field “Cluster” that references a specific entry in the

new Network Data “Clusters” entity. The new “Cluster” field provides the means for identifying an RTP Media Portal’s membership in an N+1 Fault Tolerant Service Cluster.

Figure 23 RTP Media Portal Service: Data Relationahips



The new Network Data “Clusters” entity contains configuration information for RTP Media Portal Service Clusters. This configuration information includes the Common Service Data for the Cluster, the Service Instance Data, and the Fault Tolerant Framework Data (refer to the following table). The Common Service Data is a set of configuration parameters replicated from the RTP Portal Network Element’s “Bladerunner” information. The Service Instance Data defines the parameters that are unique to each active instance of the service. The Fault Tolerance Framework Data defines the parameters that define the Service Cluster.

Table 8: RTP Media Portal Service Cluster: Configuration Data

Data Type	Parameter Name	Parameter Type	Parameter Description
Common Service Data	Cluster Name		Cluster name or id or both - something unique for this cluster. Convention: <Cxx>+<name>
	Default Gateway		Pull-down of available Gateways (from Network Data) that overrides the "Default Gateway" specified in the RTP Portal NE data.
	CallLegs		Overrides "CallLegs" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	CriticalPortUsageAlarmLevel		Overrides "CriticalPortUsageAlarmLevel" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	IdleSessionAuditPeriod		Overrides "IdleSessionAuditPeriod" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	LongCallDuration		Overrides "LongCallDuration" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	LongIdleDuration		Overrides "LongIdleDuration" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	MajorPortUsageAlarmLevel		Overrides "MajorPortUsageAlarmLevel" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	MinorPortUsageAlarmLevel		Overrides "MinorPortUsageAlarmLevel" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	PollTimerDelay		Overrides "PollTimerDelay" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	LongCallDuration		Overrides "LongCallDuration" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	StaticRTPPorts		Overrides "StaticRTPPorts" parameter present in the RTP Portal NE Config Parm Group "BladeRunner".
	Number of Port		Overrides "Number of Port" parameter present in the RTP Portal NE "Blade" Data.
	Min Port Value		Overrides "Min Port Value" parameter present in the RTP Portal NE "Blade" Data.
	Max Port Value		Overrides "Max Port Value" parameter present in the RTP Portal NE "Blade" Data.
	Session Manager		Pull-down of available Servers (from Servers) that overrides the "Session Manager" Data specified in the RTP Portal NE.*There can be multiple occurrences of this data*
	Discovery Probe Timer Period		Integer field specifying the frequency of the periodic MPCP RSIP to the controlling Call Servers. The value entered into this field overrides the value for the "Discovery Probe timer" field for each instance of "Session Manager" Data specified in the RTP Portal NE.

Fault Tolerance Framework Data	Multicast IPaddr		These two parameters uniquely define this Cluster. They represent the Peering Plane used by this Cluster for the establishment of the reliable messaging framework. The reliable messaging framework is used to carry the election protocol, checkpoint run-time service data to the Standby Service Instance, and to monitor member status.
	Multicast Port		
	Heartbeat Period		Frequency of heartbeat status check.
Service Instance Data	{N}		{implied} The number of instances of "Service Data" implies the value of "N". This correlates exactly to the expected number of servers (which is "N+1").
	Instance Name		Name of this Service Instance. Convention: <Cluster-Name>+<Ixx>+<Instance-Name>
	Controlipaddr		Pull-down of available IPaddrs (from Network Data:Addresses). This parameter provides a unique IPaddr for the RTP Media Portal Service that is different from the platform IPaddr. This is the result of abstracting the RTP Media Portal Service from the platform, and is used for conveyance of MPCP messages.
	ControlNetMask		Defines the Control-plane subnet for this Service Instance
	Net1MediaIP		Pull-down of available IPaddrs (from Network Data:Addresses) that overrides "Net1 Media IP" parameter present in the RTP Portal NE "Blade" Data. This defines one of the two media IPaddrs that establish presence for this service in the Media-Plane.
	Net1NetMask		Overrides "Net1NetMask" parameter present in the RTP Portal NE Config Parm Group "BladeRunner". Defines the Media-plane subnet for this Service Instance.
	Net2MediaIP		Pull-down of available IPaddrs (from Network Data:Addresses) that overrides "Net2 Media IP" parameter present in the RTP Portal NE "Blade" Data. This defines one of the two media IPaddrs that establish presence for this service in the Media-Plane.
	Net2NetMask		Overrides "Net2NetMask" parameter present in the RTP Portal NE Config Parm Group "BladeRunner". Defines the Media-plane subnet for this Service Instance

4.4.2 Procedural Overview

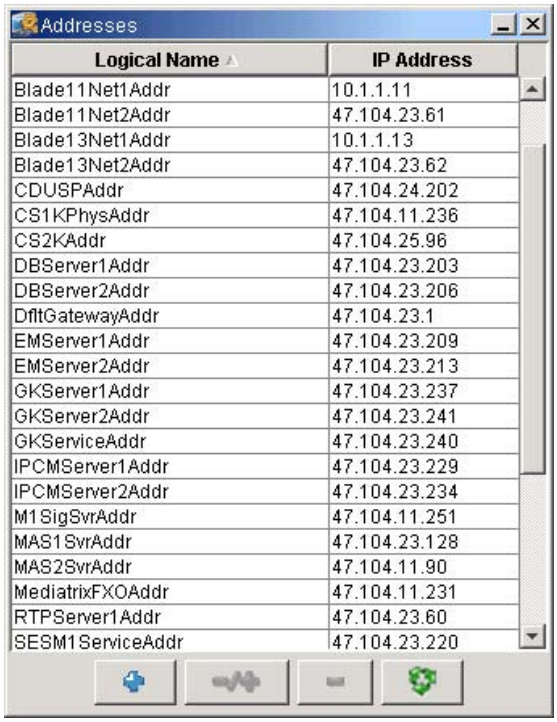
The BladeCenter-T RTP Media Portal is configured using the MCS System Management Console, and is accomplished through the use of the new “Clusters” entity in the Network Data, and a new field in the RTP Portals Network Elements (the new field references an entry in the “Clusters” Network Data to specify cluster membership). Refer to the following figure.

Figure 24 System Management Console: Affected Data Structures

Procedurally, the BladeCenter-T RTP Media Portal is configured in a fashion similar to that used to datafill the CPX8126-T RTP Media Portal – with some additional steps that are necessary to include the creation/population of the new data structures:

Step 1: Datafill Supporting Parameters
At this initial stage all new referenced data must be entered into the system:

- Enter all new IP addresses into Network Data::Addresses.

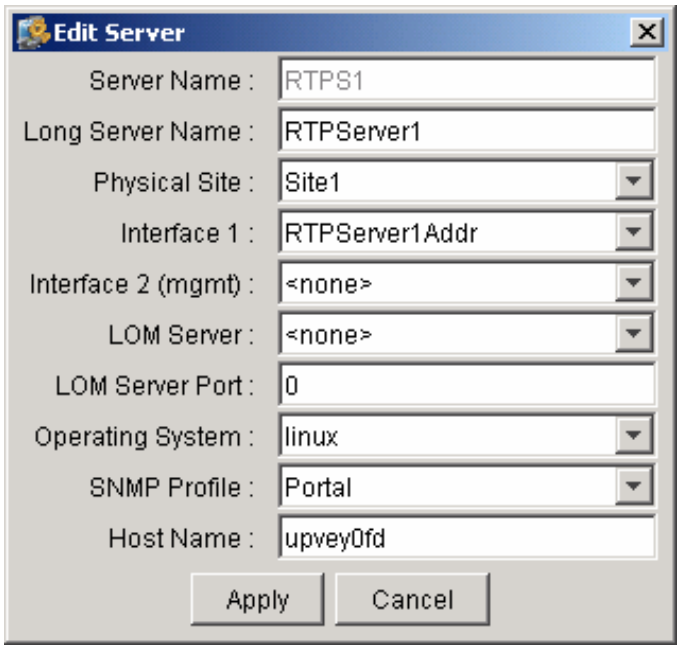


- Enter all new Gateways into Network Data::Gateways.

Note: There are no changes to the structure of this data.

Step 2: Datafill "Servers" Parameters
This stage of configuration creates a logical representation of a Server within which to group together all the data that defines a Server including physical IP address associations (the physical IP address was actually assigned during installation and commissioning):

- Datafill the “Interface1” field (pick-list of datafilled IP “Addresses”) with the intended physical IP address for each Blade Server in the BladeCenter-T chassis. This IP address is the bond0 physical address on the Blade Server – and is also used to represent the Blade Server and the RTP Media Portal Service Instance in the MCS OAM System.

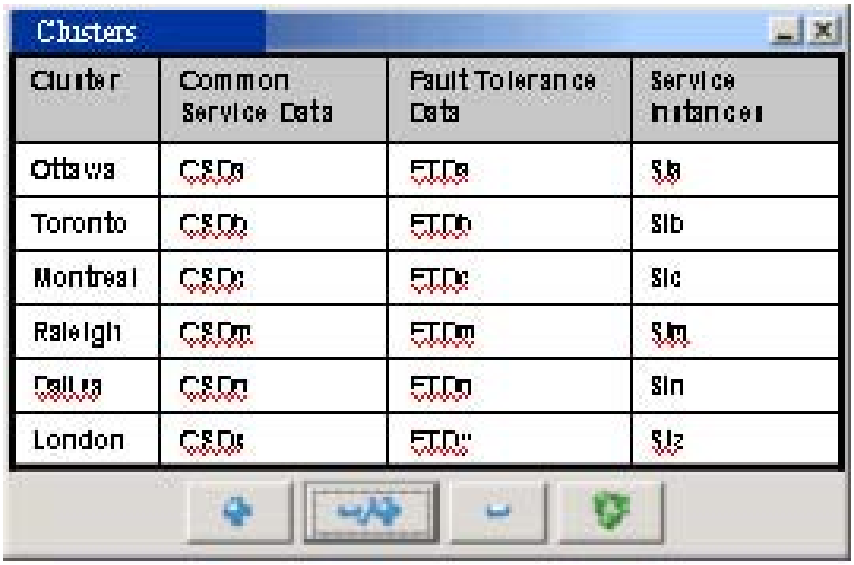


Note: There are no changes to the structure of this data.

Step 3: Datafill “Clusters” Entities
This stage of configuration creates a logical representation of the Service Cluster within which to group together all the data that defines the cluster.

The first step is to create a new Service Cluster:

- Open the “Clusters” window in Network Data, and then click the “+” button to create a new Service Cluster.



Once created the new Service Cluster can be populated with the parameters that uniquely identify this cluster as well as all of the parameters that define the service characteristics for this cluster (refer to the following figure):

- Common Service Data must be supplied that defines the operating parameters of the service instances (all service instances in a cluster run the same service configuration to maintain service consistency):
- Fault Tolerance Framework Data must be supplied to define the characteristics of the channel used for intra-cluster communication between all cluster members.
- Service Instance Data is where each of the RTP Media Portal Service Instances is defined (i.e. the MPCP control IP address, and up to two media IP addresses). There is one entry per Service Instance – this constitutes the “N” in the N+1 Fault Tolerance strategy. Refer to the second figure that follows for sample screenshots of adding a Service Instance.

Figure 25 New Network Data: Clusters

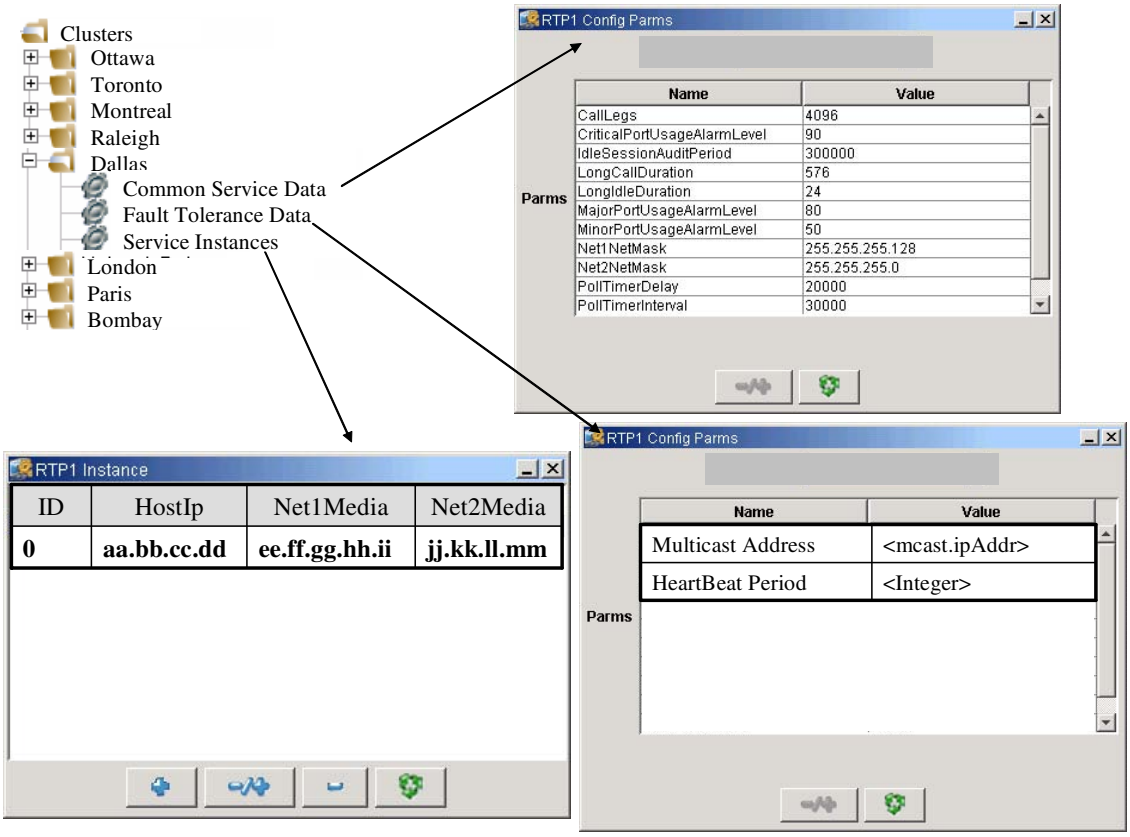
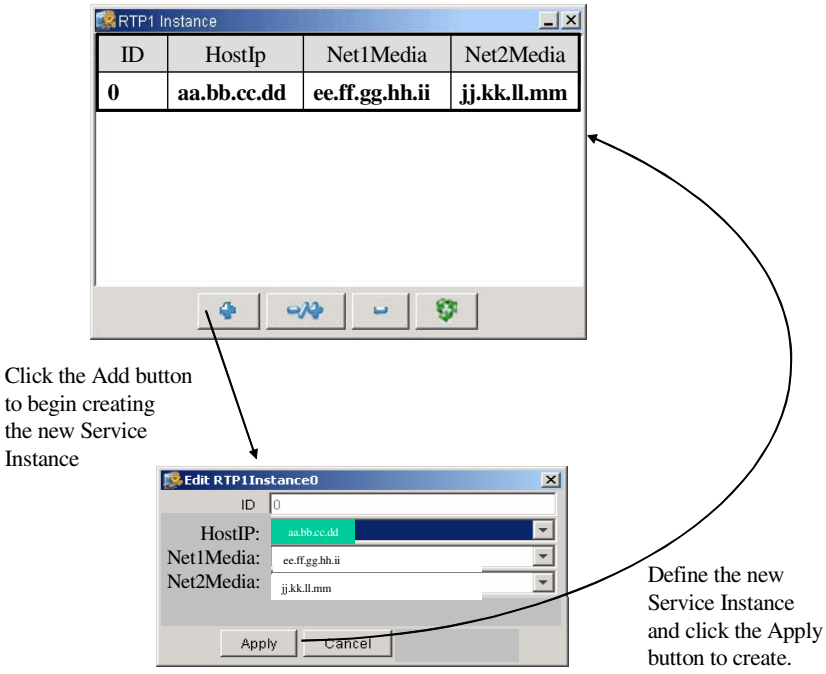


Figure 26 Clusters (Network Data): Adding a Service Instance



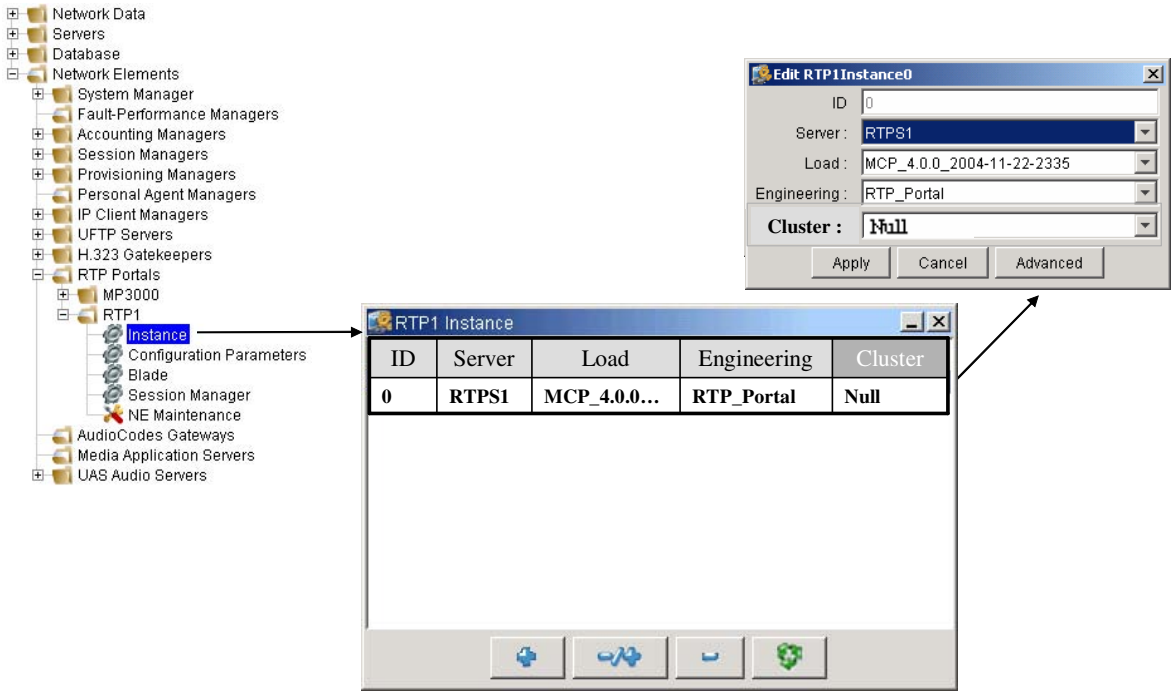
Step 4: Datafill "RTP Portals" Network Elements

As for the CPX8216-T based RTP Media Portal, the RTP Portal Network Element is the most fundamental configuration data structure. The RTP Portal Network Element provides the BladeCenter-T RTP Media Portal with: Engineering parameters, and a point of attachment into the MCS OAM Framework. It is the RTP Portal NE that: enables the deployment of the RTP Media Portal software, provides the channel for telemetry (Logs, Alarms, and Operational Measurements), and enables the maintenance events (Start, Stop, and Kill).

Also, in the context of the BladeCenter-T RTP Media Portal, each RTP Portal Network Element represents one Blade Server. This one-to-one mapping is due to the fact that the RTP Portals NE identifies the target server (through reference to an entry in the "Servers" Configuration Data).

This stage of configuration also provides the opportunity to specify membership in a BladeCenter-T RTP Media Portal Service Cluster through use of the new Cluster field in the RTP Portal NE data. Refer to the following figure.

Figure 27 RTP Portal NE: Specification of Cluster Membership



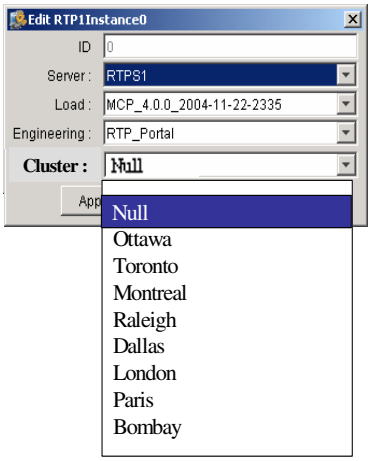
The new RTP Portal NE Cluster field is populated by selecting from a pick list. The pick-list contains an entry for each of the Clusters defined in the Network Data (and a “null” entry). Refer to Figure 62 on page 129. Each Server participating in a Service Cluster (identified within the RTP Portal Network Element data structure) is assigned Cluster membership in this manner – thuereby establishing the “N+1” servers hosting the Cluster.

Cluster membership is only available to the BladeCenter-T RTP Media Portal – the legacy CPX8216-T RTP Media Portal cannot be a member of a Service Cluster and must have “null” selected in the new “Cluster” field that appears in the Instance data of the RTP Portal NE.

Both BladeCenter-T RTP Media Portal configurations (the Stand-alone and the Service Cluster) must be configured as members of a Cluster. In the case of the BladeCenter-T RTP Media Portal Stand-alone, configuration is performed such that a “1+0” (1 Active Service Instance and 0 Standby Service Instances) cluster is created. All Clusters are uniquely defined by the combination of multicast IP Address and multicast port specified in the Fault Tolerance Data in the new “Clusters” Network Data, but what makes the Stand-Alone configuration unique is that there is onle one Service Instance configured.

Note: The legacy CPX8216-T RTP Media Portal will fail to start if it detects Cluster configuration in its datafill.

Figure 28 RTP Portal NE: Cluster Pick-List



5: Glossary

Term	Definition
APD	Address and Port Discovery
BPT	Bulk Provisioning Tool
CPU	Central Processing Unit
ERL	Emergency Response Location
FD	Functional Description
FSD	Functional Specification Document
FW	Firewall
IP	Internet Protocol
MCP	Multimedia Communications Platform
MGCP	Media Gateway Control Protocol
MP	Media Portal
MPCP	Media Proxy Control Protocol (for control of RTP Media Portal)
MPG	Media Portal Group
NAT	Network Address Translation

Term	Definition
NAPT	Network Address and/or Port Translation
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network (the legacy circuit-switched telephone network)
RSIP	Restart In Progress (an MPCP message)
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
UDP	User Datagram Protocol

Product = MCS

A00011740 -- Packet Cable Multimedia for CS2K

Functional Description

1: Applicable Solution(s)

IAC

1.1 Description

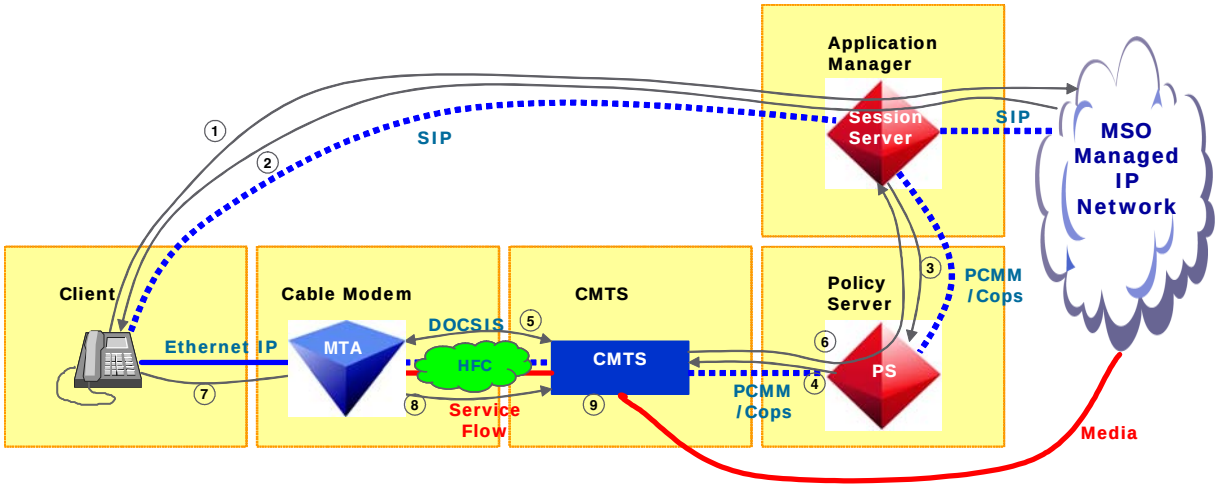
1.1.1 Functional Overview

PacketCable Multimedia is an architecture developed by CableLabs to enable MultiService Operating Companies to deliver Quality of Service enabled multimedia services over DOCSIS networks. PacketCable Multimedia extends the Dynamic Quality of Service architecture developed as part of PacketCable 1.X to allow Application Managers in the MSO network to request and obtain Quality of Service treatment for multimedia traffic flows on behalf of an end user.

This service enhances the CS2000 SIP Lines solution to take advantage of the PacketCable Multimedia mechanisms to provide QoS for voice and video sessions established over an MSO DOCSIS network. The PCMM signaling implementation is compliant with PacketCable specification PKT-SP-MM-I02-040930 (refer to section 1.7 on page 1842 for a detailed compliance matrix).

The following diagram illustrates a high level call flow for a PacketCable Multimedia (PCMM) SIP call in the CS2000.

Figure 1 PCMM SIP Call Flow

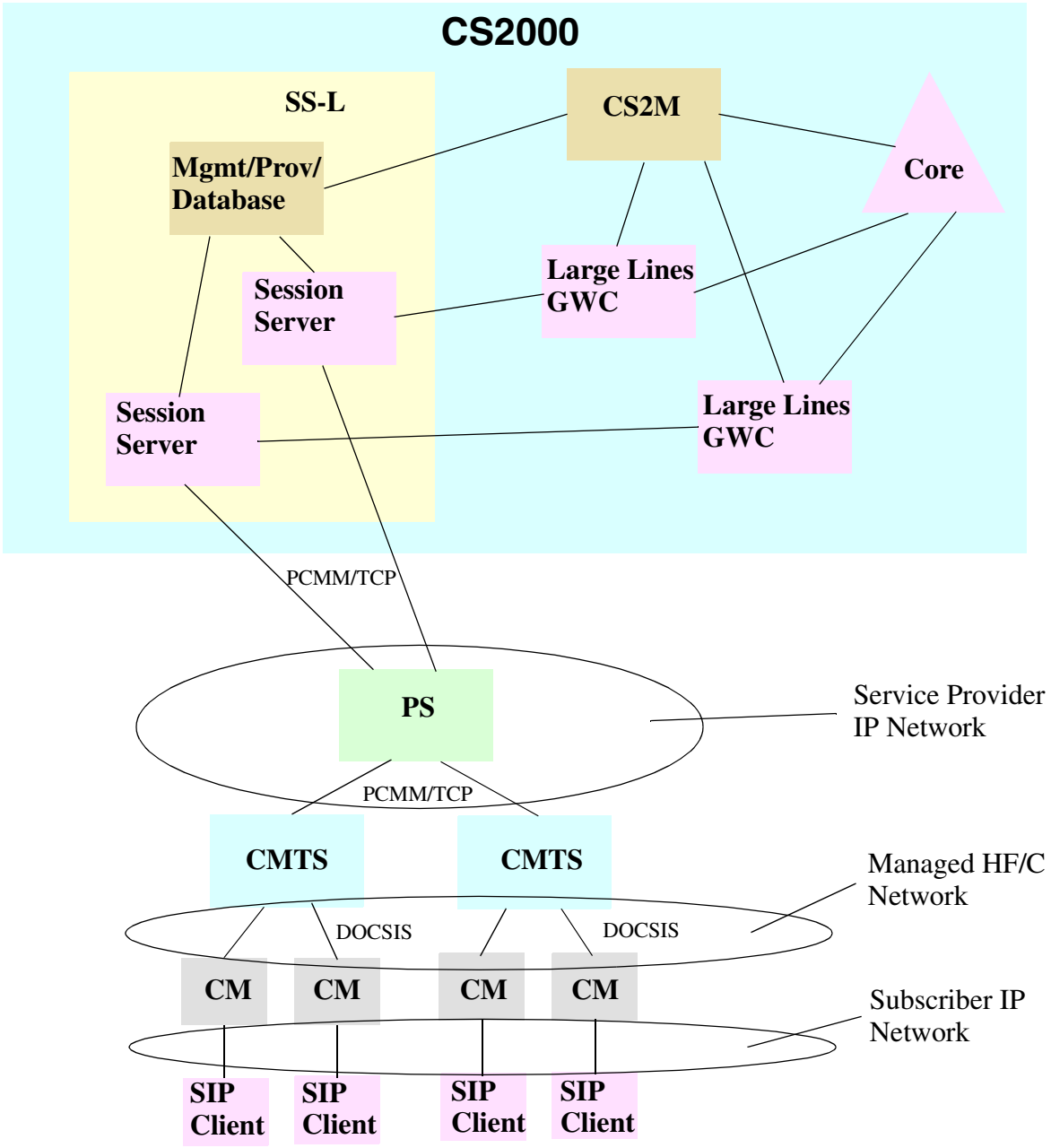


1. SIP Client originates a session application (SIP Invite) to the Session Server and into the network to a destination client
2. The destination responds with an OK (200 OK) to the SIP Client through the Session Server
3. The application manager on the session server requests managed QoS on behalf of the SIP client by signaling to the policy server
4. The Policy Server makes policy decision and sends the request to the CMTS
5. The CMTS uses DOCSIS signaling to create service flow in the Cable Modem
6. The CMTS responds with a gate-id, which is passed via Policy Server to Session Server
7. The SIP Client sends data/media to the Cable Modem
8. Cable Modem puts data on the appropriate managed service flow to the CMTS based on classifier (e.g. IP address, port)
9. CMTS enforces policy for data on the service flow and network using the gate

Signaling
Media
High QoS Media

The following diagram illustrates a typical cable network topology for a SIP lines deployment. Both MCS and CS2K are shown.

Figure 2 PCMM Network Diagram



The diagram points out three networks: the service provider IP network, the HF/C (hybrid fiber/coax) network and the subscriber IP network. The network that is not explicitly shown is the call server IP network by which the CS2K and MCS network elements communicate.

The HF/C network is the focal point of PCMM since that is where we are managing QoS. For media stream network connectivity between a SIP client

and another endpoint, DIFFSERV is used for QoS outside of the HF/C network.

The subscriber IP network may be behind a NAT. SIP clients can be SIP phones or SIP soft-clients such as the Nortel's MCS Multimedia PC client.

The following sections describe how to setup PCMM, how to determine if PCMM is working correctly, and how to alter the PCMM configuration after it is up and running.

1.1.2 Setting up PCMM

In order to setup the PCMM service the following high level steps must be carried out in order. Detailed instructions for each step can be found by following the links.

1. Enable the PCMM Service Key (see section 1.1.5 on page 1803)
2. Add a policy server IP address (see section 1.1.6 on page 1804)
3. Add a policy server (see section 1.1.7 on page 1805)
4. Configure the policy server AMIDs for each session manager (see section 1.1.8 on page 1808)
5. Assign Diffserv value for subscriber (see section 1.1.9 on page 1811)
6. Assign PCMM capability to subscribers (see section 1.1.10 on page 1814)

1.1.3 Verifying that PCMM is working

Once you have gone through the steps outlined in section 1.1.2 on page 1803, you can do the following to verify that PCMM is working as expected.

1. Check for PCMM alarms (see section 1.1.11 on page 1820)
2. View PCMM operational measurements (see section 1.1.12 on page 1824)

1.1.4 Altering PCMM configuration

If you need to alter your PCMM configuration or provisioning, please see the following sections.

- Changing PCMM configuration (see section 1.1.13 on page 1830)
- Removing PCMM service from a subscriber (see section 1.1.14 on page 1831)
- Deleting a policy server (see section 1.1.15 on page 1832)

1.1.5 Enabling the PCMM Key

The PCMM service is key coded. To use the PCMM functionality, the PCMM key must be enabled, and part of your systems license key.

The PCMM key within the license can be generated as enabled, disabled, or not present. If the key is not present then the service is disabled.

Key codes within a license key can be added or upgraded, but keys can not be removed. Once a license is added to a system with PCMM enabled, The PCMM key can not be disabled.

The generation of the license key with the PCMM key code is done using the Nortel KRS (Key Registry System).

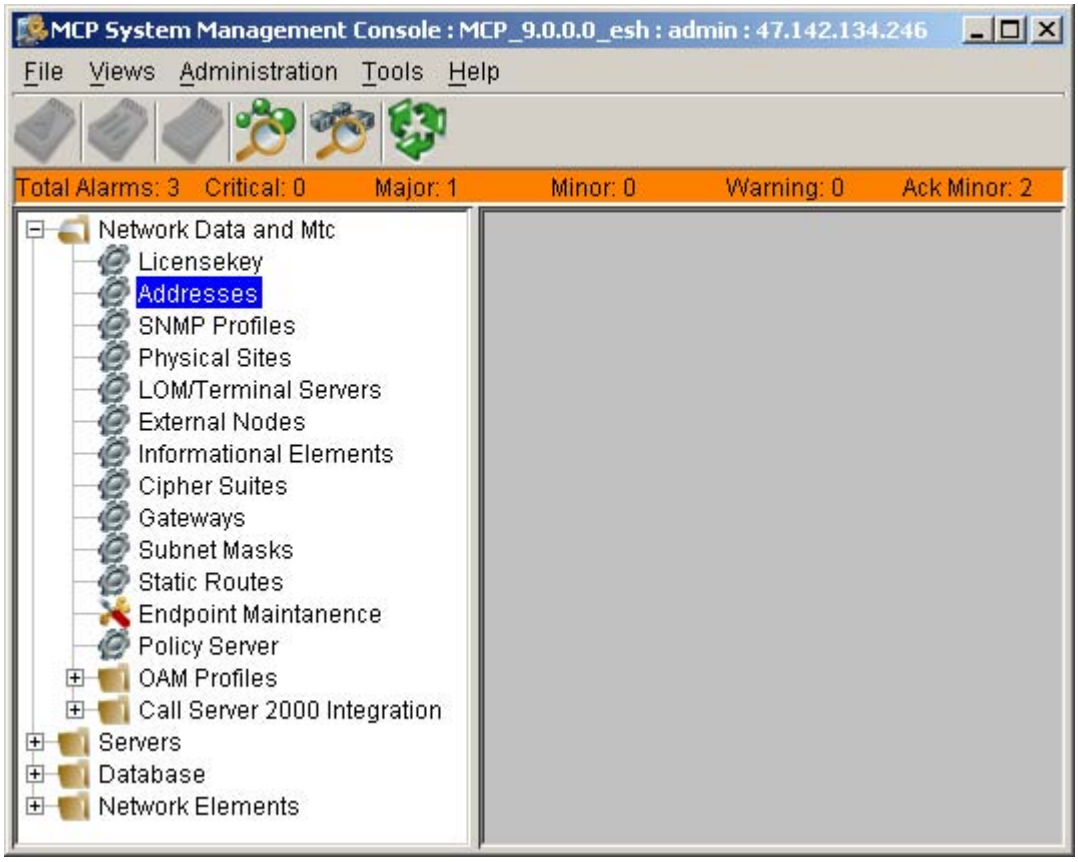
The addition of a system license key is covered as part of the installation and commissioning process.

1.1.6 Associating a Logical Name to a Policy Server IP address

To configure a policy server IP address and associate the address with a name that will be used in subsequent references to the address:

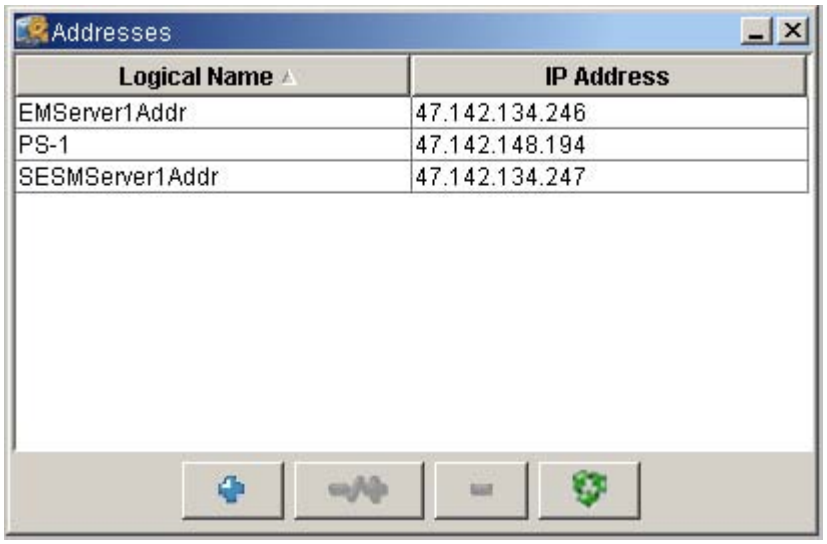
- From the MCP System Management Console expand the “Network Data and Mtc” item

Figure 3 MCP System Management Console for Addresses



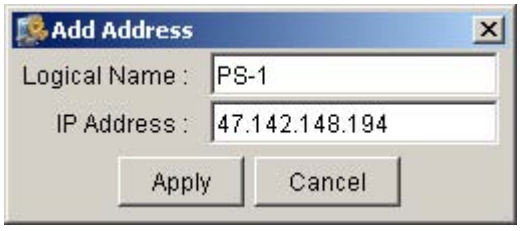
- Click the ‘Addresses’ icon, the ‘Addresses’ window will appear

Figure 4 Addresses Dialogue



- Select '+'and provide the PS address logical name and IP address in the form x.x.x.x

Figure 5 Add Address



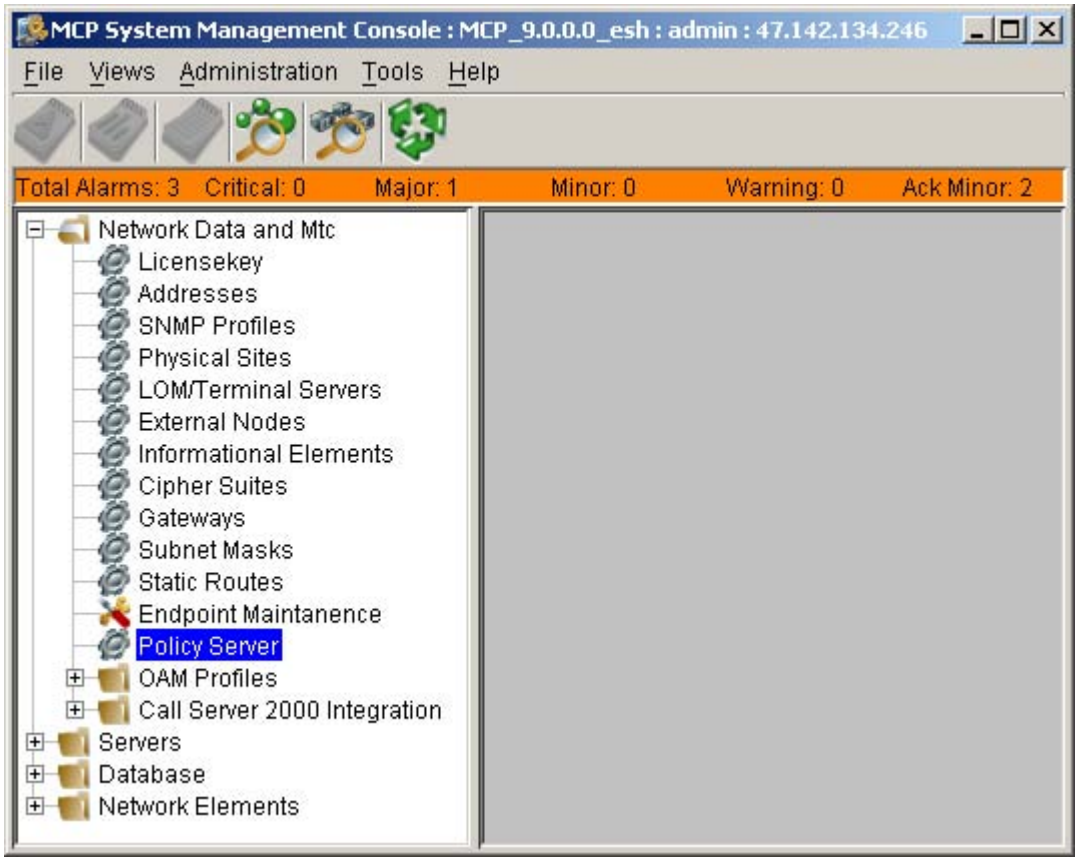
Now the logical name ("PS-1" in this example) will appear as a choice anywhere you need to enter an IP address.

1.1.7 Adding a Policy Server

To add a policy server:

- On the MCP System Management Console GUI expand the "Network Data and Mtc" tree

Figure 6 System Management Console for Policy Server

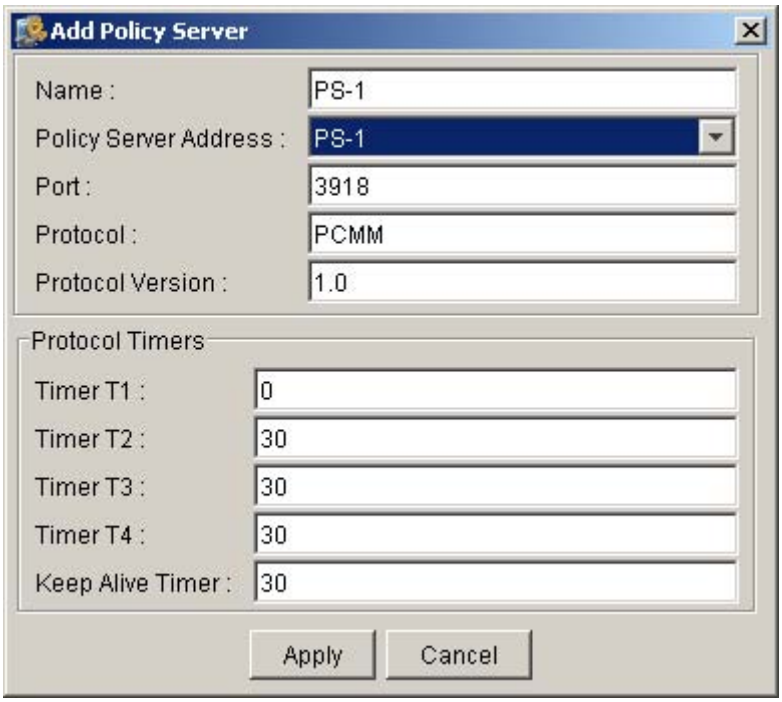


- Click “Policy Server” and a Policy Server window will appear showing the existing policy servers (if any)

Figure 7 Policy Server Dialogue

- Select the '+' icon and a new window appears. Enter the following fields:

Figure 8 Add Policy Server



a. **Name**: customer defined string up to 16 characters

b. **Policy Server Address**: select the logical address to assign from the pull down list which was configured under the 'Addresses' icon (see section 1.1.6 on page 1804). This is the address that the policy server will listen on for PCMM signaling.

c. **Port:** this is the port number the policy server will listen on for PCMM signaling. It must be and integer value from 1 to 65,535. The IANA well-known port for PCMM is 3918, so unless a different port is required by the policy server 3918 should be used.

d. **PCMM Protocol**: the PCMM signalling protocol used by the Policy Server. This should be set to the string "PCMM".

e. **Protocol Version -** the pulldown menu shows PCMM protocol versions supported by the CS2000. Choose the highest protocol version that you want the CS2000 to negotiate to for the policy server being configured. For example, if the policy server and the CS2000 both support versions 1.0 and 2.0, but you wish to continue using version 1.0, you can select 1.0 for this field.

f. **Timer T1:** timer maintained by the CMTS to determine the time in seconds that a gate can be in the 'authorized state'. A value of zero (the default) indicates that CMTS should use its own provisioned value.

The suggested range for this timer (if not zero) is between 5 and 180 seconds.

g. **Timer T2:** timer maintained by the CMTS to determine the time in seconds that excess reserved bandwidth must be held by CMTS. A value of zero disables this timer. The default value is 30 seconds. The suggested range for this timer (if not zero) is between 5 and 180 seconds.

h. **Timer T3:** timer maintained by the CMTS to determine the time in seconds that the service flow can be idle (no packets flowing) before being reported by CMTS. A value of zero disables service flow activity monitoring. **Nortel strongly recommends against disabling this timer as this can lead to hung resources in the CMTS**. The default value is 30 seconds. The allowed range for this timer is between 10 and 300 seconds.

i. **Timer T4:** timer maintained by the CMTS to determine the time in seconds that a gate can remain in the 'committed-recovery state' (due to T3 expiration). **Nortel strongly recommends against a T4 value less than 10 seconds**. The default value is 30 seconds. The allowed range for this timer is between 10 and 300 seconds.

j. **Keep Alive Timer:** this is the PCMM keep alive timer which is used to determine if the PS connection is healthy. The default value is 30 seconds. The allowed range for this timer is between 10 and 180 seconds. Keep-alive messaging cannot be disabled.

Once these fields are entered, click "Apply" and the PS will be configured.

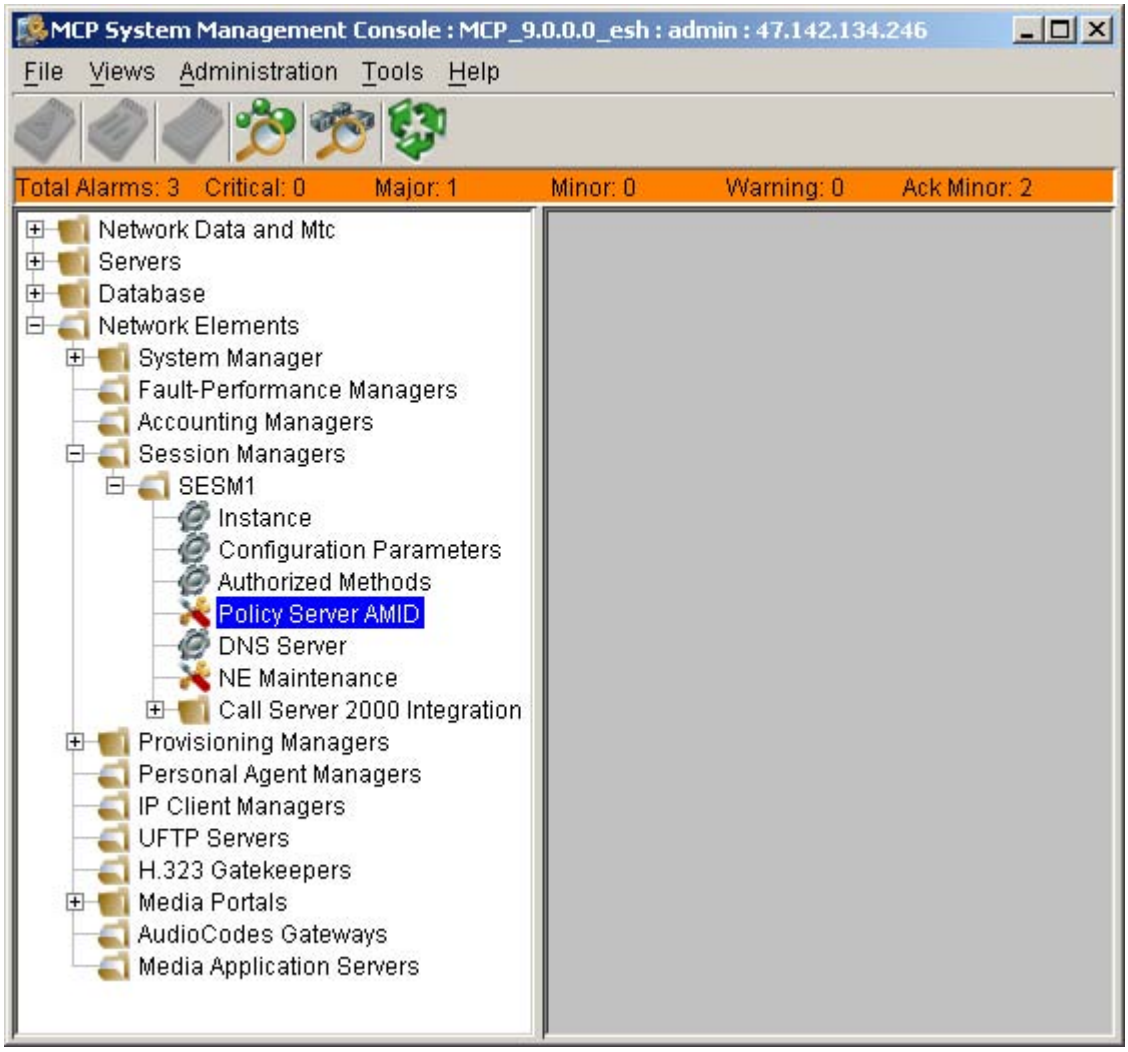
1.1.8 Configuring AMIDs for a Policy Server

For each PCMM signaling connection to a policy server, a set of application manager IDs must be configured. These AMIDs may be used by the policy server to keep track of application manager connections or may even be used to give the policy server an indication of the type of service being requested (audio or video).

In the MCS system, each active session manager has a connection to the policy server. Each active session manager must therefore have a set of AMIDs configured against the policy server. Here are the steps to set up AMIDs for a session manager. ***These steps must be repeated for each active session manager in the system.*** You need not configure AMIDs for redundant session managers.

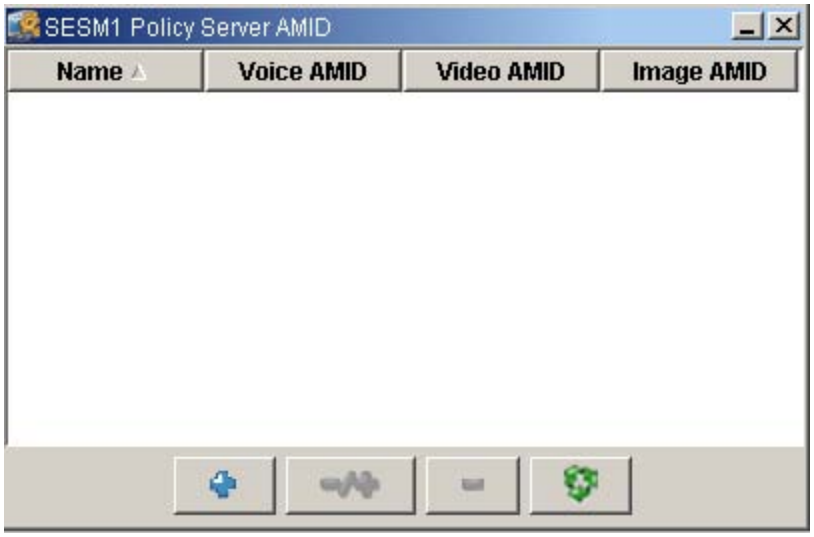
- From the MCP System Management Console, expand the Network Elements, Session Managers and then an instance of a session manager (SESM1 in this example).

Figure 9 System Management Console for AMIDs



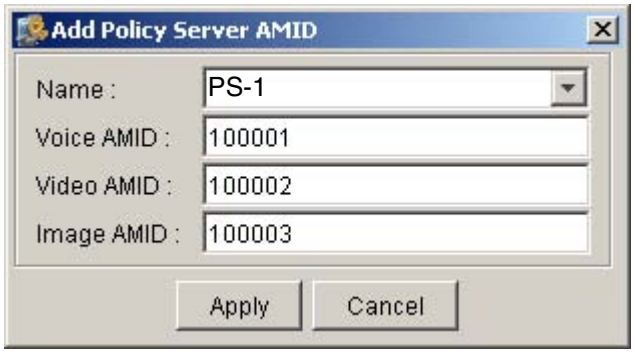
- When you click on “Policy Server AMID”, a window appears showing the configured policy servers. Select a policy server and a window will appear to allow AMID entry.

Figure 10 Policy Server AMIDs Dialogue



- Select a policy server and click on the "+" button and a window will appear to allow you to input AMID values. The MCS will ensure that the AMIDs for each Session Manager / policy server combination are unique. The voice/video/image service AMID values may be the same within each Session Manager/PS assignment.

Figure 11 Add Policy Server AMID



a. **Voice AMID:** value which represents the voice service type. Value between 0-4,294,967,295.

b. **Video AMID** - value which represents the video service type- value between 0-4,294,967,295.

c. **Image AMID** - value which represents the image (fax) service type-value between 0-4,294,967,295.

- Select 'Apply' and the Policy Server AMIDs are will be configured.
- Repeat these steps for each active session manager.

1.1.9 Setting up Diffserv for PCMM

The DiffServ parameters used for PCMM come from the existing QoS provisioning in the service package. The PCMM and QoS Services must be assigned to a domain, and both services created as part of a service package. The service is then assigned to all users you wish to have the PCMM service enabled. These associations are done using the Provisioning Client interface.

1.1.9.1 Assigning DSCP values to a Service Package

To assign the QoS service to the domain, from the Provisioning Client, select Services -> Assign Services.

Figure 12 Assigning Services

In the Assign Services window select the domain to add the QoS service package to and then click the Continue button.

Figure 13 Assigning Services to a Domain

To enable the QoS Service on the domain, from the Assign services to domain... window select QoS (a checked box to the left of the service name) from the list of available services, and once selected, click the Save button at the bottom of the screen.

To add QoS to an existing service package, under your Domain, open Service Package then List Packages.

Figure 14 Listing Service Packages

On the Service package list for domain … window to the right, select Details-Modify next to the Package you wish to add the service to.

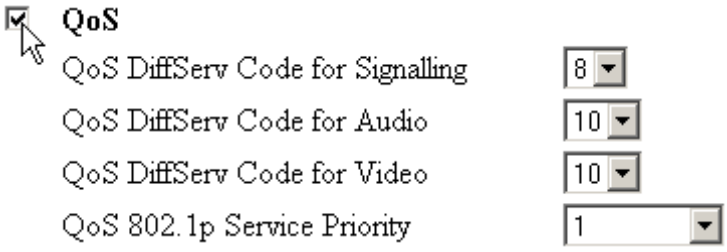
Figure 15 Package Name Details

In the window Package details for package everything belonging to domain...., select the check box to the left of the QoS Service, and Verify that the DiffServ values are correct for your domain. You can use the pull down menus to select the values for the users who subscribe to the service package.

The values in the fields represent the decimal representation of the high-order 6 bits of the DSCP/TOS field to be set in the IP header. To select the value for "expedited forwarding", for example, choose a value of 46 (decimal). This corresponds to an IP header bit pattern of 1011 1000, where the low-order 2 bits are always set to zeros.

Note that PCMM signaling does not use the QoS DiffServ Code for Signalling.

Figure 16 Setting QoS DiffServ for a Package



If the pulldown boxes don't have the DSCP value you want, you can define new DSCP values as follows:

Otherwise, click “Save and Enforce Now” to have the values updated, or “Save and Enforce Later” for that outcome.

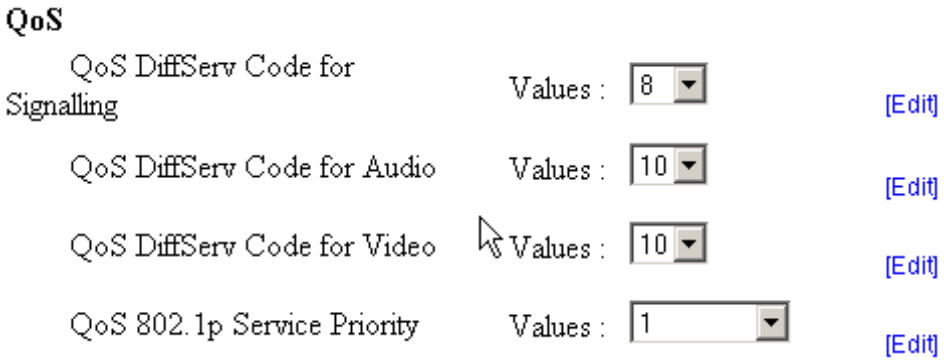
1.1.9.2 Defining New DSCP Values

To create new DSCP values for PCMM, from the Provisioning Client, open Services -> Define Service Parameters, then scroll down to the QoS Section.

Figure 17 Defining Service Parameters

In the List of available services window, scroll down to the QoS Section. If you wish to use a value that is not in the pre-defined list, then select the [edit] hyperlink to the right of the QoS fields,

Figure 18 QoS DiffServ Settings

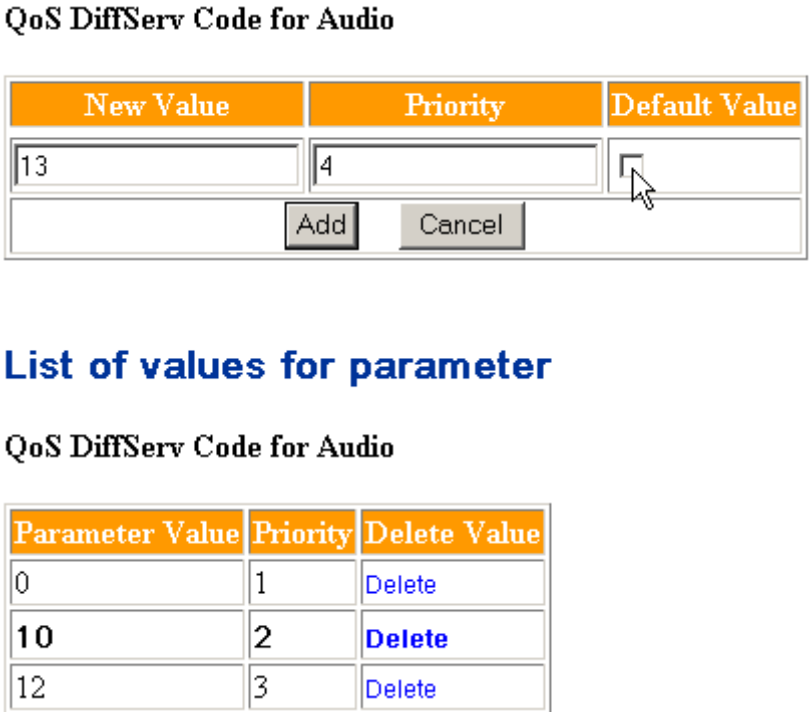


In the picture below the provisioner has chosen to edit the values for the Audio DiffServ value. After selecting edit, the window Add new parameter values for parameter will appear and allow you to add new values, assign priorities to the values, and select if it is the default value.

If you wish to make your new DSCP value the default for all new service packages, check the Default Value checkbox prior to clicking “Add” to add the new value. The default value will be displayed in the values list in bold font.

In the example below, we have chosen to add the value 13 with priority 4, and are about to select this as the default value for audio. If priority 4 already exists, the existing priority 4 value must be deleted before the new value can be added, by selecting the Delete, under the Delete value column.

Figure 19 QoS DiffServ Code for Audio



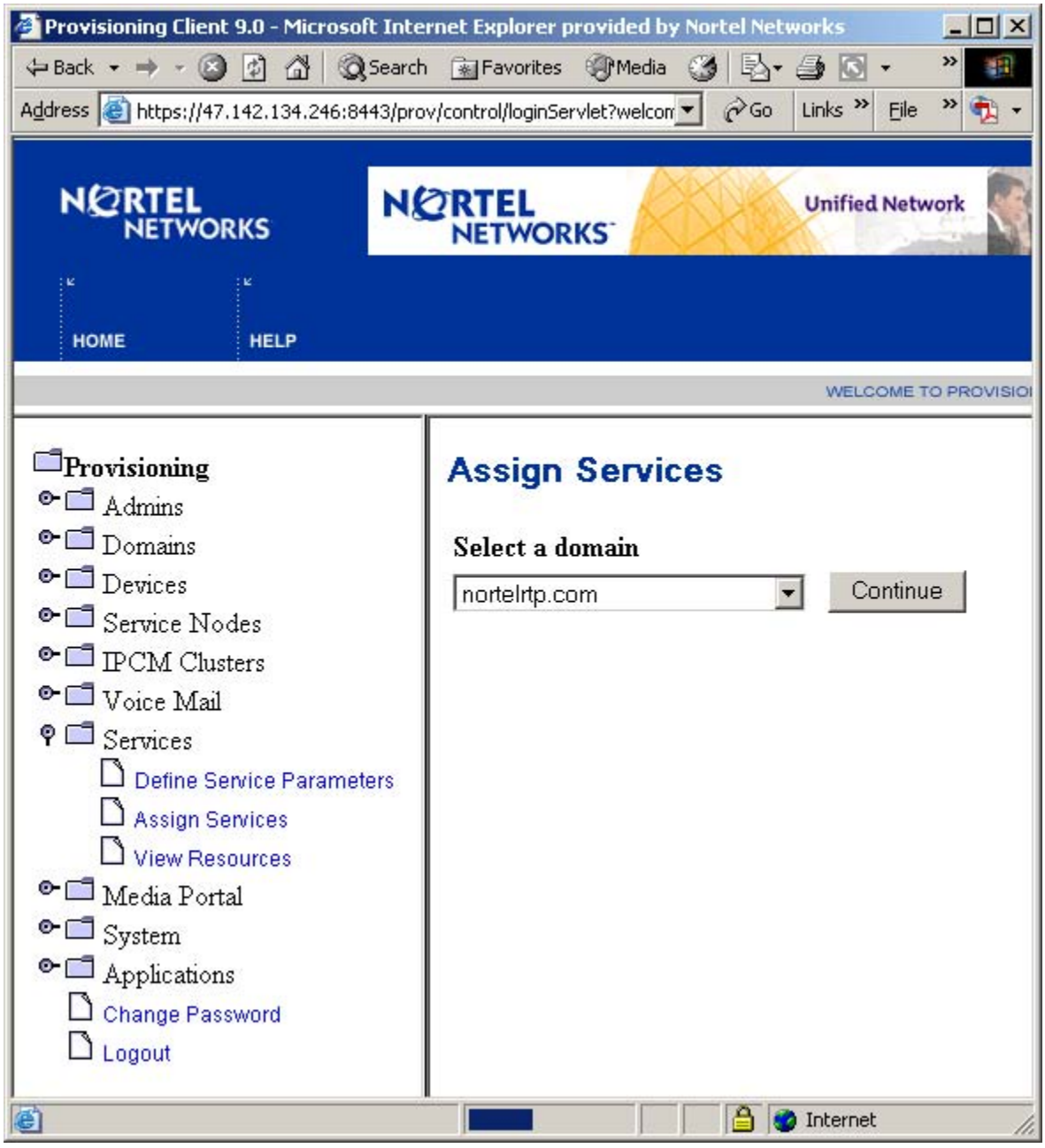
1.1.10 Assigning PCMM Capability to a Subscriber

The ability to provide managed quality of service on a per call / per subscriber level for cable SIP calls is implemented through the use of a new service called PacketCable Multimedia or PCMM. This new service is service package/domain/sub-domain enabled/disabled through the Provisioning Manager on the MCS.

The steps required to assign the PacketCable Multimedia capability on the Provisioning Manager to a subscriber are:

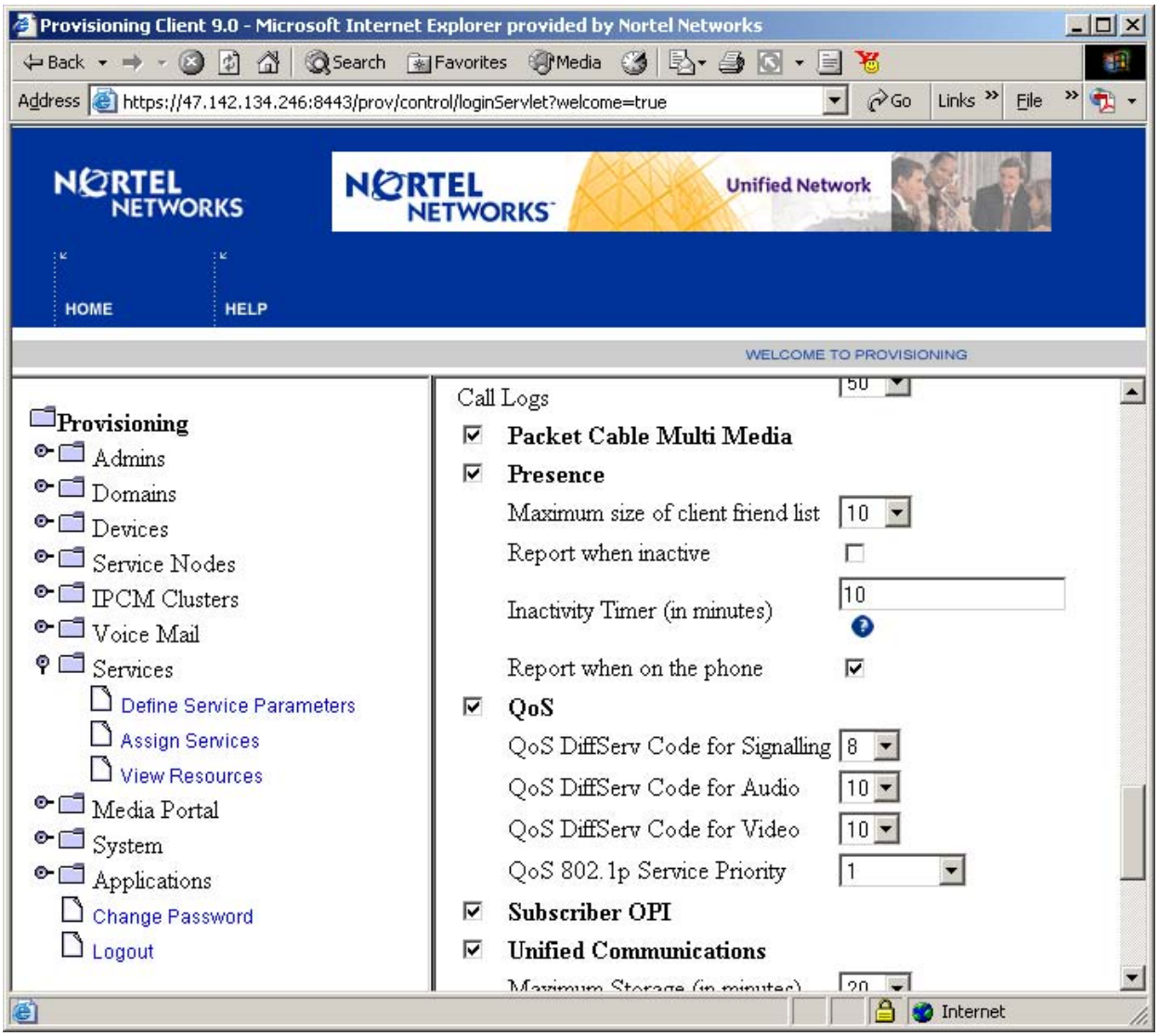
- Create a new domain or sub-domain as desired for PCMM subscribers.
- Open the MCS Provisioning Client, expand the “Services” item and click on “Assign Services”

Figure 20 Provisioning Client for Services



- Select the domain or sub-domain that you want to assign PCMM capability to from the pull-down box and click “Continue” and you will see the list of services will show up in the right-hand frame. Scroll down until you see the “PacketCable Multimedia” checkbox. Check the box and then click “Save” at the bottom of the frame.

Figure 21 Provisioning PacketCable Multimedia

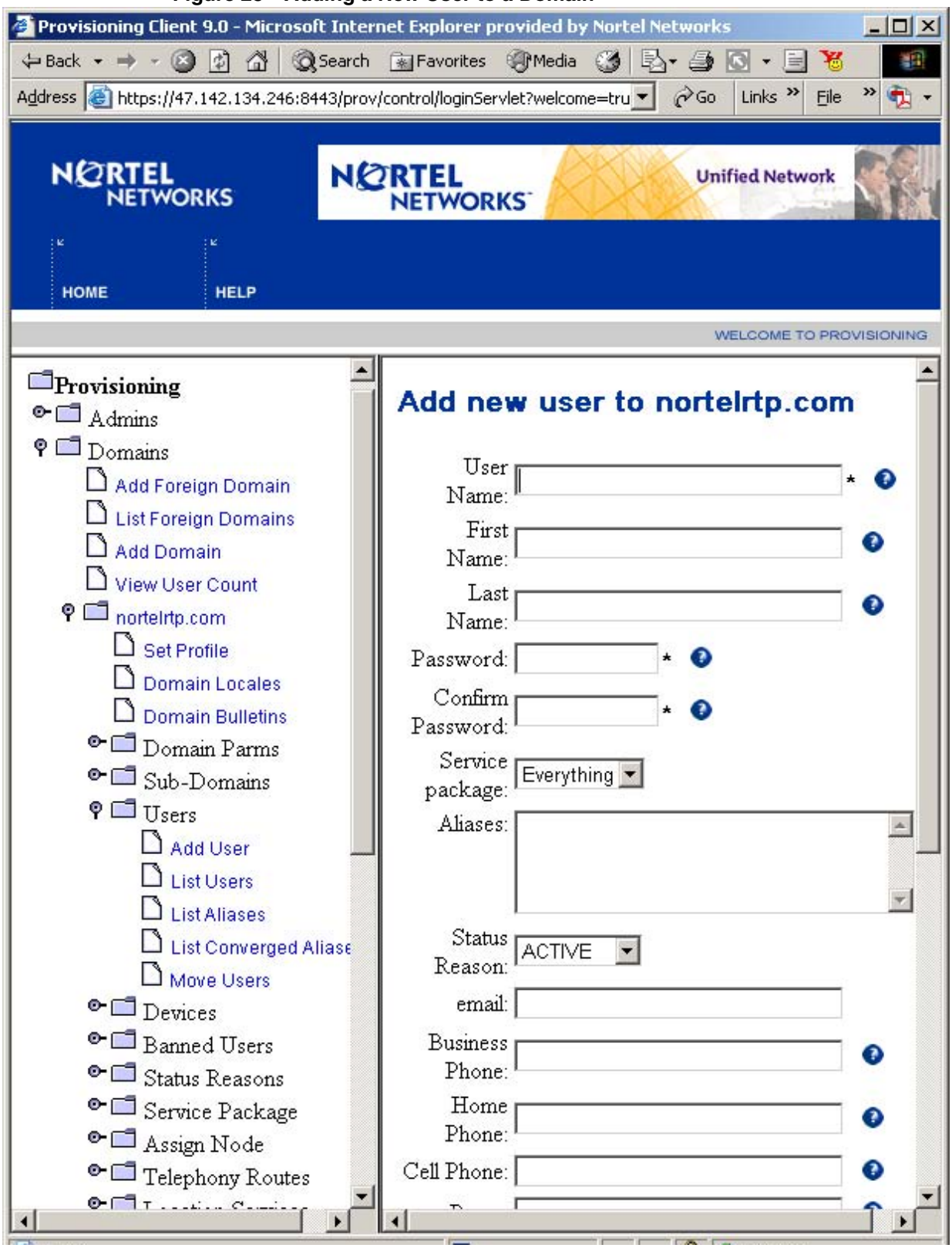


- Expand the desired domain/subdomain icon and create a service package with the PCMM service selected by clicking on “Create Package”.

Figure 22 Creating a new Package for a Domain

- Again under the specific domain/sub-domain, under the ‘Users’ icon select ‘Add User’ icon and fill in the required fields using the service package name created above.

Figure 23 Adding a New User to a Domain



The service is now assigned to a subscriber.

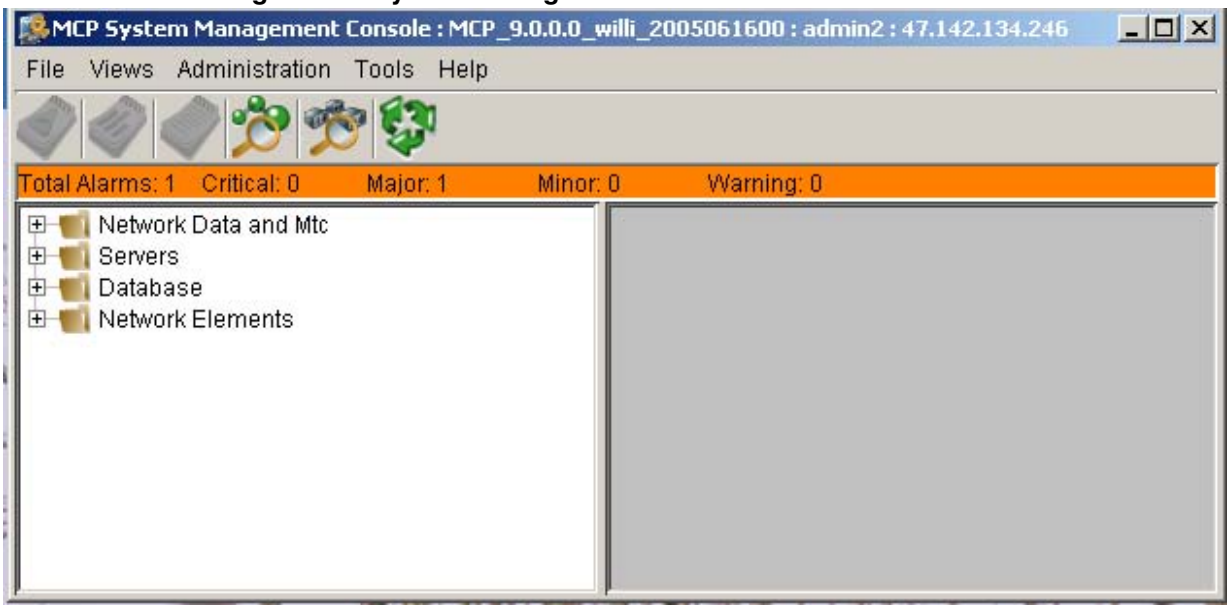
1.1.11 Checking for PCMM Alarms and Logs

As soon as the policy server is configured, the CS2000 will start trying to communicate with it. If this communication fails, a session manager alarm will be raised indicating that the PCMM signaling link cannot be setup. When the PCMM signaling link is down, calls will proceed, but without managed quality of service in the HF/C network.

To check for PCMM alarms, do the following:

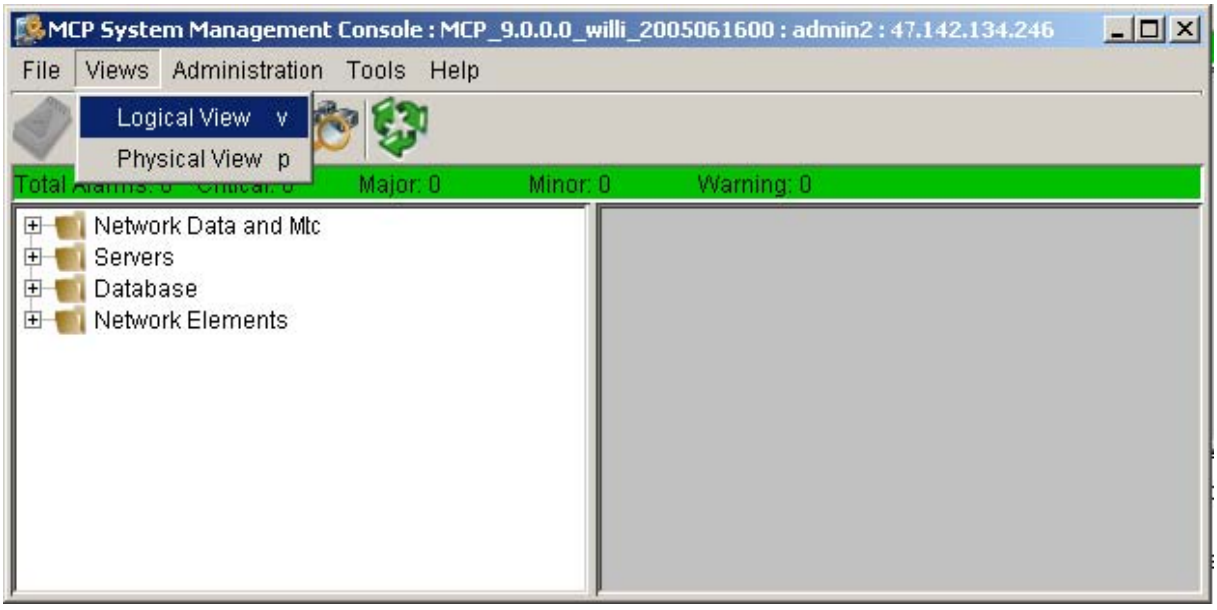
- Login to the System Management Console
- Once you successfully login you will see a screen like the following:

Figure 24 System Management Console



- Note the banner just beneath the tool-bar with a summary of the alarms for the SS-L. If there are any alarms, continue with the next steps to view the alarm details. If no alarms are present, then the PCMM signaling link is operational.
- Start a Logical View of your SS-L as follows:

Figure 25 Starting a Logical View of the MCP System



- This will cause a window like the following to appear:

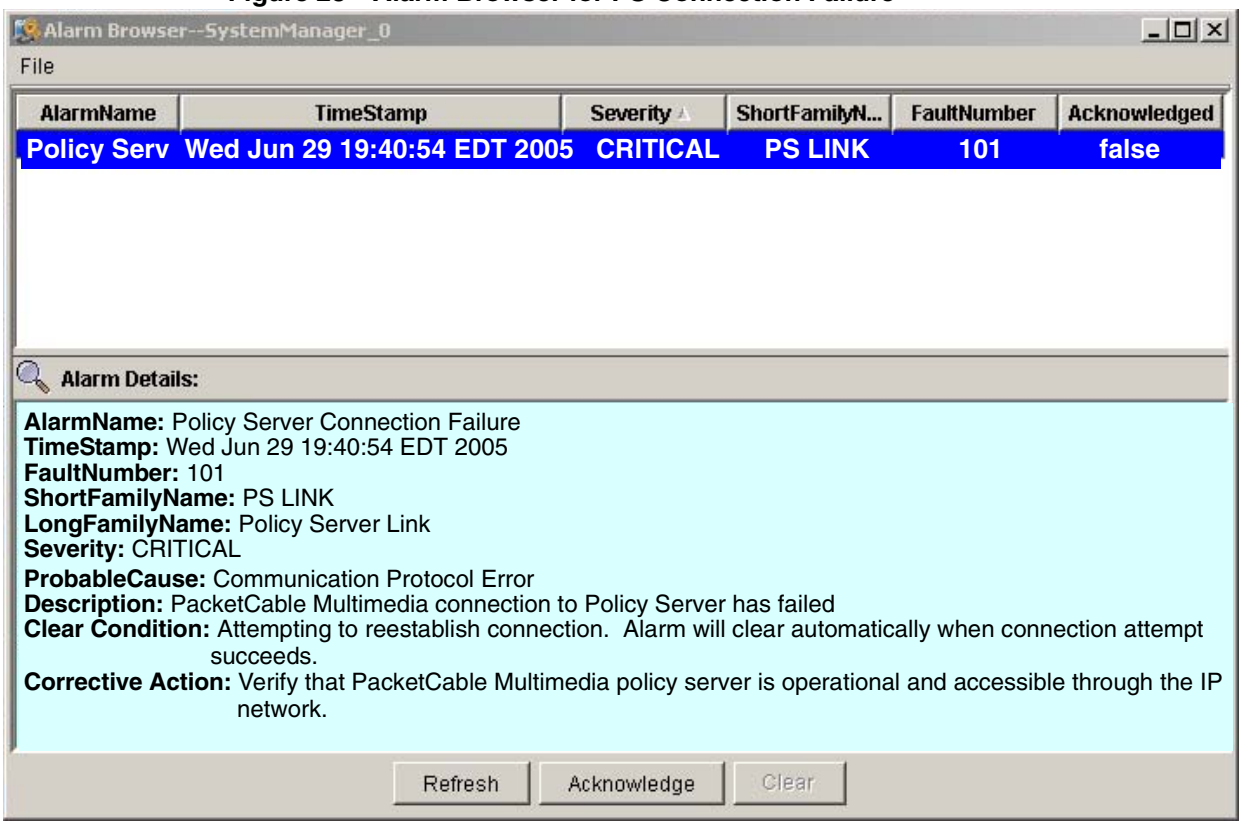
Figure 26 MCP System Logical View

- Expand Session Managers by clicking the “+” to the left of it and highlight a session manager as follows:

Figure 27 Selecting a Session Manager

- Click the button on the lower left to view the alarm browser as follows:

Figure 28 Alarm Browser for PS Connection Failure



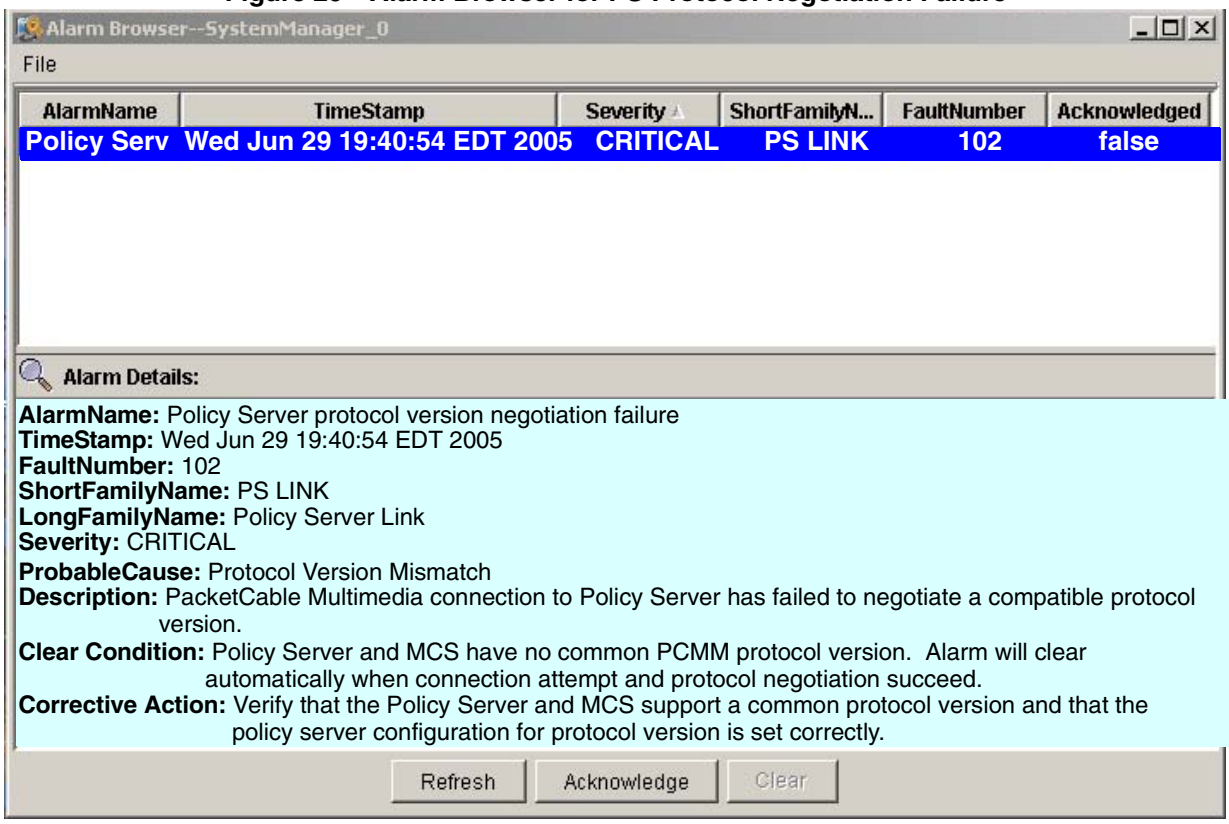
- The alarm view can be manually refreshed by clicking the “Refresh” button.
- Look for alarms with AlarmName “Policy Server Connection Failure” in the upper half of the window. These are PCMM signaling link alarms.

- If you see one, highlight it and the alarm details will be displayed in the lower half of the window.

If you have a PCMM signaling link alarm, all SIP calls from the session manager with the failed PCMM connection will receive best-effort QoS until the problem is resolved. Please refer to the Troubleshooting section of this document for next steps.

Here is an example of the PCMM protocol negotiation alarm that is raised when the PCMM connection fails to come up due to protocol negotiation failure.

Figure 29 Alarm Browser for PS Protocol Negotiation Failure



Following is a summary of all the PCMM alarms and the conditions upon which they are asserted and cleared.

Table 1: PCMM Alarm Conditions

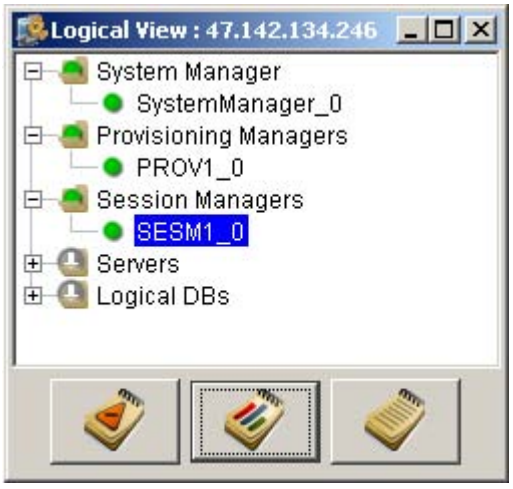
Alarm Name	Severity	Assert	Clear
Policy Server Connection Failure	Critical	Connection drop TCP-layer connection failure Initialization sequence failure other than protocol negotiation	Successful completion of initialization sequence. Deletion of PS from configuration database System or unit shutdown PCMM disabled
Policy Server Protocol Version Negotiation Failure	Critical	Protocol version negotiation failure	Successful completion of protocol negotiation.
PCMM Partial Configuration	Minor	First call to use a policy server for which the session manager AMIDs have not been configured.	Session manager AMIDs successfully configured.

1.1.12 Viewing Operational Measurements

There are a number of operational measurements associated with PCMM. To view PCMM OMs follow this procedure:

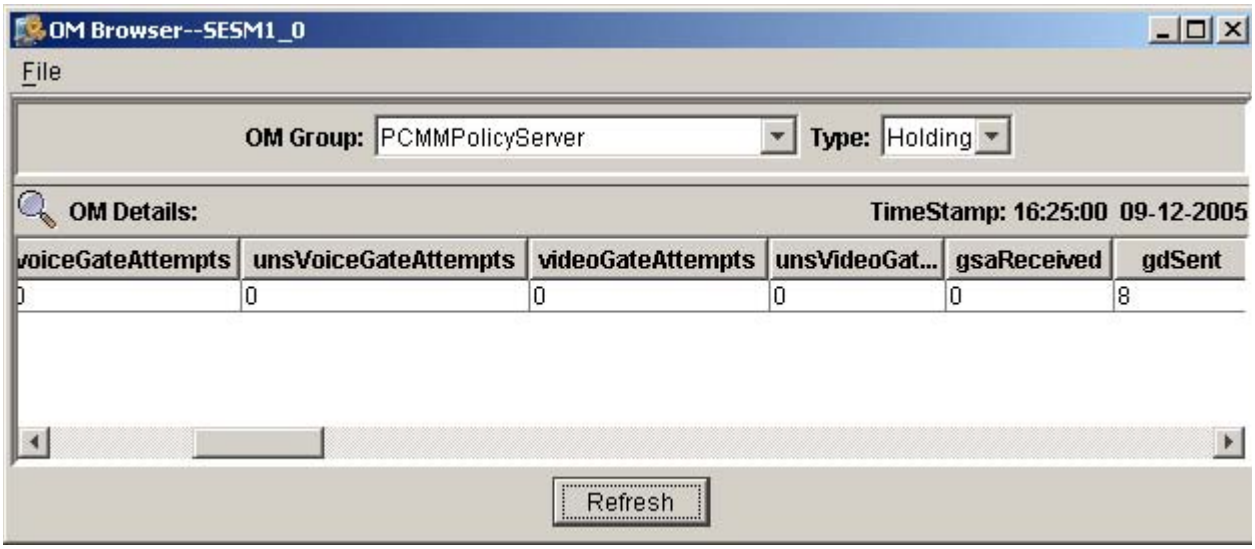
- Pull up the logical view of the MCS as follows:
- Highlight the session manager that you are interested in:

Figure 30 MCP System Logical View



- Click the center button at the bottom of the Logical View window to bring up the OM browser. You will see a window like the following:

Figure 31 Session Manager OM Browser Example



- From the OM Group pull-down menu, select “PCMMAggregate” to access the session manager-wide PCMM OMs. PCMM Aggregate OMs indicate usage of resources that are not specific to any particular policy server.
- Select “PCMMPolicyServer” to access the per-policy server PCMM OMs.

The following tables describe the PCMM operational measurements.

Table 2: PCMM Aggregate Operational Measurements

OM Name	Description
incomingMsgQHighWater	When incoming PCMM signaling messages arrive at the session server they are queued for processing. This OM indicates thehighest percentage used for the incoming PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported. If this queue gets above ~90%, it may indicate a problem with the PCMM. Please contact your next level of support for assistance.
transactionQHighWater	When the session server sends PCMM messages, the outgoing messages are queued for processing. This OM indicates the highest percentage used for the outgoing PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported. If this queue gets above ~90%, it may indicate a problem with the PCMM. Please contact your next level of support for assistance.
outstandingQHighWater	After the session server sends a PCMM message to the policy server for processing, the message is held in the outstanding transaction queue until a response is received (or until the transaction times out). This OM indicates the highest percentage used for the outstanding PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported. If this queue fills up, the oldest outstanding transactions will be removed to make room for newer transactions. This queue can fill up if the policy server is not responding or is responding slowly.
voiceGateAttempts	Total number of PCMM voice half calls processed across all policy servers connected to this session server.
unsVoiceGateAttempts	Total number of unsuccessful PCMM voice half calls processed. There are a number of reasons that a half call might fail to get managed QoS. These include: internal resource errors, no response to transaction, COPS connection down, Gate-Set-Err received from the policy server, etc. Calls that fail to get managed QoS receive best-effort QoS.
unsupCodecVoiceGateAttempts	Total number of PCMM voice half calls with an SDP containing at least one codec for which bandwidth could not be calculated. In order to reserve and commit bandwidth for a call, a mapping must be made between the codec and the flow-spec describing the network resources required. If this mapping fails, then the call might not get optimal bandwidth for managed QoS.

Table 2: PCMM Aggregate Operational Measurements

OM Name	Description
videoGateAttempts	Total number of PCMM video half calls processed across all policy servers connected to this session server.
unsVideoGateAttempts	Total number of unsuccessful PCMM video half calls processed. There are a number of reasons that a half call might fail to get managed QoS. These include: internal resource errors, no response to transaction, COPS connection down, Gate-Set-Err received from the policy server, etc. Calls that fail to get managed QoS receive best-effort QoS.
unsupCodecVideoGateAttempts	Total number of PCMM video half calls with an SDP containing at least one codec for which bandwidth could not be calculated. In order to reserve and commit bandwidth for a call, a mapping must be made between the codec and the flow-spec describing the network resources required. If this mapping fails, then the call might not get optimal bandwidth for managed QoS.
outstandingDiscStale	The number of transactions that were discarded because no response was received from the policy server or because the outstanding transaction queue was full and the oldest transaction waiting for a response was removed to make room for a new transaction.
unkMediaGateAttempts	The number of PCMM gate attempts that could not be processed because the media type was unknown (i.e. not voice, video, or image). Calls that fail to get managed QoS receive best-effort QoS.

Table 3: PCMM Policy Server Operational Measurements

OM Name	Description
numInitializations	Number of times the policy server COPS connection successfully completed the PCMM initialization sequence.
cnxPSDrop	Number of times the policy server gracefully closed the COPS TCP connection (i.e. in a way that caused a TCP FIN message to be sent from the policy server to the session server).
cnxDropProtTimeout	Number of times the connection was dropped by the session server due to lack of PCMM response from the policy server. This could be caused by failure of the session server to receive keep-alive messages or connection initialization sequence messages from the policy server (either because the policy server never sent them or the network prevented them from arriving).

Table 3: PCMM Policy Server Operational Measurements

OM Name	Description
tcpSendFail	Number of times that PCMM messages had to be discarded due to the outgoing TCP buffer being full. Normally this happens if the policy server is not keeping up with the rate of messages being sent from the MCS. TCP send failures can also occur if the network quality is poor, causing a lot of retransmissions.
transDiscLinkDown	Number of PCMM transactions that were discarded due to the PCMM signaling link being down. Since we cannot predict how long a PCMM signaling link might be down, transactions are discarded until the connection is restored. Half-calls whose PCMM transactions are discarded will get "best-effort" quality of service.
transDiscStale	Number of PCMM transactions that were discarded because no response was received from the policy server for more than seven seconds. Or, if the outstanding transaction queue is full, the number of oldest transactions that were discarded to make room for new outstanding transactions.
voiceGateAttempts	Total number of PCMM voice half calls processed for this policy server.
unsVoiceGateAttempts	Total number of unsuccessful PCMM voice half calls processed. This number includes unsuccessful voice calls for all possible reasons.
videoGateAttempts	Total number of PCMM video half calls processed for this policy server.
unsVideoGateAttempts	Total number of unsuccessful PCMM video half calls processed. This number includes unsuccessful video calls for all possible reasons.
gsaReceived	Total number of Gate-Set-Ack messages received from the policy server.
gdSent	Total number of Gate-Delete messages sent to the policy server.
upVoiceGSEReceived	Total number of Gate-Set-Err messages received from the policy server for upstream voice gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
upVoiceGSENoResources	Number of Gate-Set-Err messages for upstream voice gates with error code 1 - Insufficient Resources
upVoiceGSEUnkGateId	Number of Gate-Set-Err messages for upstream voice gates with error code 2 - Unknown GateID

Table 3: PCMM Policy Server Operational Measurements

OM Name	Description
upVoiceGSEOther	Number of Gate-Set-Err messages for upstream voice gates with error code 127 - Other, Unspecified Error
dnVoiceGSEReceived	Total number of Gate-Set-Err messages received from the policy server for downstream voice gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
dnVoiceGSENoResources	Number of Gate-Set-Err messages for downstream voice gates with error code 1 - Insufficient Resources
dnVoiceGSEUnkGateId	Number of Gate-Set-Err messages for downstream voice gates with error code 2 - Unknown GateID
dnVoiceGSEOther	Number of Gate-Set-Err messages for downstream voice gates with error code 127 - Other, Unspecified Error
gseInvSubscr	Number of Gate-Set-Err messages for voice and video, upstream and downstream gates with error code 13 - Invalid Subscriber ID
gseInvAMID	Number of Gate-Set-Err messages for voice and video, upstream and downstream gates with error code 14 - Unauthorized AMID
upVideoGSEReceived	Total number of Gate-Set-Err messages received from the policy server for upstream video gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
upVideoGSENoResources	Number of Gate-Set-Err messages for upstream video gates with error code 1 - Insufficient Resources
upVideoGSEUnkGateId	Number of Gate-Set-Err messages for upstream video gates with error code 2 - Unknown GateID
upVideoGSEOther	Number of Gate-Set-Err messages for upstream video gates with error code 127 - Other, Unspecified Error
dnVideoGSEReceived	Total number of Gate-Set-Err messages received from the policy server for downstream video gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
dnVideoGSENoResources	Number of Gate-Set-Err messages for downstream video gates with error code 1 - Insufficient Resources
dnVideoGSEUnkGateId	Number of Gate-Set-Err messages for downstream video gates with error code 2 - Unknown GateID
dnVideoGSEOther	Number of Gate-Set-Err messages for downstream video gates with error code 127 - Other, Unspecified Error

Table 3: PCMM Policy Server Operational Measurements

OM Name	Description
grsClose	Total number of Gate-Report-State messages received indicating that a gate was closed by the CMTS for all reasons.
grsCloseResReassign	Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 1 - reservation reassignment.
grsCloseMacLayer	Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 2 - lack of DOCSIS MAC-Layer responses
grsCloseT1	PCMM timer T1 specifies the number of seconds a PCMM gate can be authorized but not reserved. This OM indicates the number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 3 - timer T1 expiration
grsCloseT2	PCMM timer T2 specifies the number of seconds a PCMM gate must hold bandwidth reserved in excess of what was committed. Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 4 - timer T2 expiration
grsCloseResMaint	Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 6 - lack of reservation maintenance
grsCloseT4	Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 8 - timer T4 expiration.
grsNotif	Total number of Gate-Report-State messages received indicating a change of gate state (for any reason) that did not result in the gate being closed.
grsNotifT3	Number of Gate-Report-State messages received indicating that a gate was transitioned to the Committed-Recovery state by the CMTS due to the T3 timer expiring. If the T3 timer expires frequently, you may wish to increase the T3 timer value to a longer duration.

1.1.13 Changing Policy Server Attributes

Some policy server attributes can be changed with no service impact. Other attributes require a re initialization of the PCMM signaling link. The policy server name cannot be changed without deleting and re adding the policy server.

1.1.13.1 Changes requiring a PCMM connection reinitialization

Policy server attributes that define the address of the policy server or are communicated to the policy server only when the connection is started require

that the connection be re initialized. Changing these fields will cause the PCMM signaling connection between the MCS and the policy server to be dropped and immediately reestablished. Calls being setup during the short interval when the PCMM signaling link is down will proceed, but with best-effort quality of service. Changing any of the following fields will cause a PCMM connection reinitialization.

- Policy Server Address
- Policy Server Port
- Protocol Version
- Keep-Alive Timer

See section 1.1.7 on page 1805 for a description of policy server attributes.

When the "Apply" button is clicked after changing any of these fields, a warning dialog will be displayed indicating the consequences of changing these fields and asking you to confirm the operation. Clicking "Yes" will save the changes and reinitialize the connection. Clicking "No" will revert to the prior values.

1.1.13.2 Changes that take effect immediately

The remaining policy server fields can be changed without bouncing the policy server connection. They are:

- Timer T1
- Timer T2
- Timer T3
- Timer T4

See section 1.1.7 on page 1805 for a description of the PCMM protocol timers T1 through T4.

These values will be used for the next call that is started after the "Apply" button is clicked to save the changes.

1.1.14 Removing PCMM Capability from a Subscriber

There are two ways to remove PCMM capability from a subscriber:

- Change the service package that the subscriber is assigned to so that it no longer has the PacketCable Multimedia box checked.
- Change the subscriber to use an existing service package that does not have the PacketCable Multimedia capability assigned.

1.1.15 Deleting a Policy Server and its associated AMIDs

A policy server may be deleted using the MCS System Management Console. Before a policy server can be deleted, however, the AMIDs associated with the policy server on all active session managers must be deleted first. A window displaying an error message will appear if an attempt is made to delete a policy server when an AMID is still provisioned against that policy server on any active session manager.

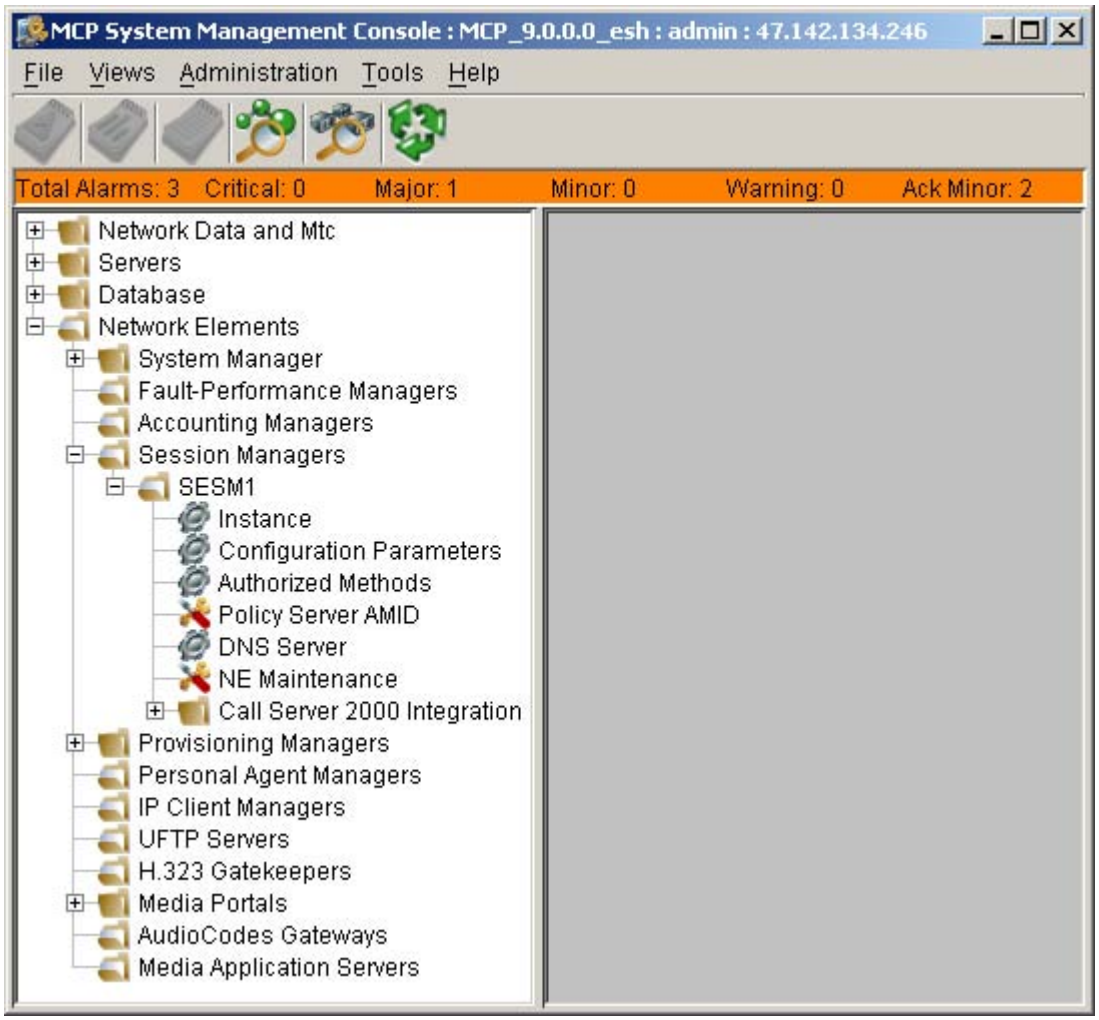
In order to delete the policy server:

- Expand the “Network Elements” and “Session Managers” items

Figure 32 System Management Console for Network Elements

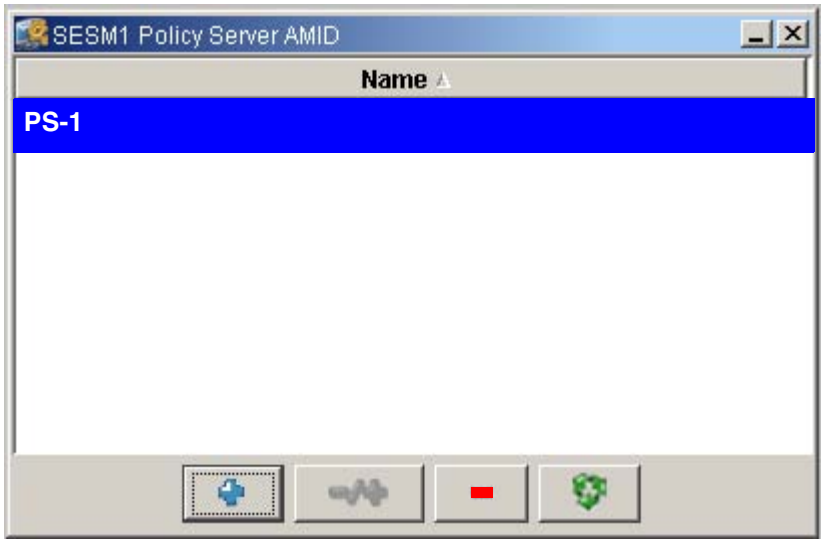
- Select and expand each active session manager

Figure 33 System Management Console for Session Managers



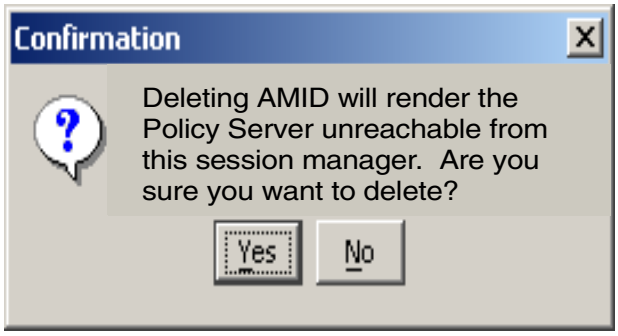
- Click Policy Server AMID and a window will appear showing the assigned policy servers.

Figure 34 Session Manager AMID Dialogue



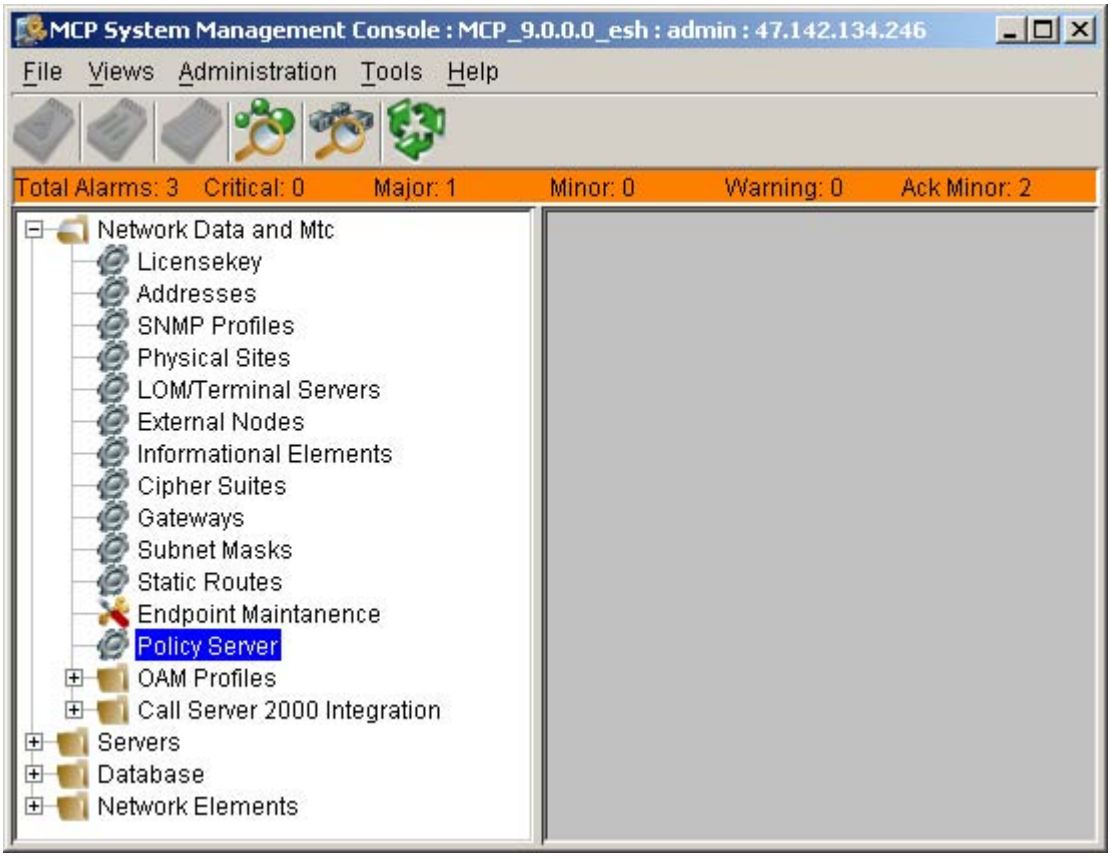
- Highlight the policy server to be deleted <<and the AMIDs will be displayed???>>
- Click the "-" minus button and click "Apply" to remove the AMIDs from that session manager
- A warning dialogue will appear indicating that removal of AMIDs will render the connection from this session manager to the policy server unusable. Once the AMID has been removed and prior to removal of the policy server, a minor alarm will appear for the session managers that no longer have AMIDs (see section 1.1.11 on page 1820). This alarm indicates that a partial configuration is present and will clear once the policy server is deleted.

Figure 35 AMID Delete Confirmation



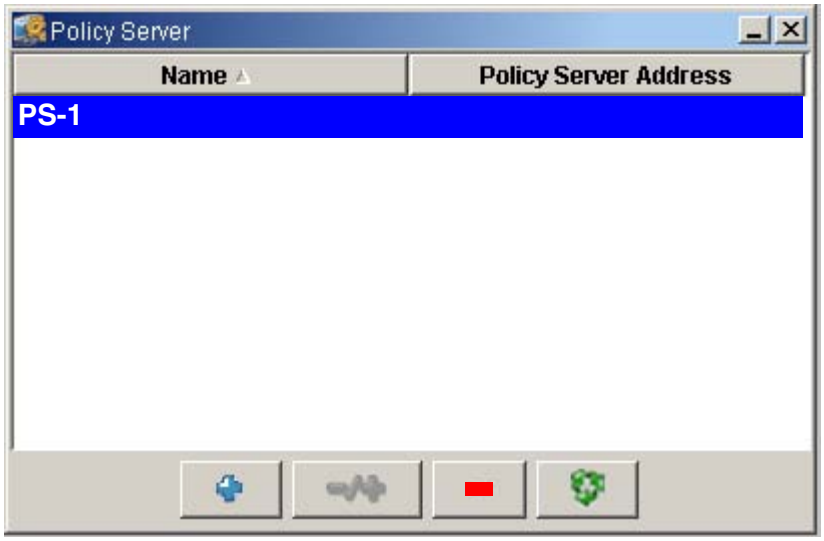
- Repeat above to remove the AMIDs from all active session managers.
- Now that all associated AMIDs have been removed, expand the "Network Data and Mtc" item

Figure 36 System Management for Policy Servers



- Select the Policy Server icon, a window will appear showing the configured policy servers.

Figure 37 Policy Server Dialogue



- Highlight the policy server to be deleted and click the "-" (minus) button and click "Apply" to delete the policy server.

WARNING: Deletion of a Policy Server will cause all new PCMM capable calls to receive best-effort quality of service within the cable network.

1.1.16 Understanding Session Manager Failover

The session manager can be configured for redundancy, thus enabling failover if something goes wrong. This section describes what happens to calls in the event of a failover. A warm failover is when the active unit fails and the standby unit is up and ready to become the active unit. A cold failover happens when there is no standby unit or when the standby unit is not ready to become active.

1.1.16.1 Warm

A stable subscriber session and its managed QoS will survive a warm failover. Subscribers on calls in the conversation phase at the time of the warm failover will not notice that a failover has occurred.

Calls that are held or for any reason have no media packets flowing at the time of the session manager failover may lose their managed QoS if the T3 and T4 timers subsequently expire. The held calls will not be torn down, but they may lose their managed QoS and continue using best-effort QoS.

Calls in the setup phase at the time of the warm failover are not guaranteed to succeed. If they do succeed, they may get only best-effort QoS.

1.1.16.2 Cold

All calls are torn down on cold failover.

1.1.17 Troubleshooting

The following table lists the more common failure modes and gives advice on resolving the problem. In general, always check for alarms first. If an alarm is present, look for logs generated around the same time the alarm was

generated. Also look at PCMM OMs to determine if there are any unexpected peg-counts.

Table 4: PCMM Troubleshooting

Condition	Possible Causes and Corrective Actions
Policy Server connection failure alarm	Incorrect policy server IP address or port. Verify that the policy server IP address and port configuration are correct. Network problem between session manager and policy server. Verify that you can ping the policy server from the session manager. Make sure any firewalls are configured to allow TCP packets between the session manager and policy server. Policy server not running or not configured correctly. Verify that your policy server is operating correctly.
Policy Server protocol version negotiation failure alarm	Protocol version misconfigured. Verify that your PCMM protocol version number is set to the highest protocol that you want to allow for the PCMM connection. For this initial release, the protocol version should be set to 1.0. Policy server is running incompatible software. Verify that the policy server supports the protocol version for which you have configured the CS2000 PCMM protocol version.
Poor voice or video quality	PCMM signaling connection is down. Verify that you don't have any Policy Server alarms. The audio or video codec being use for the call is not supported for PCMM. Calls not using G.711 or G.729 for voice, or H.263 or DIVX for video do not receive managed QoS. Other PCMM signaling problems are occurring. Check your PCMM operational measurements (OMs) to see if any unexpected peg counts are present. Please refer to the OM section of this document for a complete description of all PCMM OMs. Calls active at the time of a failover can lose their managed QoS if they are subsequently placed on hold (no media packets flowing) for longer than the combined length of the T3 and T4 timers. (The T3 and T4 timers are configured against the policy server in the MCP System Management Console.)

1.2 MCP Provisioning Client PCMM Help Information

In lieu of additional PCMM help information in the MCP Provisioing Client the following provides a description PCMM service.

Service Name : PCMM

Parameters : None

Desciption: When assigned to a user thru a service package, this parameter in conjunction with a configured Policy Server will provide the user the ability to receive managed quality of service for all voice and or video sessions. The service is provisioned on a service package level for domains or sub-domains--see the MCS Provisioning Client Help information under “Defining and Assigning Services” and “Assigning Services and Creating Service Packages”.

1.3 Hardware Requirements or Dependencies

In order to implement the PCMM feature, the MSO needs to have cable network elements that are not supplied by Nortel. These cable network elements include cable modems, CMTSs, and a policy server.

There are no additional CS2000 hardware elements required for PCMM other than what was necessary for a basic SIP lines deployment.

Nortel has tested PCMM with all endpoints supported by the CS2000 SIP lines program, including the following SIP clients:

- Nortel Networks PC Client
- Cisco 7960 SIP phone

1.4 Software Requirements or Dependencies

The policy server and CMTSs in the cable network must support PacketCable Multimedia specification PKT-SP-MM-I02-040930. The cable modems must support DOCSIS 1.1.

The CS2000 components must be at SN09 including the MCS software for PCMM.

1.5 Limitations and restrictions

This initial release of the PCMM service has the following limitations:

- Single policy server per CS2000
- Emergency calls are not distinguished from normal calls with respect to PCMM
- No support for IPSec on the PCMM signaling connection

- No PCMM marking in billing records
- Support for audio codecs G.711 and G.729 only
- Support for video codecs H.263 and DIVX only
- Inability to disable DSCP overwrite
- DSCP must be the same for upstream and downstream flows
- PCMM signaling only for committed state

The following items indicate *optional* protocol elements that are not included in this release of the PCMM service:

- No support for optional Time Based Usage Limits
- No support for optional Volume Based Usage Limits
- PCMM signaling only for committed state
- Only Flow-Spec Traffic-Profile supported
- No support for optional Opaque-Data
- No support for optional state synchronization with policy server
- Single classifier based on media source and destination IP addresses and ports (no classification based on DSCP)

1.6 Interactions

The PCMM feature sets up managed quality of service for SIP line calls originating from or terminating to the cable network. PCMM operates on a half-call basis. This means that PCMM signaling and managed QoS happen only for the half of the call that is in the cable network. For example, an on-net to off-net call will only do PCMM signaling for the originating line half of the call. The trunk half of the call is not touched by PCMM.

The PCMM service works for all call types supported by the CS2000 SIP lines program.

1.6.1 Basic Call

The PCMM feature attempts to set up managed quality of service when the SDP information is known for both of the media endpoints (originating and terminating). If PCMM fails to set up managed QoS, the call proceeds with "best-effort" QoS. Calls will never fail due to PCMM, but it is possible under some error conditions that a call might not receive managed QoS.

1.6.2 Codec Support

The following codecs and packetization rates are supported:

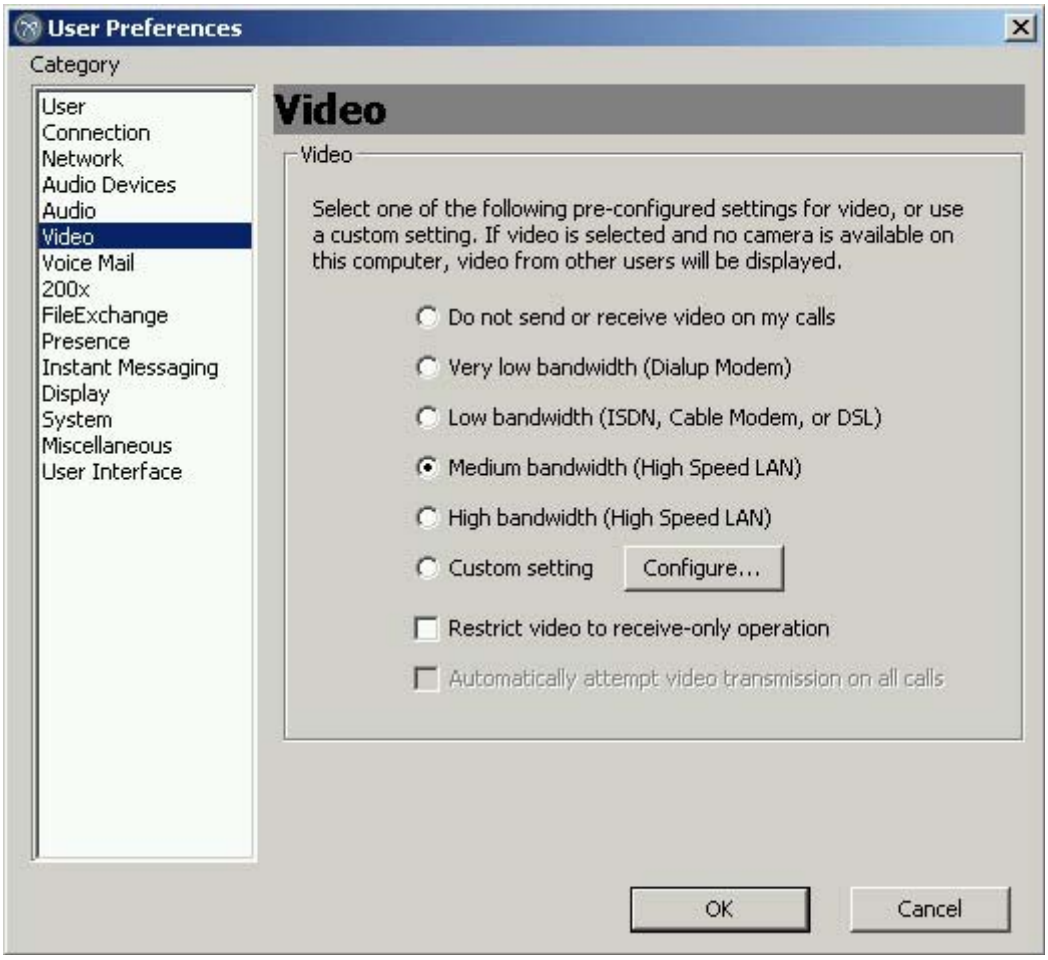
Table 5: PCMM Supported Codec/ptime Combinations

Codec	ptime
PCMU	10 20 30
PCMA	10 20 30
G.729A	10 20 30
H.263	
DIVX	

1.6.3 Supported Video Configuration using Multimedia PC Client

The Nortel Networks Multimedia PC Client provides extensive flexibility in the configuration of video parameters. Not all configurations cans be supported with the PacketCable Multimedia capability.

Figure 38 Multimedia PC Client Video Preferences



There are 4 preset configurations optimized for different bandwidth usage from “very low bandwidth” to “high bandwidth”. Each of these settings can be used with the PacketCable Multimedia capability.

The “custom setting” is not supported for use with the PacketCable Multimedia capability.

1.7 PacketCable Requirements Compliance

The following table lists the PacketCable requirements from PKT-SP-MM-I02-040930 that apply to an application manager and indicates Nortel CS2000 compliance.

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15004	The AMID MUST be a globally unique value assigned to the Application Manager by the service provider.	Yes	MUST	
MMREQ15005	The Application Manager MUST use the assigned AMID in all its interactions with Policy Servers.	Yes	MUST	
MMREQ15011	The Policy Server or Application Manager MUST define the Traffic Profile for a Gate using one of the following: (1) the FlowSpec, (2) DOCSIS Service Class Names, or (3) DOCSIS-Specific Parameters.	Yes	MUST	
MMREQ15014	There MUST be at least one set of Traffic Profile parameters specified when the Gate is first being installed.	Yes	MUST	
MMREQ15017	A controlled load service MUST contain only the TSpec token bucket parameters, and not the RSpec.	Yes	MUST	
MMREQ15018	A guaranteed service MUST contain both the TSpec and the RSpec.	Yes	MUST	
MMREQ15022	If the Application Manager wishes to use this third way of defining a Traffic Profile, it MUST include an object containing the DOCSIS Specific Parameters.	Yes	MUST	
MMREQ15041	To reserve resources, the Policy Server MUST issue a subsequent Gate-Set message with a Traffic Profile that includes the Reserved Envelope.	Yes	MUST	
MMREQ15051	The Reserved envelope MUST always be less than or equal to the Authorized envelope.	Yes	MUST	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15053	However, all requests to modify Authorized, Reserved or Committed envelopes MUST conform to the general rule:	Yes	MUST	
MMREQ15061	In the Committed state, the Application Manager MAY delete the Gate by issuing a Gate-Delete message to the Policy Server, which in turn MUST relay the message onto the CMTS.	Yes	MUST	
MMREQ15073	The Application Manager MUST either refresh the policy by issuing a Gate-Set message, or remove the Gate by issuing a Gate-Delete message.	Yes	MUST	
MMREQ15093	In contrast, PacketCable Multimedia implementations MUST use the TransactionID object to match responses with requests and SHOULD send RPT messages as soon as they are ready.	Yes	MUST	
MMREQ15095	Protocol messages for Gate Control MUST be transported within the COPS protocol messages.	Yes	MUST	
MMREQ15096	The PDP and PEP MUST establish and use a TCP connection for communication, and utilize the mechanisms specified in [17] to secure the communication path.	Yes	MUST	
MMREQ15097	The Application Manager, Policy Server and CMTS MUST use the COPS Common Message format as defined below as the message format for all message exchanges.	Yes	MUST	
MMREQ15098	This field MUST be set to 1.	Yes	MUST	
MMREQ15099	, a solicited decision sent in response to a request) this flag MUST be set to 1.	Yes	MUST	
MMREQ15100	, an unsolicited decision) the flag MUST NOT be set (value = 0).	Yes	MUST	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15101	In keeping with the DQoS model, the first Decision message sent in response to a Request message is a solicited response and its solicited message flag MUST be set.	Yes	MUST	
MMREQ15102	All other Decision messages are unsolicited and the solicited message flag MUST be cleared.	Yes	MUST	
MMREQ15103	All other flags MUST be set to zero.	Yes	MUST	
MMREQ15104	For PacketCable Multimedia use, the Client-Type MUST be set to PacketCable Multimedia client (0x800A).	Yes	MUST	
MMREQ15105	For Keep-Alive messages (Op-code = 9) the Client-Type MUST be set to zero, as the KA is used for connection verification rather than per-client session verification.	Yes	MUST	
MMREQ15106	Messages MUST be aligned on 4-byte boundaries, so the length MUST be a multiple of four.	Yes	MUST	
MMREQ15107	All the objects MUST conform to the same object format where each object consists of one or more 4-byte words with a four-octet header, using the following format.	Yes	MUST	
MMREQ15108	Length is a 2-byte unsigned integer value that MUST give the number of bytes (including the header) that compose the object.	Yes	MUST	
MMREQ15109	If the original length in octets is not a multiple of four, padding MUST be added to the end of the object so that it is aligned to the next 4-byte boundary.	Yes	MUST	
MMREQ15110	Each of these objects MUST conform to the format and rules relating to the individual object as defined in[10].	Yes	MUST	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15111	These objects MUST be placed inside a Decision object, C-Num = 6, C-Type = 4 (Client Specific Decision Data) when carried from PDP to PEP in a Decision message.	Yes	MUST	
MMREQ15113	S-Num and S-Type MUST be one octet.	Yes	MUST	
MMREQ15114	The COPS Length field MUST be two octets.	Yes	MUST	
MMREQ15115	The TransactionID MUST also contain the command type that identifies the action to be taken or response.	Yes	MUST	
MMREQ15116	The TransactionID Object MUST con-form to the following format.	Yes	MUST	
MMREQ15118	Gate Command Type is a 2-byte unsigned integer value which identifies the Gate Control message type and MUST be one of the following:	Yes	MUST	
MMREQ15119	The Application Manager MUST include this object in all messages it issues to the Policy Server.	Yes	MUST	
MMREQ15122	The AMID object MUST conform to the following format.	Yes	MUST	
MMREQ15123	The SubscriberID object MUST con-form to the following format.	Yes	MUST	
MMREQ15126	The GateID object MUST conform to the following format.	Yes	MUST	
MMREQ15127	The GateSpec object MUST conform to the following format.	Yes	MUST	
MMREQ15128	Bit 0: direction bit, MUST be either zero for a downstream Gate, or one for an upstream Gate.	Yes	MUST	
MMREQ15129	Bit 1: DSCP/TOS enable bit, MUST be either zero to disable DSCP overwrite, or one to enable.	Yes	MUST	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15130	Bits 2-7: reserved, MUST be zero.	Yes	MUST	
MMREQ15139	The Classifier object MUST conform to the following format.	Yes	MUST	
MMREQ15140	Source IP Address and Destination IP Address MUST be a pair of 4-octet IPv4 addresses, or zero for no match (i.e.,	Yes	MUST	
MMREQ15141	Source Port and Destination Port MUST be a pair of 2-byte unsigned integer values, or zero for no match	Yes	MUST	
MMREQ15142	Protocol ID MUST conform to section C.2.1.5.2 of [1], or zero for no match.	Yes	MUST	
MMREQ15143	DSCP/TOS Field is a 1-byte bit field which MUST conform to the following alternative structures:	Yes	MUST	
MMREQ15146	Thus, all traffic parameters associated with a given Gate MUST be included in every message that includes a Traf-fic Profile.	Yes	MUST	
MMREQ15147	Only the following values are legal: 001, 011 and 111; the Envelope Field MUST be set to one of these three legal values.	Yes	MUST	
MMREQ15148	Otherwise, the PDP MUST ensure that exactly one set of envelope parameters is included for each of the envelope types that are indicated in the envelope field.	Yes	MUST	
MMREQ15149	The FlowSpec object MUST conform to the following specification:	Yes	MUST	
MMREQ15153	The DOCSIS Service Class Name object MUST conform to the following specification:	Yes	MUST	
MMREQ15154	The Service Class Name is MUST be 2-16 bytes of null-terminated ASCII string.	Yes	MUST	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15155	This name MUST be padded with null bytes to align on a 4-byte boundary.	Yes	MUST	
MMREQ15156	The Best Effort object MUST conform to the following specification:	Yes	MUST	
MMREQ15158	The Non-Real Time Polling object MUST conform to the following specification:	Yes	MUST	
MMREQ15161	The Real-Time Polling object MUST conform to the following specification:	Yes	MUST	
MMREQ15164	The Unsolicited Grant object MUST conform to the following specification:	Yes	MUST	
MMREQ15165	The Unsolicited Grant with Activity Detection object MUST conform to the following specification:	Yes	MUST	
MMREQ15167	The Downstream object MUST conform to the following specification:	Yes	MUST	
MMREQ15170	The Event Generation Info object MUST conform to the following specification:	Yes	MUST	Optional - not used
MMREQ15171	Primary-Record-Keeping-Server-IP-Address is a 4-byte field which MUST contain the IPv4 address of the primary RKS to whom event records are to be sent.	Yes	MUST	Optional - not used
MMREQ15172	Primary-Record-Keeping-Server-Port field is a 2-byte unsigned integer which MUST contain the port number on the primary RKS where event records are to be sent.	Yes	MUST	Optional - not used
MMREQ15173	Secondary-Record-Keeping-Server-IP-Address is a 4-byte field which MUST contain the IPv4 address of the secondary RKS to whom records are to be sent if the primary RKS is unavailable.	Yes	MUST	Optional - not used

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15174	Secondary-Record-Keep-ing-Server-Port is a 2-byte unsigned integer which MUST contain the port number on the secondary RKS where event records are to be sent.	Yes	MUST	Optional - not used
MMREQ15175	Billing-Correlation-ID is a 24-byte field which MUST contain the identi-fier assigned by the AM or PS for all records related to this session.	Yes	MUST	Optional - not used
MMREQ15176	It MUST NOT be used in any other messages.	Yes	MUST	Optional - not used
MMREQ15177	The Volume-Based Usage Limit object MUST conform to the following speci-fication:	Yes	MUST	Optional - not used
MMREQ15178	The Time-Based Usage Limit object MUST conform to the following speci-fication:	Yes	MUST	Optional - not used
MMREQ15180	It MUST NOT be used in any other messages issued by the PDP to the PEP.	Yes	MUST	Optional - not used
MMREQ15198	Messages that perform gate control between the Application Manager and Policy Server are defined and MUST be formatted as follows.	Yes	MUST	
MMREQ15199	Note that messages from the Applica-tion Manager to Policy Server MUST be formatted as COPS Decision mes-sages, and messages from Policy Server to Application Manager MUST be formatted as COPS Report-State messages.	Yes	MUST	
MMREQ15202	For Gate Control command messages, the Context object (C-Num = 2, C-Type = 1) in the COPS Decision message MUST have the R-Type (Request Type Flag) value set to 0x08 (Configuration Request) and the M-Type set to zero.	Yes	MUST	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15203	The Command-Code field in the mandatory Decision-Flags object (C-Num = 6, C-Type = 1) MUST be set to 1 (Install Configuration).	Yes	MUST	
MMREQ15211	Any Application Manager or Policy Server (PDP) with a need to contact a PEP MUST initiate a TCP connection to the PEP on that port.	Yes	MUST	
MMREQ15214	Upon successful receipt of the Client-Open message, the PDP MUST send a Client-Accept message if the protocol version specified in the Version Info object is supported.	Yes	MUST	
MMREQ15215	This message MUST include the Keep-Alive-Timer object, which tells the PEP the maximum interval between Keep-Alive messages.	Yes	MUST	
MMREQ15216	If the protocol version supplied by the PEP is not supported, the PDP MUST send a Client-Close messages with a COPS Error Object specifying error code 4 (Unable to process).	Yes	MUST	
MMREQ15217	After sending the Client-Close, the PDP MUST retain the TCP connection and security association with the PEP so that the PEP can reattempt the COPS initialization without reestablishing the TCP connection and security association.	Yes	MUST	
MMREQ15219	The PDP MUST then send a Client-Close message to the PEP to acknowledge that protocol negotiation has failed.	Yes	MUST	
MMREQ15221	Devices compliant with this specification MUST use a version of 1.0, i.e.	Yes	MUST	
MMREQ15227	Upon receipt of the COPS KA message, the PDP MUST echo a COPS KA message back to the PDP.	Yes	MUST	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15230	All messages from the PDP to the PEP MUST be sent using Client-Specific objects within the Decision object of a COPS Decision message.	Yes	MUST	
MMREQ15233	The Decision messages and Report-State messages MUST contain the same Client-Handle as provided in the initial Request sent by the CMTS when the COPS connection was initiated.	Yes	MUST	
MMREQ15237	The PDP MUST keep track of when KAs are received.	Yes	MUST	
MMREQ15238	If the PDP has not received a KA from the PDP in the time interval specified in [10] or the PDP has not received an error indication from the TCP connection, then the PDP MUST tear down the TCP connection and attempt to re-establish the TCP connection.	Yes	MUST	
MMREQ15239	, Gate-Set, Gate-Info, and Gate-Delete) MUST include (in addition to other mandatory objects) both AMID and SubscriberID objects.	Yes	MUST	
MMREQ15249	At any one point in time, the Committed envelope MUST fit within the Reserved Envelope which MUST fit within the Authorized envelope.	Yes	MUST	
MMREQ15254	For traffic profiles in the form of a Service Class Name, the Service Class Name string MUST exactly match the preexisting Service Class Name on the CMTS.	Yes	MUST	
MMREQ15255	The Gate-Set message MUST contain exactly one GateSpec object, describing one upstream or downstream Gate.	Yes	MUST	
MMREQ15284	: The Application Manager MUST handle received reports.	Yes	MUST	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15285	Thus, the Application Manager MUST enforce the Time-Based Usage Limit of the Gate.	Yes	MUST	Optional - not used
MMREQ15286	Upon receiving the Gate-Set-Ack for a Gate with a Time-Based Usage Limit, the AM MUST start an application timer.	Yes	MUST	Optional - not used
MMREQ15287	When the application timer is equal to the Time-Based Usage Limit, the Application Manager MUST respond by performing one of the following actions:	Yes	MUST	Optional - not used
MMREQ15299	The PDP in response MUST automatically delete any state associated with the PEP when the TCP connection is terminated.	Yes	MUST	
MMREQ15324	If present, this object MUST contain a valid BCID which can be used by the AM, PS, and CMTS to correlate billing information for the flow.	Yes	MUST	Optional - not used
MMREQ15330	The PS MUST include the BCID in the EM header for all subsequently generated Policy Event Messages associated with this request.	Yes	MUST	Optional - not used
MMREQ15332	Also, the PS MUST include the BCID in the Gate-Set message sent to the CMTS.	Yes	MUST	Optional - not used
MMREQ15373	The Application Manager - Policy Server COPS interface MUST be secured using the IPsec ESP protocol, as specified in Section 7.2.1.3.2 of [17].	No	MUST	Planned
MMREQ15374	The key management requirements for this interface MUST comply with Section 7.2.1.4.1 of [17].	No	MUST	Planned

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15375	For this interface, Application Manager MUST comply with all the Gate Controller requirements listed in Sections 7.2.1.3.2 and 7.2.1.4.1 of [17].	No	MUST	Planned
MMREQ15376	The first component of Application Manager's principal name MUST be:	No	MUST	Planned
MMREQ15377	The value of <Sub-System Name> for an Application Manager MUST be the following 2-character string: am.	No	MUST	Planned
MMREQ15381	Guaranteed service MUST contain both the TSpec and the RSpec.	Yes	MUST	
MMREQ15387	The RSpec parameters MUST be specified for a guaranteed service.	Yes	MUST	
MMREQ15389	If the Application Manager/Policy Server wishes to set those Service Flow parameters to something other than the defaults specified by this specification, the Application Manager/Policy Server MUST use either the Service Class Names or the DOCSIS-specific parameterization formats to define the traffic profile.	Yes	MUST	
MMREQ15484	A default value of 64 SHOULD be used if a specific priority value is not required.	Yes	SHOULD	
MMREQ15485	If all of the envelope types that are indicated in the envelope field share a common set of envelope parameters, then the PDP SHOULD ensure that exactly one set of envelope parameters are present in the traffic profile.	Yes	SHOULD	
MMREQ15486	A default Traffic Priority of 0 SHOULD be used if a specific Traffic Priority value is not required.	Yes	SHOULD	
MMREQ15487	A default Request/Transmission policy of 0 SHOULD be used if a specific Request/Transmission Policy value is not required.	Yes	SHOULD	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15488	A default Maximum Sustained Traffic Rate of 0 SHOULD be used if a specific Maximum Sustained Traffic Rate is not required.	Yes	SHOULD	
MMREQ15489	A default Maximum Traffic Burst of 3044 bytes SHOULD be used if a specific Maximum Traffic Burst is not required.	Yes	SHOULD	
MMREQ15490	A default Minimum Reserved Traffic Rate of 0 SHOULD be used if a specific Minimum Reserved Traffic Rate is not required.	Yes	SHOULD	
MMREQ15491	A default Assumed Minimum Reserved Traffic Rate Packet Size of 0 SHOULD be used if a specific Assumed Minimum Reserved Traffic Rate Packet size is not required.	Yes	SHOULD	
MMREQ15492	A default Traffic Priority of 0 SHOULD be used if a specific Traffic Priority value is not required.	Yes	SHOULD	
MMREQ15493	A default Maximum Sustained Traffic Rate of 0 SHOULD be used if a specific Maximum Sustained Traffic Rate is not required.	Yes	SHOULD	
MMREQ15494	A default Maximum Traffic Burst of 3044 bytes SHOULD be used if a specific Maximum Traffic Burst is not required.	Yes	SHOULD	
MMREQ15495	A default Minimum Reserved Traffic Rate of 0 SHOULD be used if a specific Minimum Reserved Traffic Rate is not required.	Yes	SHOULD	
MMREQ15496	A default Assumed Minimum Reserved Traffic Rate Packet Size of 0 SHOULD be used if a specific Assumed Minimum Reserved Traffic Rate Packet size is not required.	Yes	SHOULD	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compliance	Category	Comment
MMREQ15497	A default Nominal Polling Interval of 0 SHOULD be used if a specific Nominal Polling Interval is not required.	Yes	SHOULD	
MMREQ15498	A default Maximum Sustained Traffic Rate of 0 SHOULD be used if a specific Maximum Sustained Traffic Rate is not required.	Yes	SHOULD	
MMREQ15499	A default Maximum Traffic Burst of 3044 bytes SHOULD be used if a specific Maximum Traffic Burst is not required.	Yes	SHOULD	
MMREQ15500	A default Minimum Reserved Traffic Rate of 0 SHOULD be used if a specific Minimum Reserved Traffic Rate is not required.	Yes	SHOULD	
MMREQ15501	A default Assumed Minimum Reserved Traffic Rate Packet Size of 0 SHOULD be used if a specific Assumed Minimum Reserved Traffic Rate Packet size is not required.	Yes	SHOULD	
MMREQ15502	A default Tolerated Polling Jitter of 0 SHOULD be used if a specific Tolerated Polling Jitter is not required.	Yes	SHOULD	
MMREQ15503	A default Traffic Priority of 0 SHOULD be used if a specific Traffic Priority value is not required.	Yes	SHOULD	
MMREQ15504	A default Maximum Sustained Traffic Rate of 0 SHOULD be used if a specific Maximum Sustained Traffic Rate is not required.	Yes	SHOULD	
MMREQ15505	A default Maximum Traffic Burst of 3044 bytes SHOULD be used if a specific Maximum Traffic Burst is not required.	Yes	SHOULD	
MMREQ15506	A default Minimum Reserved Traffic Rate of 0 SHOULD be used if a specific Minimum Reserved Traffic Rate is not required.	Yes	SHOULD	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15507	A default Assumed Minimum Reserved Traffic Rate Packet Size of 0 SHOULD be used if a specific Assumed Minimum Reserved Traffic Rate Packet size is not required.	Yes	SHOULD	
MMREQ15508	A default Maximum Downstream Latency of 0 SHOULD be used if a specific Maximum Downstream Latency is not required.	Yes	SHOULD	
MMREQ15509	When the PDP is going to shutdown, it SHOULD send a COPS Client-Close message to the PEP.	No	SHOULD	
MMREQ15510	In the COPS Client-Close message, the PDP SHOULD NOT send the PDP redirect address object PDPRedirAddr.	No	SHOULD	
MMREQ15514	This field MAY be unspecified in which case the DSCP/TOS field in the packet is not over-written by the CMTS.	Yes	MAY	
MMREQ15515	This field MAY be used in both the upstream and downstream directions.	Yes	MAY	
MMREQ15516	A Classifier MAY have wild-carded fields (indicated by zeroed fields), but care must be taken so that multiple IP flows do not unintentionally match the same Classifier, which can lead to unexpected results.	Yes	MAY	
MMREQ15517	The Policy Server and Application Manager MAY specify a second set to represent the reserved envelope, and a third set to represent the committed envelope.	Yes	MAY	Optional - not used
MMREQ15519	Alternatively, the PS/AM MAY issue separate Gate-Set messages to tell the CMTS to authorize and reserve and then to commit via a subsequent Gate-Set message.	Yes	MAY	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15520	If the approximations do not give the Policy Server or Application Manager the control it desires, the PS/AM MAY use the other methods of defining the Traffic Profile, which includes the ability to define some DOCSIS-specific parameters.	Yes	MAY	
MMREQ15534	Application Managers that provide novel services MAY use the Configurable field to specify new session classes.	Yes	MAY	
MMREQ15537	The Application Manager or Policy Server MAY also query for this object as part of a failure recovery or other mechanism.	Yes	MAY	
MMREQ15538	The Opaque Data object contains information that a Policy Server or Application Manager MAY store on a CMTS that remains opaque to the CMTS.	Yes	MAY	
MMREQ15542	At this point, the PDP MAY periodically attempt to re-establish the connection.	Yes	MAY	
MMREQ15543	Messages that MAY be initiated by the Application Manager and Policy Server include Gate-Set, Gate-Info and Gate-Delete.	Yes	MAY	
MMREQ15546	The Gate-Set message MAY be sent by the PDP to the PEP to initialize or modify the operational parameters of a Gates.	Yes	MAY	
MMREQ15551	To modify the Traffic Profile associated with an existing Gate, an Application Manager MAY send a Gate-Set message with the GateID of the Gate to be modified and the new Traffic Profile.	Yes	MAY	

Table 6: PacketCable Requirements Compliance Matrix

REQ Tag	Requirement Text	Compli-ance	Cate-gory	Comment
MMREQ15552	To modify the Usage Limits associated with an existing Gate, an Application Manager MAY send a Gate-Set message with the GateID of the Gate to be modified.	Yes	MAY	
MMREQ15557	For applications that require a high-degree of time accuracy, the AM MAY query the CMTS for its Gate Time Info object after it moves a Gate into or out of a committed state.	Yes	MAY	Optional - not used
MMREQ15562	An Application Manager MAY provide an optional Event Generation Info object in a Gate-Set message.	Yes	MAY	Optional - not used
MMREQ15564	The Application Manager MAY specify a primary RKS IP address in the optional Event Generation Info object or the Application Manager MAY allow the Policy Server to use its default primary and secondary RKS IP Addresses.	Yes	MAY	Optional - not used
MMREQ15565	If the AM specifies a primary RKS IP Address, it MAY also specify a secondary RKS IP Address.	Yes	MAY	Optional - not used
MMREQ15566	In some situations, where the Application Manager and the Policy Server is acutely aware of DOCSIS, it MAY specify the Traffic Profile for the Gate using the DOCSIS Service Class Name or the DOCSIS-specific parameterization format.	Yes	MAY	
MMREQ15576	All envelopes used in a Traffic Profile MUST be the same type, i.e. either FlowSpec, DOCSIS Service Class Names, or DOCSIS-Specific Parameters.	Yes	MUST	

1.8 Glossary

Term	Definition
AM	Application Manager - logical network element defined in the PacketCable Multimedia architecture responsible for making bandwidth requests on behalf of a cable agnostic client.
Best effort	The default service flow. The characteristics for this service flow are defined in the cable modem config file. If a packet does not match any classifier then it is assigned to the best effort service flow.
CableLabs	A standards body that writes interface specifications and defines functional behavior for cable network elements.
Classifier	The set of parameters by which a media packet is judged to determine which service flow the packet belongs on.
Client	A SIP client
CM	Cable Modem - a cable network device that provides access to the cable network from an ethernet IP network.
CM	Call Manager - an MCS architecture component responsible for managing call-halves.
CMTS	Cable Modem Termination System - gateway between the cable HF/C network and the ethernet IP network. The CMTS receives the PCMM messages and communicates with the cable modem via DOCSIS to set up managed service flows.
COPS	Common Open Policy Service - a protocol defined in RFC 2748 that sets up a master/slave relationship between network elements for policy decisions. The PCMM protocol is an extension of COPS.
CS2M	CS2000 Management Tools - the CS2K GWC provisioning GUI
DOCSIS	Data Over Cable System Interface Specification - the protocol used between cable modems and their CMTS to set up service flows and classifiers.
DIFFSERV	Differentiated Services - an IP packet marking scheme that allows IP packets to be treated differently in the network
DSCP	DIFFSERV Code Point - the bit pattern used for DIFFSERV
GETS	Government Emergency Telephone Service - a telephony service that gives higher priority to some callers so that government services can function in the presence of extremely high call loads
HF/C	Hybrid-Fiber/Coax
IKE	Internet Key Exchange - used in PCMM to authenticate the PS from the AM
IPSec	IP Security - used in PCMM to secure the PCMM signaling between the AM and the PS (and between the PS and the CMTS)
KRS	Key Registration System
NAT	Network Address Translator - a device that translates between public network addresses and private network addresses.

Term	Definition
PacketCable	A subdivision of CableLabs that focuses on standards for VoIP over cable and multimedia over cable.
PC	Personal Computer (in this case)
PCMM	PacketCable Multimedia - an architecture and protocol for managing cable network bandwidth on behalf of cable agnostic clients.
PDP	Policy Decision Point - the COPS network element responsible for formulating network policy. The AM is a PDP. The PS is a PEP w.r.t. the AM and a PDP w.r.t. the CMTS.
PEP	Policy Enforcement Point - the COPS network element responsible for enforcing policies created by the PDP. The CMTS is a PEP. The PS is a PEP w.r.t. the AM and a PDP w.r.t. the CMTS.
Policy	A policy in the context of PCMM defines the access to and level of managed QoS available to a PCMM subscriber.
PS	Policy Server - network element defined in the PacketCable Multimedia architecture responsible for receiving PCMM signaling from and AM and forwarding it to the correct CMTS.
QoS	Quality of Service - the set of network characteristics that determine how a media packet is treated
SA	IPSec or IKE Secure Association
Service Flow	A managed QoS pipeline through the cable HF/C network defined by the quality of service given to the packets that transit the service flow.
SIP	Session Initiation Protocol - a VoIP signaling protocol
Socket	The IP address and port number used to communicate over an IP network to a particular service.
SS-L	Session Server Lines - a name for the MCS application server when used with CS2000
TOS	Type Of Service - a set of bits in the IP header that can be used to mark IP packets for different treatment in the network. Some of the TOS bits are used for DSCP.

Product = MG 9000

A00008858 -- CS2M User Inactivity Time-out and MG9K EM User Inactivity Time-out

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Description

This SN09 feature provides a standard and consistent design across MG9KEM and CallServer 2000 Management Tools (CMT) for client user inactivity time-out. There are three timers that will be configurable from the SSPFS CLI after the initial SSPFS installation. The three timers are:

- User Inactivity Timeout
- User Termination Timeout
- Reauthentication Disable Timeout

1.1.1 Configuration Behavior

Default Assignment - The default value of 10 minutes will be set on SSPFS installation for User Inactivity Timeout and User Termination Timeou. The default for Reauthentication Disable Timeout will be 30 seconds.

Accepted Values - The values for User Inactivity Timeout and User Termination Timeout can be entered in increments of full minutes(e.g 1, 2,3) The values can range from a minimum of 5 minute to a maximum of 1440 minutes(24 hours). The value ‘0’ will be used to indicate that no timeout implementation is desired, effectively turning this feature off.This applies to either value as follows. The accepted values for Reauthentication Disable Timeout are 0-300 in seconds.

- If the user wants to turn off the entire timeout feature, a value of ‘0’ for USER_INACTIVITY_TIMEOUT will indicate this.
- If the user wants the timeout feature to be activated but does not desire a USER_TERMINATION_TIMEOUT to be enforced, the value ‘0’ will indicate this

When the CLI is used to configure the timeout values, they will take effect immediately for all new client launches. No restart is required. The configuration access is located centrally to all supported applications and requires ‘root’ access to the SSPFS server.

1.1.2 CLUI Behavior

After user runs the CLUI, If there is no user input on the command line for the duration of the first timer, the process is killed and user exits from the session to the shell.

1.1.3 General GUI Behavior

When the User Inactivity Timeout expires for a given application, all application windows will be minimized, which prevents all users input and provides no data output to the user. Proper login authentication is required to release the application lock and make the application visible. Once the re-authentication occurs, the user’s desktop view will be restored with no

updates lost.If the application user does not re-authenticate within an acceptable time frame, as defined by the User Termination Timeout, the application user will be forced to exit the application before making another authentication request. Note that the User Termination Timeout does not start until the User Inactivity Timeout expires.

1.1.4 Re-authentication Behavior

The SSPFS Security Servlet enforces security limitations during re-authentication attempts. No userid will be displayed in the re-authentication window. If there are 3 failed authentication attempts, the re-authentication window will be locked for 30 seconds. After the 30 second timer, which is configurable, re-authentication will be allowed.

Table 1 Application Behavior Summary

Type	Name	Behavior
Launch Page	CS2M Launch Point	After user launches the Launch Page, If there are no user initiated mouse movements for the duration of the first timer, the client is iconizied and a dialog is popped up to prompt the user re-login. Only after successful re-authentication, the launch page is de-iconized. If there are no user initiated mouse movements on the screen for the duration of the second timer (At that time the client should be iconized and a login dialog is shown), a warning dialog is popped up which saying that the client is locked due to long time non-operation. When user confirm it, the client as well as the re-login dialog are both closed.

Type	Name	Behavior
Java GUI	CS2000 Management Tool GUI Line Maintenance Manager GUI GWC EM Independent GUI GWC EM Independent GUI launched from SAM21 EM Succession SAM21 Element Manager GUI SAM21 EM GUI launched from GWC EM Network Patch Manager GUI	After user launches the GUI, If there are no user initiated mouse movements for the duration of the first timer, the client is iconizied and a dialog is popped up to prompt the user re-login. Only after successful re-authentication, the GUI is de-iconized. If there are no user initiated mouse movements for the duration of the second timer (At that time the client should be iconized and a login dialog is shown), a warning dialog is popped up which saying that the client is locked due to long time non-operation. When user confirm it, the client as well as the re-login dialog are both closed.
Web GUI	Trunk Maintenance Manager Batch Configuration Monitor	After user launches the web client, If there are no user initiated **mouse clicks** on any html link/button/droplist for the duration of the first timer, when user mouse clicks, the Web Page will be redirected to the re-login page, on which it shows user "Application Session Invalid" and provide the link for re-login as well as the link for close current window. After user re-authenticated successfully, the page is re-direct to the original page. If there are no user initiated mouse clicks on the screen for the duration of the second timer, when user perform any mouse clicks, a warning message which says that the client is locked due to long time non-operation. Then the web client is closed directly after user confirm the message.
CLUI	GWCEM CLUI NPM CLUI SAM21 EM CLUI OSSGate CLUI BPT CLUI AMS CLUI	After user runs the CLUI, If there is no user input on the command line for the duration of the first timer, the process is killed and user exists from the session to the shell. If there is no user input on the command line for the duration of the shell time out value, user will exist from the shell automatically.

1.2 Hardware Requirements or Dependencies

None.

1.3 Software Requirements or Dependencies

None

1.4 Limitations and restrictions

Limitations and restrictions are:

1) The following CLUIs which run inside SSH/Telnet session, are not supported by this design. They are the SSPFS cli tool, SESM configure tool, App Start/Stop script and the Unix self-contained commands.

2) The UAS GUI is non-compliant with this design. There is no plan to support user inactivity timeout.

3) The APS GUI is partially compliant with this design. A fixed timeout is supported which logs the user out, but there is no re-login or minimization support planned

4) The Security Server Manager, used to configure secure IPSec connections between and SSPFS server and another destination(e.g. MG9000) is partially compliant to this design. A default 5 minute timeout exists and the user must initiate an action before being redirected to a page that will allow re-authentication. No changes were added to this functionality as a part of this feature.

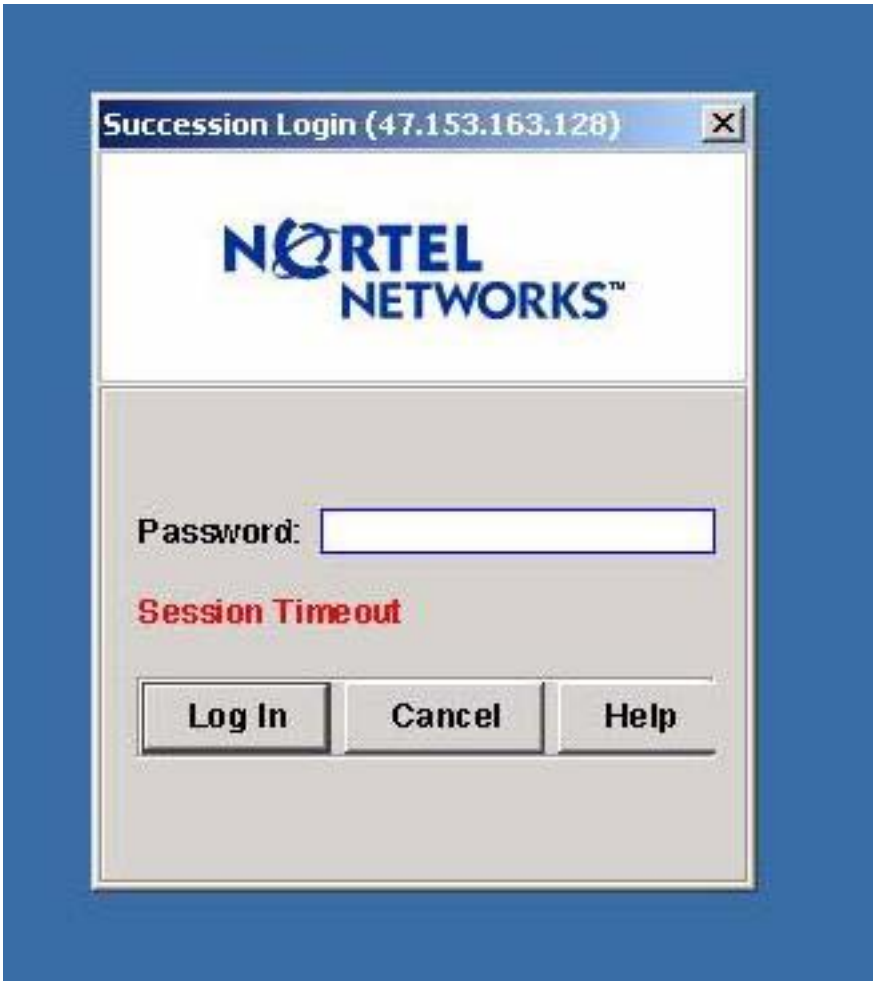
5) There may be some platform specific behavor in the GUI desktop. This applies strictly to the requirement to restrict all user access and provide no data output to the user when the timeout occurs. Based on the software platform the top-level view may be iconified or disappear all together.

6) Although the configuration is centrally located within the SSPFS platform, the craftsperson or system administrator must manually ensure that the timeout values across SSPFS servers are kept in sync between CMT and MG9KEM servers if this is the desired behavior. In other words, as long as the defaults are in place the CMT and MG9KEM applications will behave in exactly the same manner. Once the administrator makes a change on one SSPFS server there is not a design or expectation that this will be automatically synchronized.

Note: Though no specific design support is planned for the Unix shell applications as mentioned herein, the SSPFS does currently support a shell timeout that will kill a shell session if there is no activity within a specific time period. The value for this shell timeout is configured via the /etc/profile file as the TMOUT value

1.5 Screenshots

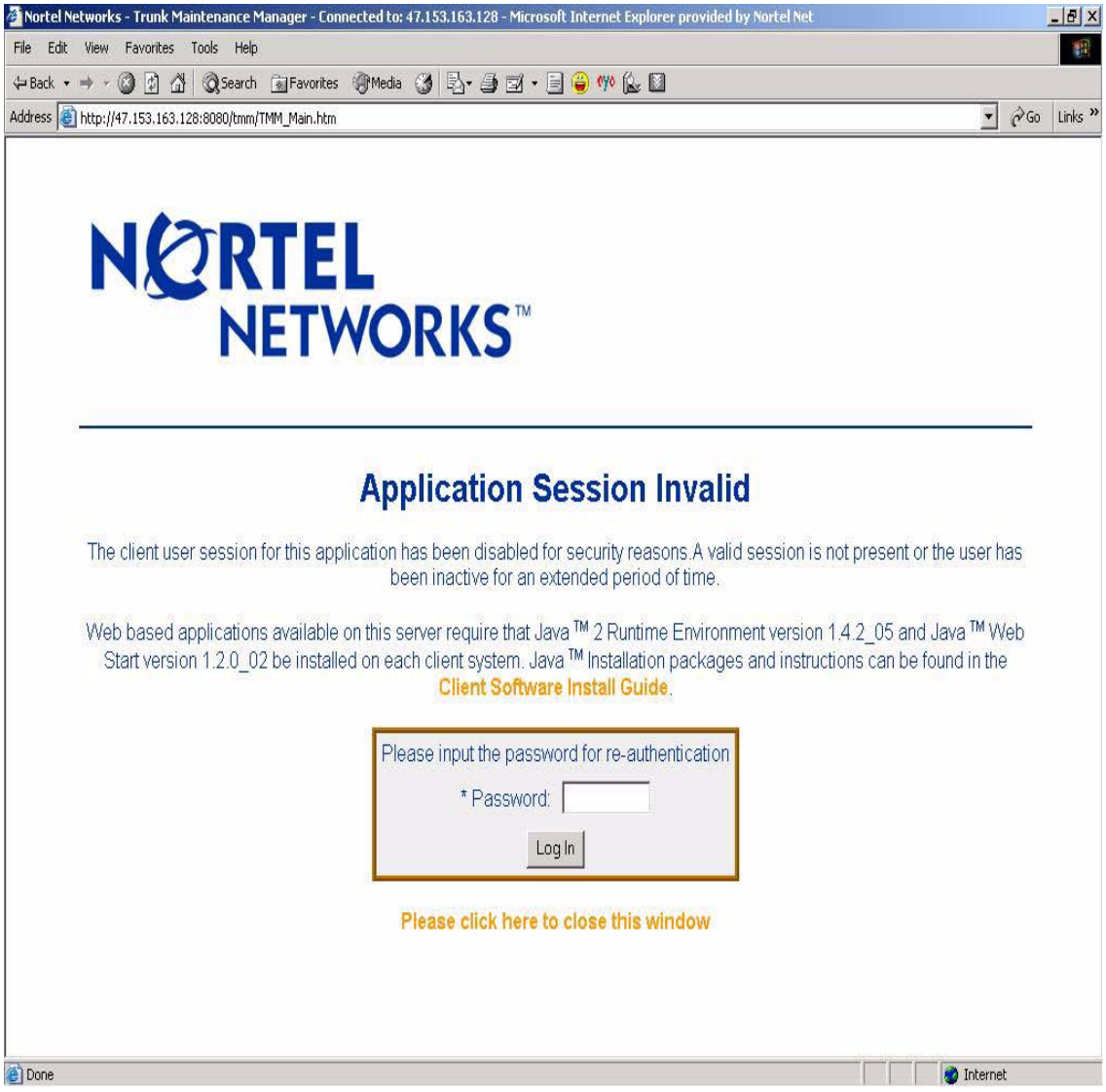
GUI Timeout



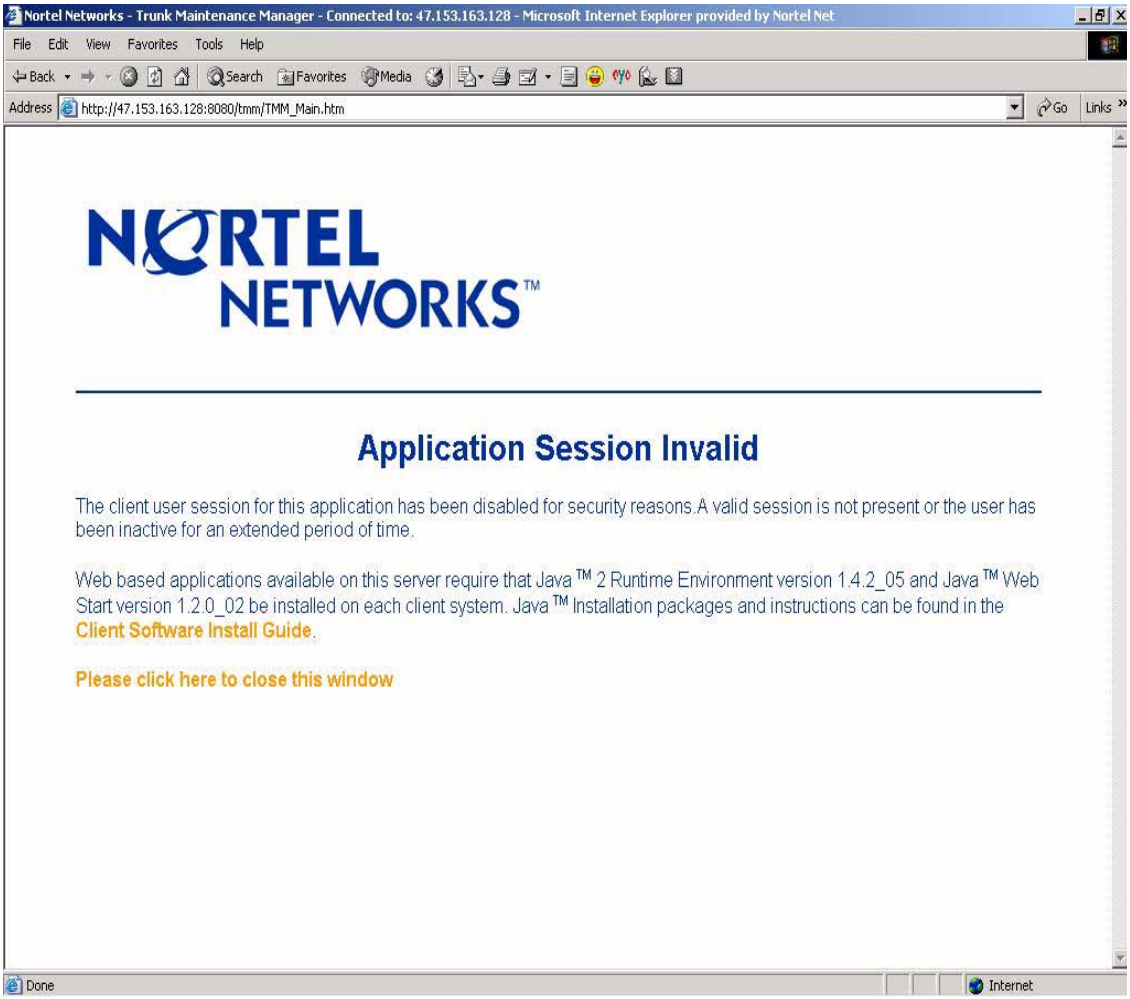
GUI Terminate Timeout

GUI After 3 Retries Fail

TMM Timeout


Nortel Networks - Trunk Maintenance Manager - Connected to: 47.153.163.128 - Microsoft Internet Explorer provided by Nortel Net
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://47.153.163.128:8080/tmm/TMM_Main.htm
Go Links
NORTEL NETWORKS™
Application Session Invalid
The client user session for this application has been disabled for security reasons.A valid session is not present or the user has been inactive for an extended period of time.
Web based applications available on this server require that Java ™ 2 Runtime Environment version 1.4.2_05 and Java ™ Web Start version 1.2.0_02 be installed on each client system. Java ™ Installation packages and instructions can be found in the Client Software Install Guide.
Please input the password for re-authentication
* Password:
Log In
Please click here to close this window
Done
Internet

TMM Terminate Timeout



1.6 Interactions

None

1.7 Glossary

MG9K EMMedia Gateway 9000 Element Manager

CLUI Command Line User Interface

CS2M CS2000 Management Components

CMT CS2000 Management Tools

GWCEM Gateway Controller Element Manager

NPM Network Patch Manager

SSPFS Succession Server Platform Foundation Software

SESM Succession Element & Sub-element Manager

SAM21 EMCS2000 SAM21 Manager

Product = MG 9000

A00008969-- ATM50 SSI Monitoring

Excerpts fromt he Design Description

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Description

This document defines and describes monitoring the rate of SSI(Signal State Change Interrupt) coming from the ATM ports and raising an alarm if the given threshold exceeded . This feature includes following parts:

- Collect the SSI event count from the all types of ATM ports.
- Decide that SSI alarm condition occurrence.
- Raise SSI alarm.

1.2 Problem description

While investigating a recent ABI outage it was observed an exteremely high number of ATM50 SSI pegs occurred in the SCO & ITX cards. For this situation, monitor the rate of SSI (Signal State Change) indications from all types of ATM parts and alarm if the rate exceeds a given threshold. This feature will enable the detection of faulty hardware components in the field.

1.3 Adjustments made

Signal Condition Change Interrupts (SSI) are collected every minute for each port of the ATM50 device. Several variables are added to conduct counts and comparisons. If the SSI count is too high, an ATM50 SSI alarm is raised, called Hardware Port Unstable.

Product = MG 9000

A00009218-- MG9KEM Data Audit Robustness

Functional Description

1: Applicable Solution(s)

UA-AAL1, UA-IP

1.1 Description

MG9KEM audits can currently only be run for an entire NE, even when data mismatches exist for only a small portion of the NE data. Experience in the field has shown that subsystem data corruption (e.g VMG data mismatch on a single shelf) is the most common type of data corruption. In these types of scenarios, the customer has to wait for lengthy NE audits to run to fix issues that in reality require only a small amount of time to run.This activity will enable subsystem audits. This capability was built in from the start, but has not been enabled in previous releases. This change offers both efficiency and robustness improvements as well as enhanced usability:

- ïRobustness improvements. The EM does not have to use unnecessary database resources and strain the MG9000 with unnecessary SNMP traffic, which has been known to affect call processing performance.
- ïUsability improvements. Selective audits will allow the user to quickly fix call processing affecting data mismatches. This will translate into significantly reduced outage times if data mismatches are call affecting. Also minimizing the audit times will in turn reduce the periods in which the GUI response of the EM is sluggish because the server is busy.

1.2 Hardware Requirements or Dependencies

No additional requirements are needed for this feature besides the standard MG9000 EM and the MG9000 Gateway.

1.3 Software Requirements or Dependencies

This is a standalone feature and has no special requirements or dependencies.

1.4 Limitations and restrictions

Subsystem audits will only be allowed for non-scheduled audits only.

1.5 Interactions

N/A

1.6 Applicable customer facing sections

Fault Management

Logs____

Alarms____

Configuration

Data Schema_____

User Interface_____

Element Management____

Security_____

Service Order_____

Office Parameters_____

Accounting (includes AMA billing)_____

Performance (includes operational measurements)_____

1.7 Glossary

Term	Description
EM	Element Manager
GUI	Graphical User Interface
MG9000	Media Gateway 9000
SNMP	Simple Network Management Protocol
WMG	Virtual Media Gateway

2: Configuration for A00009218

2.1 Hardware and Software Requirements

This functionality is for MG9000 EM that has SN09 or higher software version.

2.2 Initial Configuration

No changes to the initial configuration.

2.3 Upgrade Impact

2.3.1 Dump and Restore

N/A

2.3.2 12.3.2 Element Management Upgrade

N/A

2.4 Element Management

2.4.1 GUI information

Table 1 New or modified GUIs

GUI name	New, Changed or Deleted
Audit View	Changed
Create Audit View	Deleted
Select VMG frame	New

2.4.1.1 Audit View -- Functional description

In release SN09, the Audit GUI gives the user the ability to run an audit at any time even though a scheduled audit exists for the particular NE. In previous releases the user had to delete an existing scheduled audit in order to run an immediate audit. Additionally, for immediate audits users have the option to specify which sub-system (or VMG) to run the audit on. For example the user might choose to audit just the line circuits in the system, or just a single problem VMG.

2.4.1.2 Audit view - GUI usage and implications

The “Add” and “Remove” buttons no longer exist in the gui. From MG9kEMS software UE9000 MG Element Manager View when the audit view is selected, a list of NEs in the subnet is shown in the NE list. This shows only those NEs that are discovered (and are thus auditable). The user chooses an NE of interest and schedules the audit directly in the properties panel. Two tabs exist, one for scheduled audits, and another for immediate ones.

2.4.1.3 Audit view - GUI size

Not Applicable

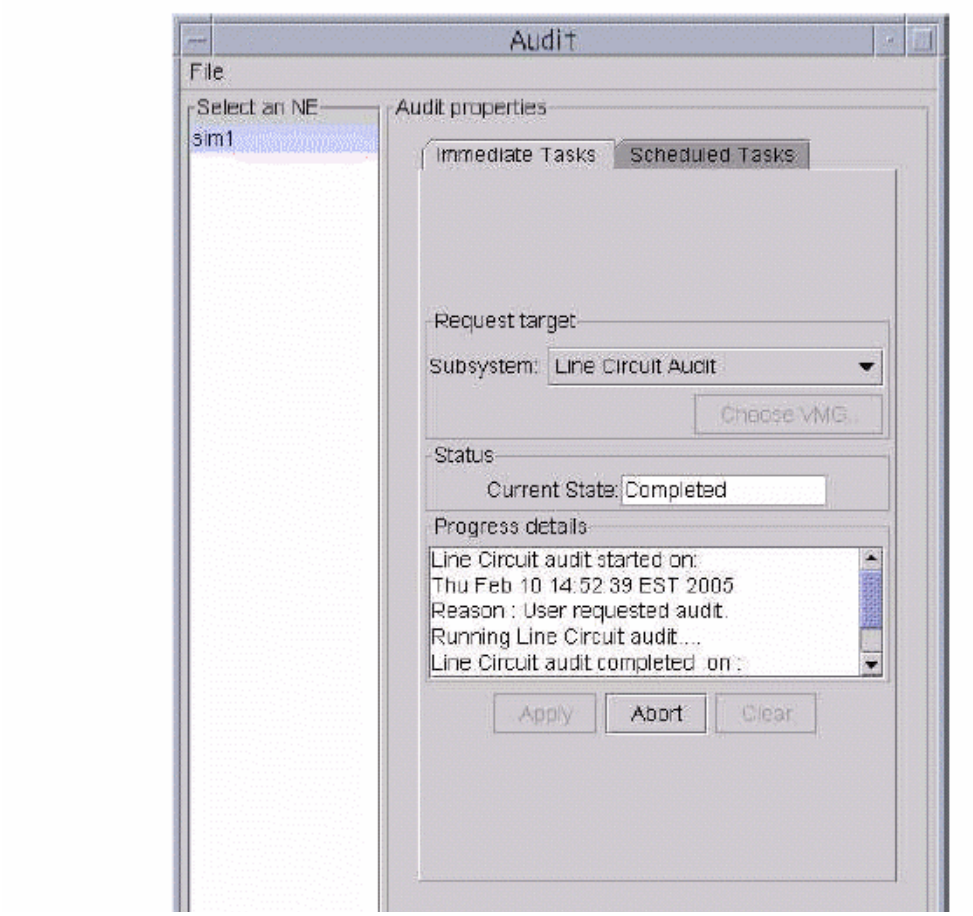
2.4.1.4 Audit view - GUI fields

Subsystem: A drop down menu for selecting a type of audit to run.

2.4.1.5 Audit view - Usage example 1

The following example shows a user selecting and running line circuit audit:

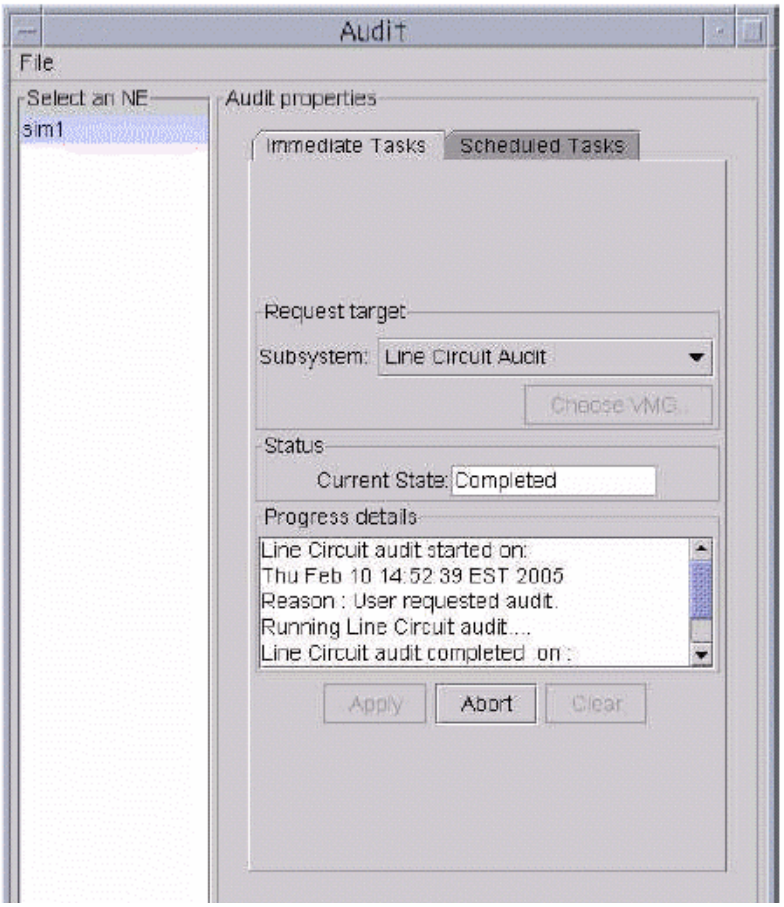
Figure 1 Running an immediate audit



2.4.1.6 Audit view - Usage example 2

The following example shows a user selecting to run a single VMG audit. The user has selected “VMG” from the subsystem drop down menu and clicked on the “Choose VMG” button. Clicking on the “Apply” button on the VMG selection frame will start an audit on the VMG named SLOA011-0-0:

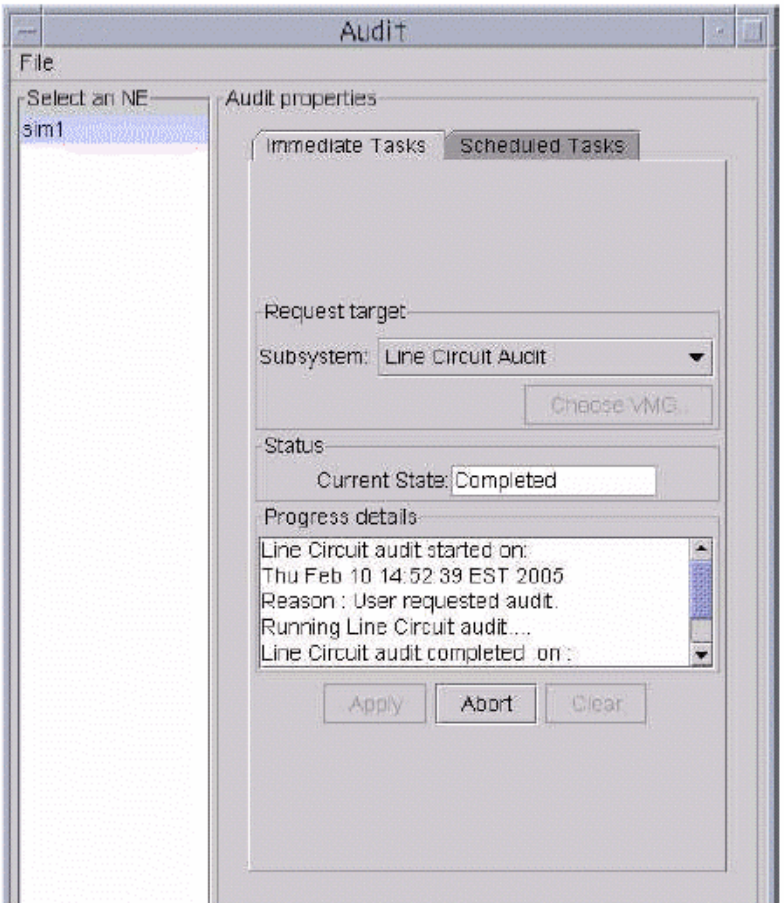
Figure 2 Running a VMG audit



2.4.1.7 Audit view - Usage example 3

The following example shows a user scheduling an audit to run in the future. This audit will run starting at 3:00PM on every Tuesday and Friday of the week, until it is aborted:

Figure 3 Scheduling an audit



Product = MG 9000

A00009280-- MG9K Line Circuit Enhancements

Functional Description

1: Applicable Solution(s)

UA-IP, UA-AAL1

1.1 Description

The MG9K EM Line Circuit Enhancements concentrates on the below requirements for SN09 release:
1> Color indication for alarms on the port ilog of the Card Display.
2> User can manually mark a port as faulty.
3> Color indication for faulty port on the port ilog of the Card Display.

4> Display of directory number in the LineCircuit view
5> Display of directory number at the Alarm Browser screen for alarms reported.
Also the associated directory number would get added in the line circuit alarm log.
6> Circuit Listing at the NE desktop level to list the faulty ports.

1.2 Alarms display at the Port level

The line circuit ilogs on a LineCard would be displayed with an appropriate alarm color (if any alarm exists on the line circuit). User can easily make out the ports with alarms without opening a Port View. Currently alarms show in color at many different levels in the EM such as the shelf and card but not at the port level. After the addition of this functionality EM would be consistent at all levels in displaying alarms. The existing port view would not be changed. WLC,XDSL,GLC and SAA card view currently displays a list of line circuits. Existing alarm colors would be used to indicate the appropriate alarms on the port ilog of a line card view.

say: Critical alarm: Red
Major alarm: Red
Minor alarm: Orange
Warning : Yellow

1.2.1 Manually marking a port as faulty from the Port view

The new Line Circuit view would enable a User to mark a port (line circuit) as faulty. User can mark a port as faulty only when it is locked. Authorization level for this method would be ‘ewsmtc’. Fault setting option would be disabled (greyed out) if the port is unlocked.

User would get a warning message when he tries to unlock a faulty port. But if User wishes to go ahead irrespective of the port being marked as faulty, the request would get submitted.

‘Fault State’ field would be added in the ‘Circuit Status’ section of a port view. This new variable will be persisted only on the EM. There is no associated MIB variable for this state.

1.2.2 Display of faulty ports with a specific color

Currently User has no indication of the port being faulty. This functionality would help User to indentify a faulty port/circuit from the Line Card View.

A faulty port would be displayed with magenta color. Faulty color indication on a port would take precendence over alarms color indication.
say: A port which has alarms and is also marked by the User as faulty would be displayed with magenta color.

1.3 Display of Directory number(DN) at the Line Circuit view

With every line circuit associated to a VMG, there can be an associated DN. The DN will be displayed in the 'Circuit Provisioning' section of the Line Circuit view.

This would help the User to be positive that he is on the correct port. Display of the directory number that is associated with a port ensures proper location.

If the DN is not yet created for a line circuit, then the field would have 'None' as the value.

Any subsequent changes to DN would get udpated on a open Line Circuit view.

1.4 Display of Directory number(DN) on Alarm Browser

Directory number(DN) associated with a particular Line Circuit would be displayed in the description part of the Line Circuit alarm on a Alarm Browser.

eg: The description part of a line circuit alarm would have an added entry
`DN Affected: 6195210102`

If no DN is associated with the line circuit, then the description part of the line circuit alarm would have an appended entry saying
`DN Affected: None`

DN associated when the alarm was reported would be displayed. Any subsequent changes to the DN would not get updated on the Alarm Browser.

Physical location and the directory number details for a line circuit alarms would be helpful in troubleshooting.

Alarm log would also reflect the DN associated with the line circuit alarm.

1.5 'Faulty Circuit Listing' view at the NE Desktop level

A new menu item would be added in Services Menu list, on NE desktop view, namely 'Faulty Circuit Listing'. Clicking this menu item would display the 'Faulty Circuit Listing' view which has the below information:
1> Associated Frame number
2> Associated Shelf number
3> Associated Slot number
4> Port Number

'Faulty Circuit Listing' view at NE desktop level would have readonly values. This GUI would have an associated time stamp and a refresh button. Refresh button is used to refresh the GUI with the latest port being marked as faulty. Refresh button is used to avoid dynamic updates when the faulty status of the port changes.
Timestamp would reflect the last time when the 'Refresh' button was used to collect the latest faulty ports information.

1.6 Hardware Requirements or Dependencies

None

1.7 Software Requirements or Dependencies

None.

1.8 Limitations and restrictions

- User will be allowed to mark a port/line circuit as faulty only when it is locked.
- User would get an appropriate warning message when he tries to do unlock a faulty port.
- XDSL Data Circuits cannot be marked as faulty.
- Fault color display on a line circuit would take precedence over alarm color indication.
- No new color indication would be displayed for a port which is locked.
- Once the line circuit alarm is reported to the Alarm Browser, any subsequent changes to the DN of that particular Line Circuit would not get updated in the description part of the Alarm Browser for a line circuit alarm.
- Existing Circuit Listing GUI would not be changed. Line Card level circuit listing GUI will behave as before and would not undergo any changes as a part of this feature

1.9 Interactions

None.

1.10 Glossary

Term	Description
WLC	World Line Card
SAA	Service Adaptive Access
XDSL	X Digital Subscriber Line Card
MG9k	Media Gateway 9000
MG9K-EM	Media Gateway 9000 - Element Manager
GLC	Global Line Card
DN	Directory Number

2: Fault Management for A00009280

2.1 Fault management strategy

'A00009280 LineCircuit Enhancements' feature do not introduce new faults.

2.2 Fault management tools and utilities

2.2.1 Faults, Alarms and Logs

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

2.3 Logs

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format.

There is no change in the existing format of Line Circuit alarms, except that the description part has an added statement about the DN number associated with the Line circuit alarm. If no DN is associated, then the 'DN Affected: None' would be displayed.

Once an alarm is reported, any subsequent changes to the DN would not get reflected in the alarm log of that line circuit or in the description part of the line circuit alarm on the Alarm Browser.

2.3.1 Formats

2.3.1.1 NTSTD

```
NorLineFault
SWLN301 ***Jan12 01:02:40 3409 TBL MG9K NorLineFault
Location: 18-c018-FrameFFF.Shelf3.Slot21.SAAL.p7
Notification Id: 399
State: not acknowledged
Category: equipment
Cause: Equipment Malfunction
Time: Jan 12 01:02:40 1970
Component Id: Card.frame0.shelf3.slot21.SAAL.p7
Specific Problem:norLineFault
Description: linefault
DN Affected: 6195210102
Site   Flr RPos Bay_id
Cary 02 H02    MG9F 012
```

2.3.1.2 SCC2

NorLineFault
*** SWLN301 3409 TBL MG9K NorLineFault
Location: 18-c018-FrameFFF.Shelf3.Slot21.SAAL.p7
Notification Id: 399
State: cleared
Category: equipment
Cause: Equipment Malfunction
Time: Jan 12 01:02:40 1970
Component Id: Card.frame0.shelf3.slot21.SAAL.p7
Specific Problem: NorLineFault
Description: linefault
DN Affected: 6195210102
Site Flr RPos Bay_id
Cary 02 H02 MG9F012

2.4 Alarms

No new alarms are added as a part of this CCAF.

The Description part of a line circuit alarm would have an added statement namely:

DN Affected: <Associate DN>

If no DN is associated with a line circuit then the below statement would be appended to the description part of the line circuit alarm:

DN Affected: None

Once alarm is reported any subsequent changes to DN would not get reflected in the alarm log of that line circuit or in the description part of the line circuit alarm on the Alarm Browser.

2.5 Related documentation

None.

3: Configuration for A00009280

3.1 Hardware and Software Requirements

This functionality is for MG9000 EM that has SN09 or higher software version.

3.2 Initial Configuration

No changes for initial configuration

3.3 Upgrade Considerations

None.

3.4 Element Management

3.4.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
WLC View	CHANGED
GLC View	CHANGED
XDSL View	CHANGED
SAA View	CHANGED
LINE CIRCUIT View	CHANGED
FAULTY CIRCUIT LISTING	NEW

3.4.2 GUI information

3.4.2.1 GUI name: Line Card View (WLC, XDSL,GLC,SAA)

3.4.2.1.1 Functional description

From release SNO9, the line card view would display alarm color indication for the ports. A faulty port would be indicated with magenta color on the line card view. Display of only voice circuit ilogs changes on a XDSL view for faulty ports.

An example of WLC view is shown in Figure 1.

Figure 1 WLC View with faulty and alarm status indications on port ilogs

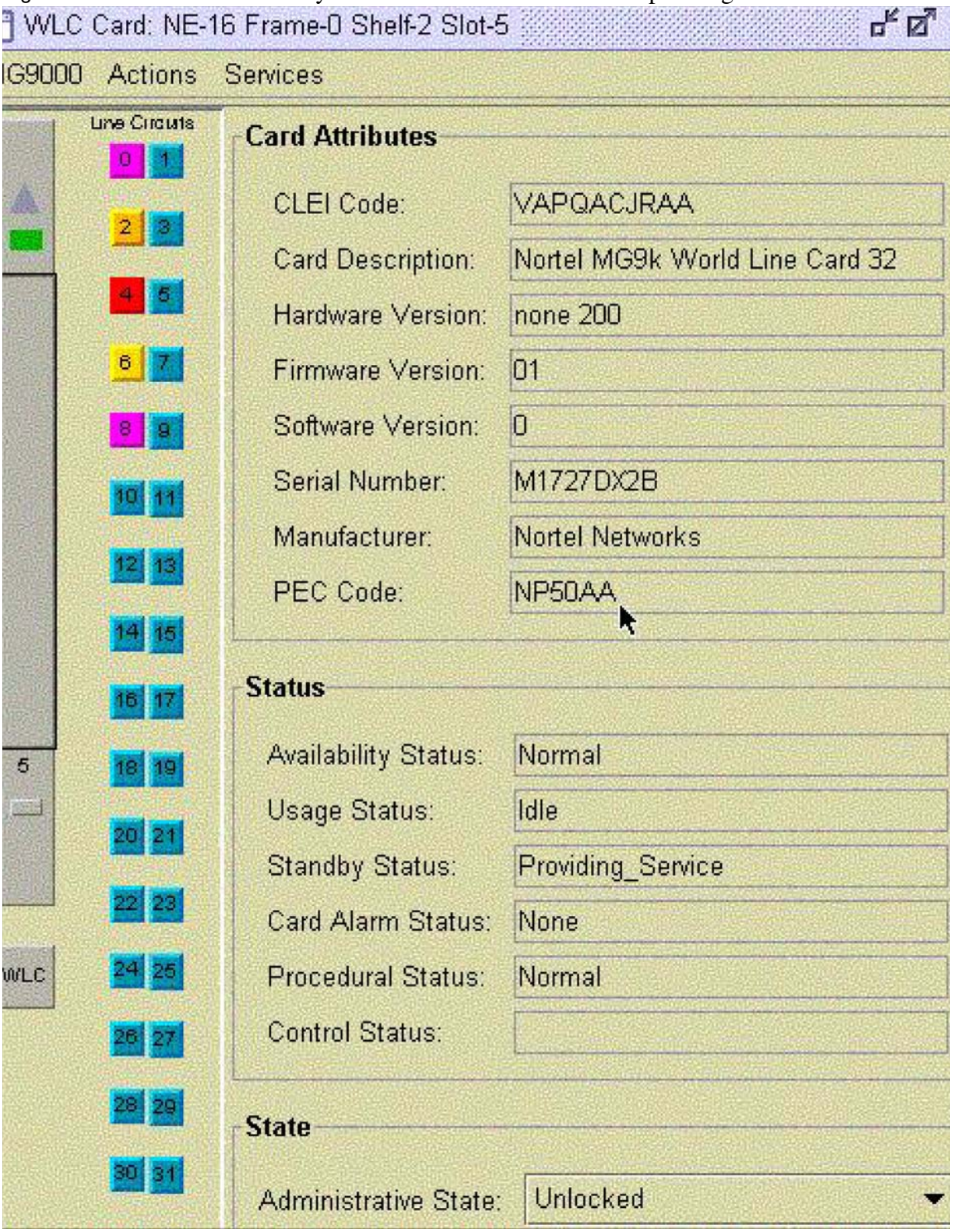


Figure 1 shows the WLC Card view with minor alarm on port 2, critical alarm on port 4, and warning on port 6. Also port 0 and port 8 are manually marked as faulty by the User

3.4.2.1.2 GUI fields

No new GUI fields are added.

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Circuit Listing	Changed	NA	NA	Line Circuits listed on the WLC card view would be displayed with an appropriate alarm color or fault color. The default color of the port is blue	NA

3.4.2.2 GUI name: Line Circuit View

3.4.2.2.1 Functional description

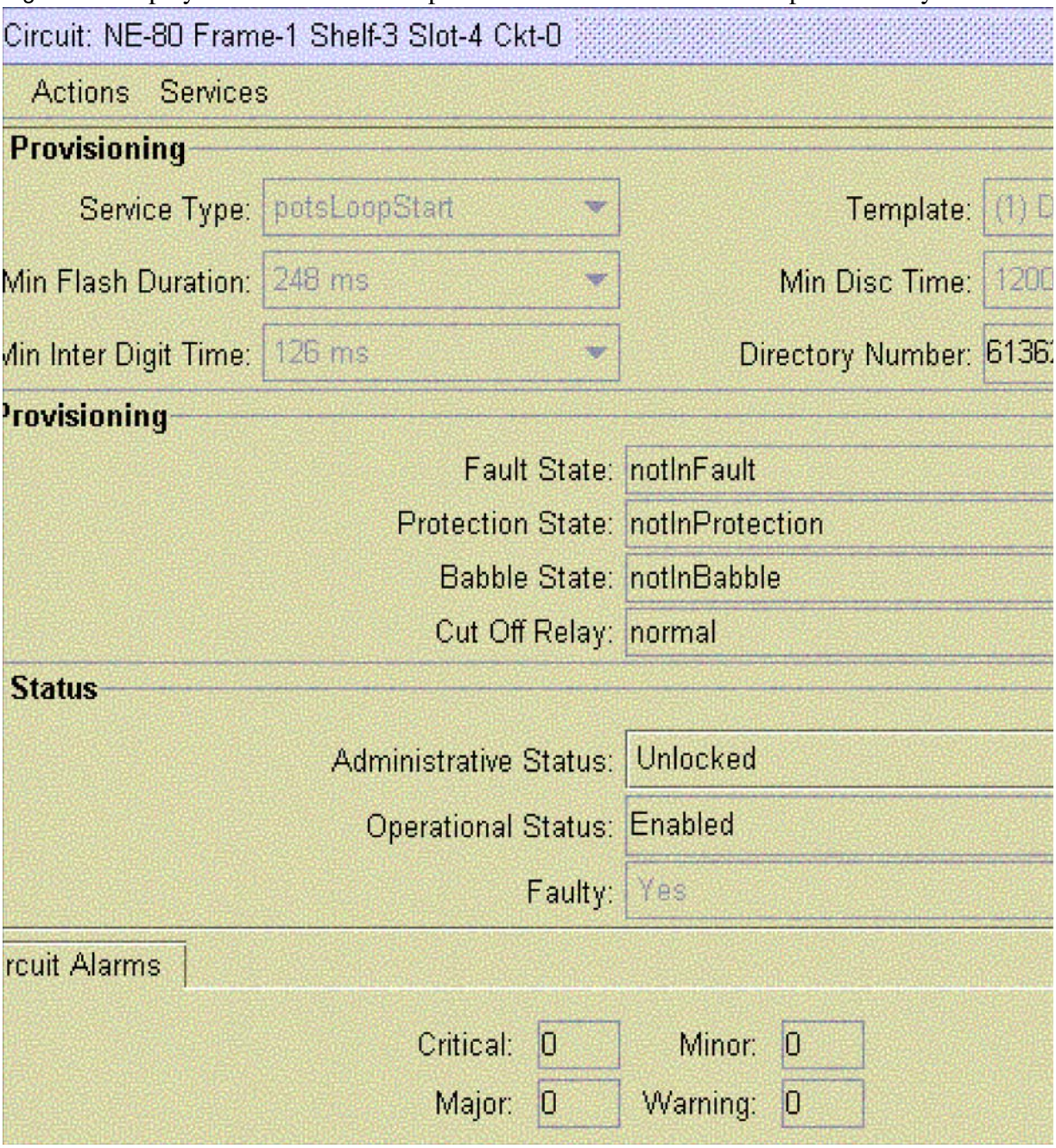
1> From release SNO9, the Line Circuit view would allow the User to mark a port as faulty with a prerequisite that the port should be locked.

The faulty combo box would be available in the 'Circuit Status' section of the Line Circuit View. This combo box would be disabled(greyed out) when the port is unlocked.

2> From release SNO9, the Line Circuit View would display the Directory Number (DN) associated with a termination point (line circuit). This information is displayed in the 'Circuit Provisioning' section of a Line Circuit View.

Figure 2 shows the display of Line Circuit view with associated DN Affected: 6136210202 displayed in Circuit Provisioning section. Also shown is the ability for the User to manullay mark the port as faulty when the port is locked from the Circuit Status section.

Figure 2 Displays associated DN and provision for the User to mark a port as faulty



User can select ‘No’ or ‘Yes’ from the ‘Faulty’ drop down to set the port as faulty or non faulty, accordingly. This dropdown is enabled only when the Administrative Status of the port is locked.

User can unlock the circuit which is marked as faulty. But he is displayed a warning message saying:

"The circuit is marked as faulty; the existing service may be degraded Are you sure?"

By selecting 'OK' option, he can submit the 'unlock' request to the Gateway.

By selecting 'Cancel' option, he would not submit the 'unlock' request to the Gateway.

3.4.2.2.2 GUI fields

3.4.2.3 GUI name: Faulty Circuit Listing View

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Faulty - Combo Box	New	NA	1> No 2> Yes	The Faulty Port Status Combo box and label are displayed in the 'Circuit Status' section of Line Circuit View This field is enabled when the port is locked. By selecting combo item 'No', User removes the faulty bit set for the port By selecting combo item 'Yes', User marks manually a port as faulty.	NA
Directory Number TextBox	New	NA	1>None 2><Associated DN>	The Directory Number label and text box are displayed in the 'Circuit Provisioning' section of the Line Circuit View. This is a read-only field. If any DN is associated with the line circuit then it gets displayed, else the field displays 'None' in the text box.	NA

3.4.2.3.1 Functional description

From release SNO9, the Faulty Circuit Listing view would be added to a new menu item of the Services menu option, on the NE desktop view.

3.4.2.3.2 GUI usage and implications

From the NE desktop view, go to the 'Services' Menu list.

The drop down would list ‘Faulty Circuit Listing’ menu item. Clicking on this menu item would display the ‘Faulty Circuit Listing’ view.

This view would list all the ports manually marked as faulty by the User on an NE along with their location information.

The view would have a timestamp associate with the last refresh and a ‘Refresh’ button. Using ‘Refresh’ button user can view the latest faulty port information.

Figure 3 shows the new ‘Faulty Circuit Listing’ GUI when no faulty ports are available. The text above the table header would display ‘No Faulty circuits found’.

Figure 3 Faulty Circuit Listing GUI with no faulty ports

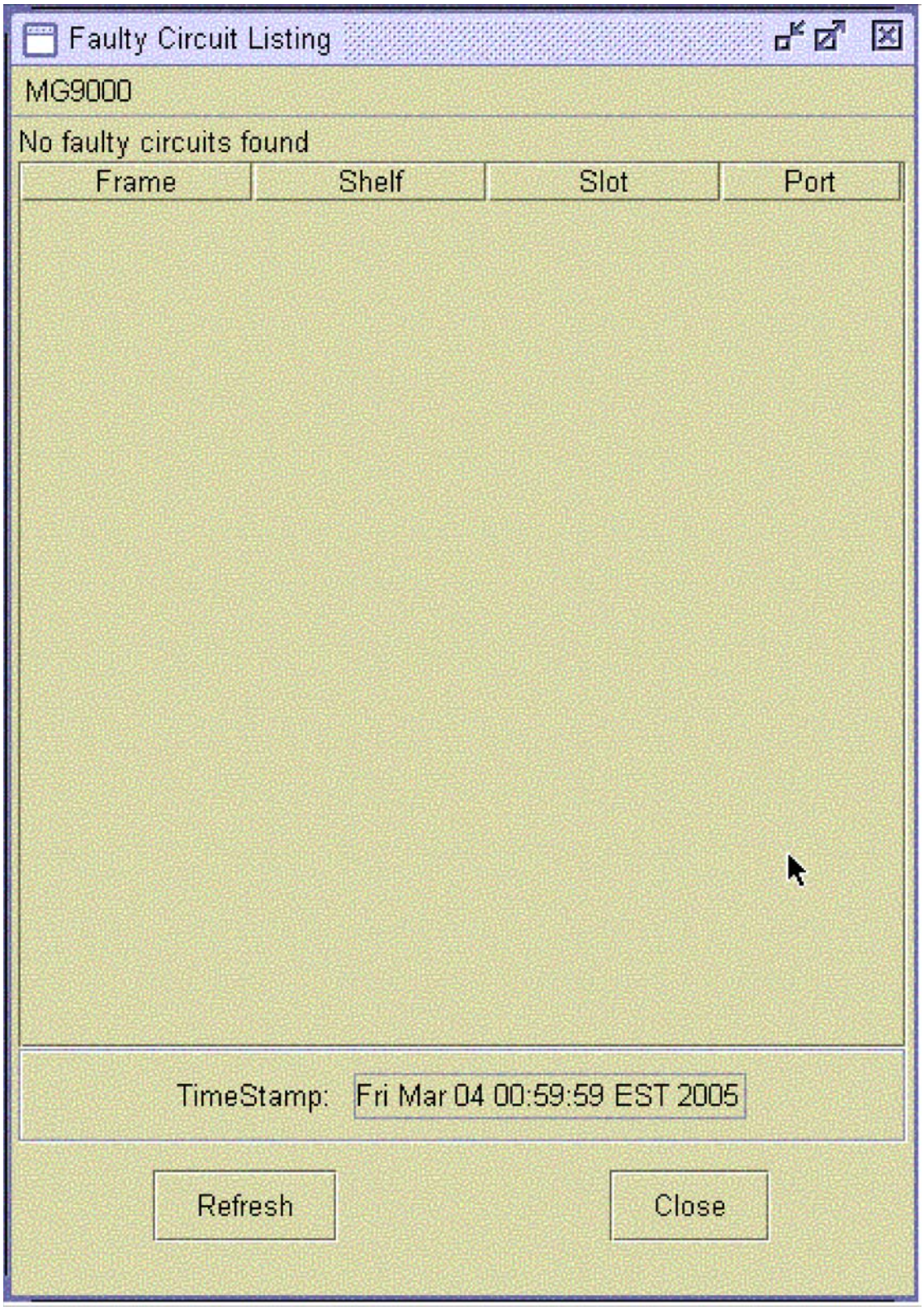
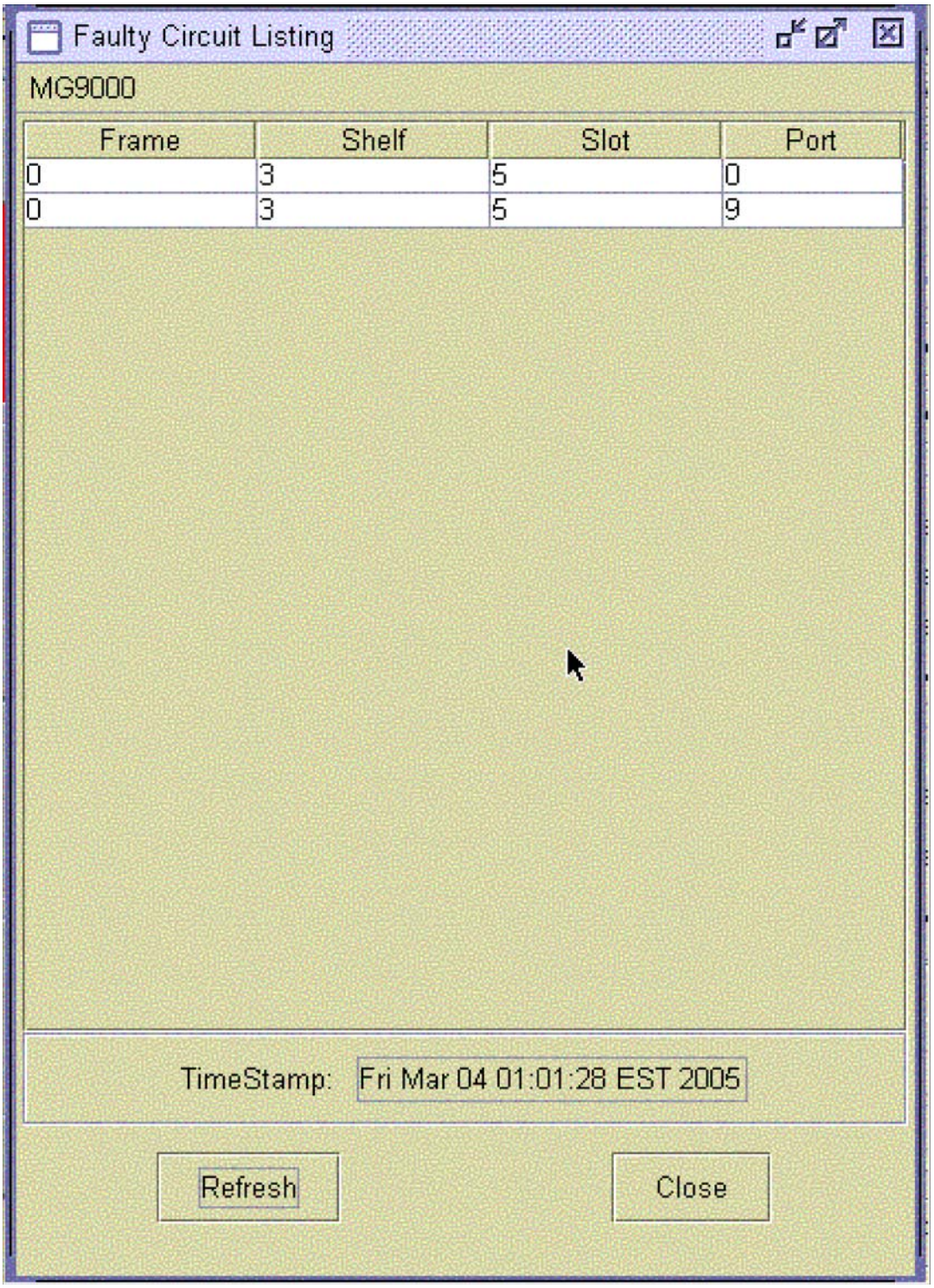


Figure 4 shows the ‘Faulty Circuit Listing’ gui when faulty ports exist. The Time Stamp field indicates the last time when the data was pulled from DB.

Figure 4 Faulty Circuit Listing



3.4.2.3.3 GUI size

3.4.2.3.4 GUI fields

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Faulty Circuit Listing View	1	1	

The following table lists the new fields for the Faulty Circuit Listing View.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Frame Number	New	NA	NA	The associated frame number of the faulty port	NA
Shelf Number	New	NA	NA	The associated shelf number of the faulty port	NA
Slot Number	New	NA	NA	The associated slot number of the faulty port	NA
Port Number	New	NA	NA	This field speaks about the faulty port number	NA

3.5 Security

NA

Product = MG 9000

A00011167 -- MG9KEM Central Userid and Password Support

Functional Description

1: Applicable Solution(s)

UA-IP, UA-AAL1

1.1 Description

This activity enables central IEMS/ Radius authentication of the MG9K userid and password for EM SFTP access to the MG9K. The userid and password will be configured on a per MG9K Element Manager (EM) basis in addition to an NE basis. If Radius is not available when the EM communicates with the MG9K, the NE-level userid and password will be used for authentication instead of the EM-level userid and password. If the Radius is available, there will not be an attempt to authenticate using the NE-level userid and password.

The same userid and password must be configured on the EM and Radius. At the EM, the EM-level userid and password will be configured using a new GUI that is accessed at the subnet level. A warning message will inform the user that the EM-level userid and password will be used instead of the NE-level userid and password. The EM-level userid and password will be stored in the EM Oracle database.

1.2 Hardware Requirements or Dependencies

None.

1.3 Software Requirements or Dependencies

This feature will be delivered in the SN09 software release.

1.4 Limitations and restrictions

For the Radius server authentication to work correctly, when the central userid and password is changed at the Radius server, the EM level userid and password must be changed to match the Radius central userid and password. Note that if an NE-level userid and password happens to match the Radius userid and password, the authentication will work if the Radius server is not available.

1.5 Interactions

None

1.6 Glossary

NA

2: Configuration for A00011167

2.1 Hardware and Software Requirements

This functionality is for an MG9K Element Manager (EM) that has SN09 or higher software version.

2.2 Initial Configuration

No changes.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

The EM (subnet) level userid and password configuration information is in the Element Manager section of this document.

2.4 Upgrade Considerations

2.4.1 Dump and Restore (CM)

NA

2.4.2 Element Management Upgrade

For an upgrade to SN09, the central userid and password will be defaulted to "mg9kadm/mg9kadm". The already-defined NE-level userid and passwords will not be affected by the upgrade and will be used as the second level of authentication as described previously.

2.4.3 Downgrade impact

During a downgrade, the central userid and password will no longer be configured and the NE-level userid and passwords will be the same as they were in the previous release, unless they have been changed by the customer after the upgrade.

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

The Office Wide Defaults table in the EM Oracle database will have two new rows used to store the EM-level userid and password: "centralid" and centralpw".

2.5.2 Table/MIB/Remote Database Schema information

NA

2.6 Service Orders (SO) (CM & SESM)

NA

2.7 Software optionality control (SOC)

NA

2.8 Element Management

The MG9K Element Manager will be used to define the EM-level userid and password.

2.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Subnet View	Changed
Subnet Level User Id and Password	New

2.8.2 GUI information

2.8.2.1 GUI name: Subnet View

2.8.2.1.1 Functional description

This GUI is used to manage EM data that pertains the all the NEs defined for the EM.

2.8.2.1.2 GUI usage and implications

There is no requirement to datafill GUIs in a specific order.

2.8.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Subnet View	1	1	NA

2.8.2.1.4 GUI fields

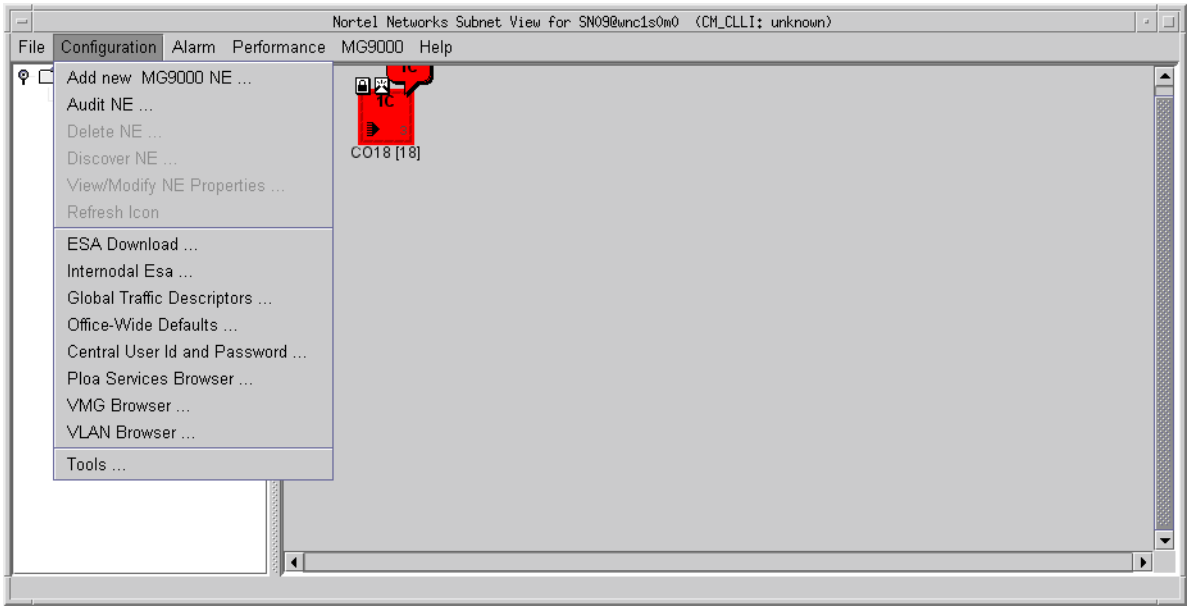
A new entry will be added to the Configuration pull-down menu on the Subnet View GUI. The following table lists fields for the pull-down menu in SubnetView.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Configuration	Changed	User Id and Password	NA - pull-down menu item	Selection of this item will open the User Id and Password GUI	NA

2.8.2.1.5 Usage example

The following figures show the Configuration level and User Id and Password GUIs.



2.8.2.1.6 GUI release history update

A new menu item, User Id and Password will be added to the pull-down Configuration menu.

Context sensitive launching information

The EM GUI is launched using JavaWebStart. There are no changes to the launching of the GUI.

2.8.2.1.7 Supplementary information

None.

2.8.2.2 GUI name: User Id and Password View

2.8.2.2.1 Functional description

This GUI is used define the subnet-level userid and password.

2.8.2.2.2 GUI usage and implications

There is no requirement to datafill GUIs in a specific order.

2.8.2.2.3 GUI size

Table 4 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
User Id and Password View	1	1	NA

2.8.2.2.4 GUI fields

The following table lists fields for the User Id and Password GUI. The ability to Apply data, Refresh data, and Close the GUI will also be provided via buttons at the bottom of the GUI.

Table 5 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
User Id	New	None	NA - pull-down menu	1- 32 characters (must be alphabetic characters or numbers)	NA
Password	New	None	NA - pull-down menu	1- 128 characters The entered data will not be visible to the user.	NA
Password (Verify)	New	None	NA - pull-down menu	1- 128 characters The entered data will not be visible to the user. This field must match what is entered in the Password field and is used to verify entry of the same password in both fields.	NA

2.8.2.2.5 Usage example

The GUI will contain three new editable fields, User Id, Password, and Password (Verify). When the password is entered, it will not be visible to the user and must be entered twice to confirm that the customer has entered it correctly. The GUI will contain Apply, Refresh, and Close buttons.

2.8.2.2.6 GUI release history update

The new User Id and Password GUI is created.

Context sensitive launching information

The EM GUI is launched using JavaWebStart. There are no changes to the launching of the GUI.

2.8.2.2.7 Supplementary information

When the user configures or changes the userid and/or password, an Information message will be output to indicate that the entered userid and password will be used instead of the NE-level userid and password.

2.8.3 CLUI Interface

NA

2.9 User interface changes

NA

2.10 OSSGate Interface Changes

NA

2.11 Security

This activity provides IEMS/ Radius authentication of the MG9K userid and password. The userid and password will be configured on a per MG9K Element Manager (EM) basis instead of only on an NE basis. If Radius is not available when the EM communicates with the MG9K, the NE-level userid and password will be used for authentication instead of the EM-level userid and password.

2.11.1 Network configuration

NA

2.11.2 Key management

NA

2.11.3 Protocol

NA

2.11.4 Authentication

The same EM-level userid and password must be entered at the IEMS/Radius server and at the EM GUI.

2.12 Configuration Walkthrough

To allow the IEMS/Radius server to provide central authentication of the MG9K userid and password, the same EM-level userid and password must be

entered at the IEMS/Radius server and at the EM GUI. This authentication is required during ESA or OM data transfer to the MG9K.

The following provides additional information and the recommended configuration.

- The NE-level userid is not configurable (mg9kadm) and passwords can be configured on a per-MG9K basis.
  - When customers change the NE-level account password of a MG9K, the corresponding MG9K's password must be updated via the MG9K EM.
  - Based on customers' security policies, the NE-level account passwords can be all different or the same. MG9K EM/MG9K does not ensure that all NE-level account passwords are all different or the same. They are managedly independently of each other by the customers.
- An office-wide central account should be created and managed separately.
  - It is recommended that customers name the account using a different ID (i.e., not 'mg9kadm').
  - The userid and password for this central account should be changed via IEMS (Radius) first and then must be updated via the SN09 MG9K EM to keep it in sync.
  - After the MG9K EM is upgraded to SN09, the MG9Ks should be upgraded.
  - After all the MG9Ks have been upgraded to SN09, the userid and password defined in Radius for SN08 should be removed.
  - Although MG9K does not support authorization in SN09, it is recommended that the SN09 central account be a member of the MGADM group.

Product = CS 2000 Management Tools

A00008522 -- SESM Support for SIP Lines

Functional Description

1: Applicable Solution(s)

UA-IP, MCS

1.1 Description

Feature A00008522 will deliver the lines flow through and pre-provisioning functionality in the Succession Element and Sub-element Manager (SESM) required for the Session Server (SS) integration with Succession. The design will be split into Nodes provisioning for SS virtual gateways (GWs), and lines provisioning for SIP terminations/users.

The Nodes provisioning feature component will provide for the provisioning of SS GWs. Nodes provisioning will also provide functionality to pre-provision the SIP terminations in the GWC-EM and to pre-provision LENs (Line Equipment Numbers) in XACore table LNINV. The Lines Provisioning component will provide flow through of service information entered at OSSGate (SERVORD+ commands). New line provisioning functionality will be delivered to allow line data to be transmitted to the SS Element Manager (SS-EM).

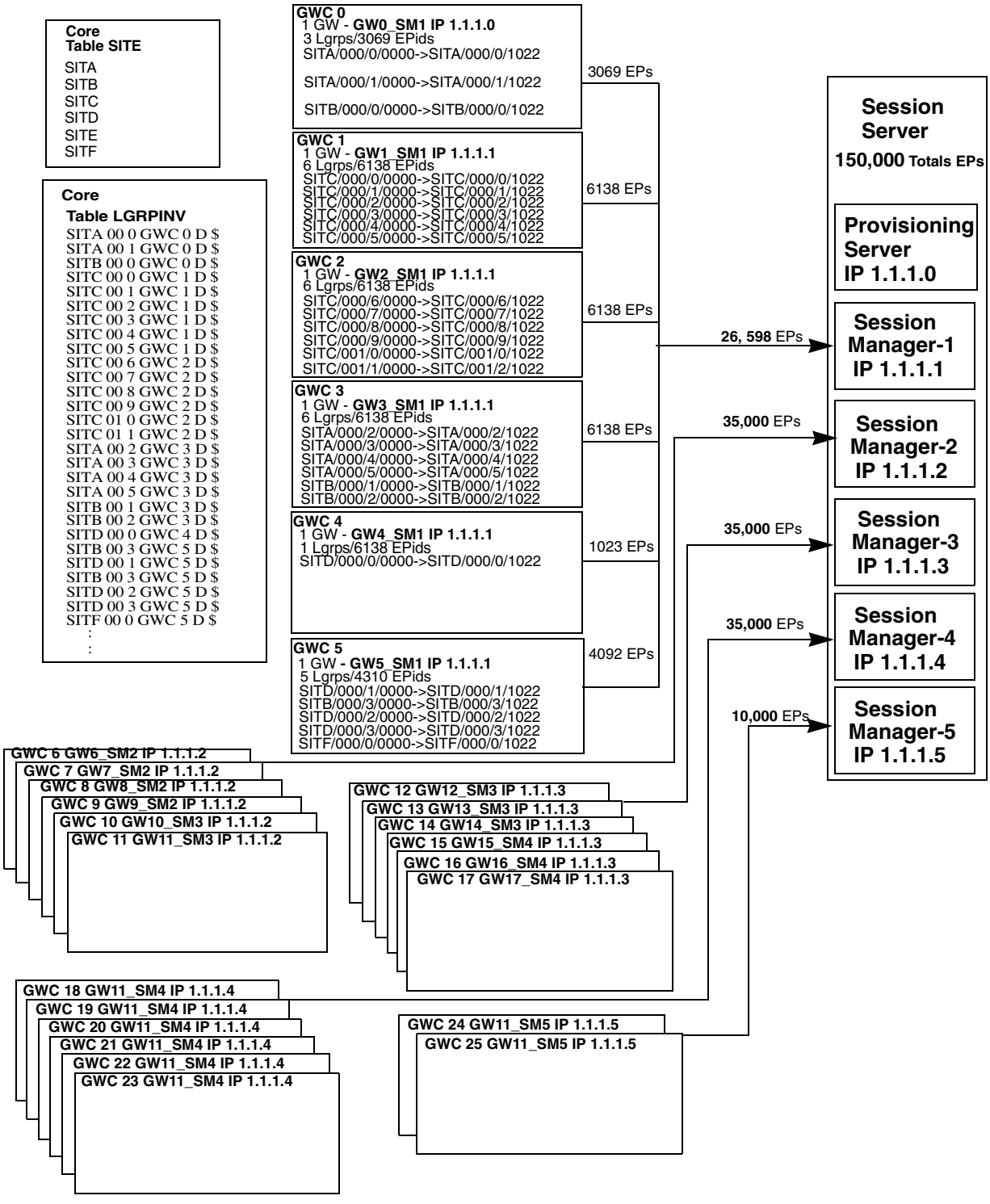
1.1.1 SS Provision Concepts

From figure 1, the interaction of various devices and tables is shown. Starting with the upper left is Table SITE in the CM. These site names are used to name line groups in the CS2KSS. This is performed during provisioning the GW.

From the example, GWC 0 has two GWs provisioned (also called a virtual gateway or VMG) called GW0_SM1 and GW1_SM2. More than GW is permitted on a GWC, as long as the GWs refer to different SS gateways. The GWC may support up to 12276 lines, or 12 LGRPs (12 LGRPs * 1023 endpoints per LGRP). These 12 LGRPs may be distributed over the 2 provisioned GWs in any fashion.

Note that multiple site names can be used in naming the LGRPs and the site names can span multiple GWs. The frame and group portions of the LGRP name are determined by the SESM/Nodes Provisioning and not by the user.

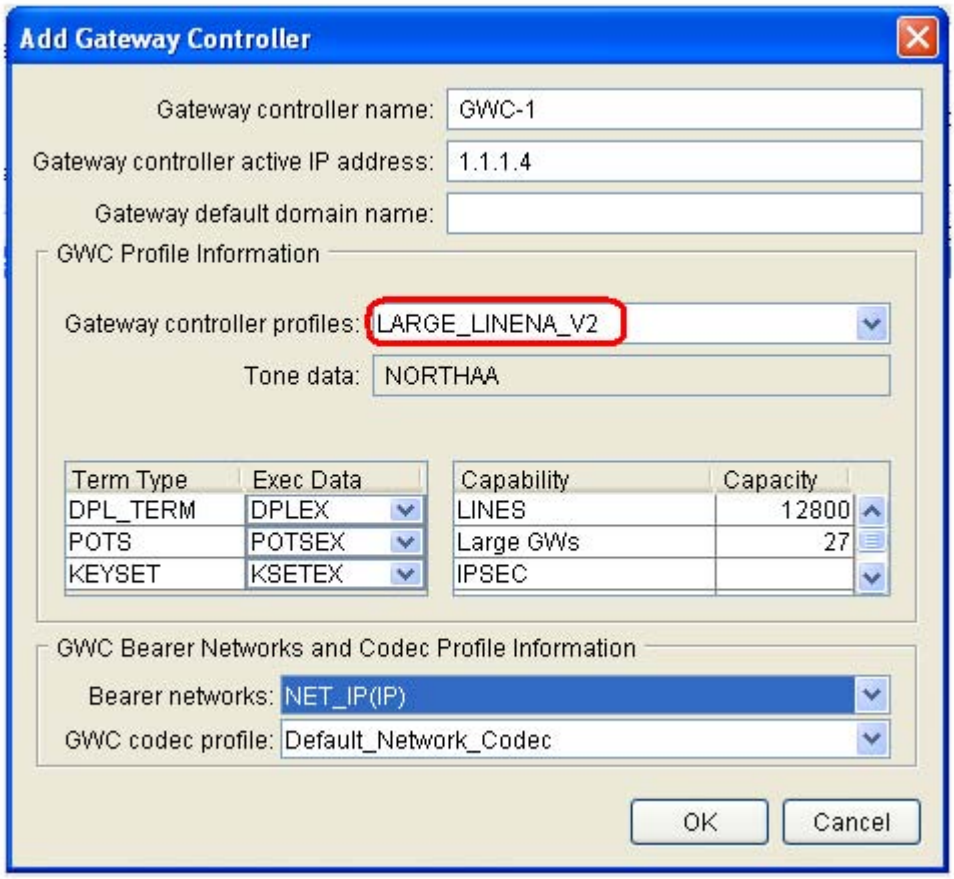
Figure 1 Example of MSM Provisioning Relationship


Core
Table SITE
SITA
SITB
SITC
SITD
SITE
SITF
Core
Table LGRPINV
SITA 00 0 GWC 0 D $
SITA 00 1 GWC 0 D $
SITB 00 0 GWC 0 D $
SITC 00 0 GWC 1 D $
SITC 00 1 GWC 1 D $
SITC 00 2 GWC 1 D $
SITC 00 3 GWC 1 D $
SITC 00 4 GWC 1 D $
SITC 00 5 GWC 1 D $
SITC 00 6 GWC 2 D $
SITC 00 7 GWC 2 D $
SITC 00 8 GWC 2 D $
SITC 00 9 GWC 2 D $
SITC 01 0 GWC 2 D $
SITC 01 1 GWC 2 D $
SITA 00 2 GWC 3 D $
SITA 00 3 GWC 3 D $
SITA 00 4 GWC 3 D $
SITA 00 5 GWC 3 D $
SITB 00 1 GWC 3 D $
SITB 00 2 GWC 3 D $
SITD 00 0 GWC 4 D $
SITB 00 3 GWC 5 D $
SITD 00 1 GWC 5 D $
SITB 00 3 GWC 5 D $
SITD 00 2 GWC 5 D $
SITD 00 3 GWC 5 D $
SITF 00 0 GWC 5 D $
GWC 0
1 GW - GW0_SM1 IP 1.1.1.0
3 Lgrps/3069 EPids
SITA/000/0/0000->SITA/000/0/1022
SITA/000/1/0000->SITA/000/1/1022
SITB/000/0/0000->SITB/000/0/1022
3069 EPs
GWC 1
1 GW - GW1_SM1 IP 1.1.1.1
6 Lgrps/6138 EPids
SITC/000/0/0000->SITC/000/0/1022
SITC/000/1/0000->SITC/000/1/1022
SITC/000/2/0000->SITC/000/2/1022
SITC/000/3/0000->SITC/000/3/1022
SITC/000/4/0000->SITC/000/4/1022
SITC/000/5/0000->SITC/000/5/1022
6138 EPs
GWC 2
1 GW - GW2_SM1 IP 1.1.1.1
6 Lgrps/6138 EPids
SITC/000/6/0000->SITC/000/6/1022
SITC/000/7/0000->SITC/000/7/1022
SITC/000/8/0000->SITC/000/8/1022
SITC/000/9/0000->SITC/000/9/1022
SITC/001/0/0000->SITC/001/0/1022
SITC/001/1/0000->SITC/001/2/1022
6138 EPs
GWC 3
1 GW - GW3_SM1 IP 1.1.1.1
6 Lgrps/6138 EPids
SITA/000/2/0000->SITA/000/2/1022
SITA/000/3/0000->SITA/000/3/1022
SITA/000/4/0000->SITA/000/4/1022
SITA/000/5/0000->SITA/000/5/1022
SITB/000/1/0000->SITB/000/1/1022
SITB/000/2/0000->SITB/000/2/1022
6138 EPs
GWC 4
1 GW - GW4_SM1 IP 1.1.1.1
1 Lgrps/6138 EPids
SITD/000/0/0000->SITD/000/0/1022
1023 EPs
GWC 5
1 GW - GW5_SM1 IP 1.1.1.1
5 Lgrps/4310 EPids
SITD/000/1/0000->SITD/000/1/1022
SITB/000/3/0000->SITB/000/3/1022
SITD/000/2/0000->SITD/000/2/1022
SITD/000/3/0000->SITD/000/3/1022
SITF/000/0/0000->SITF/000/0/1022
4092 EPs
Session Server
150,000 Totals EPs
Provisioning Server IP 1.1.1.0
Session Manager-1 IP 1.1.1.1
Session Manager-2 IP 1.1.1.2
Session Manager-3 IP 1.1.1.3
Session Manager-4 IP 1.1.1.4
Session Manager-5 IP 1.1.1.5
26, 598 EPs
35,000 EPs
35,000 EPs
35,000 EPs
10,000 EPs
GWC 6 GW6_SM2 IP 1.1.1.2
GWC 7 GW7_SM2 IP 1.1.1.2
GWC 8 GW8_SM2 IP 1.1.1.2
GWC 9 GW9_SM2 IP 1.1.1.2
GWC 10 GW10_SM3 IP 1.1.1.2
GWC 11 GW11_SM3 IP 1.1.1.2
GWC 12 GW12_SM3 IP 1.1.1.3
GWC 13 GW13_SM3 IP 1.1.1.3
GWC 14 GW14_SM3 IP 1.1.1.3
GWC 15 GW15_SM4 IP 1.1.1.3
GWC 16 GW16_SM4 IP 1.1.1.3
GWC 17 GW17_SM4 IP 1.1.1.3
GWC 18 GW11_SM4 IP 1.1.1.4
GWC 19 GW11_SM4 IP 1.1.1.4
GWC 20 GW11_SM4 IP 1.1.1.4
GWC 21 GW11_SM4 IP 1.1.1.4
GWC 22 GW11_SM4 IP 1.1.1.4
GWC 23 GW11_SM4 IP 1.1.1.4
GWC 24 GW11_SM5 IP 1.1.1.5
GWC 25 GW11_SM5 IP 1.1.1.5

1.1.2 Adding a GWC

1.1.2.1 Add GWC

GWCs for CS2K Session Server gateways are provisioned using either the Large_LineNA_v2 or Large_LineINTL_v2 GWC profile. These GWC profiles will cause a GWC to be added to the CM, table SERVRINV, with the exec lineup of DPLEX/DPL, POTSEX/POT and KSETEX/KEYSET.

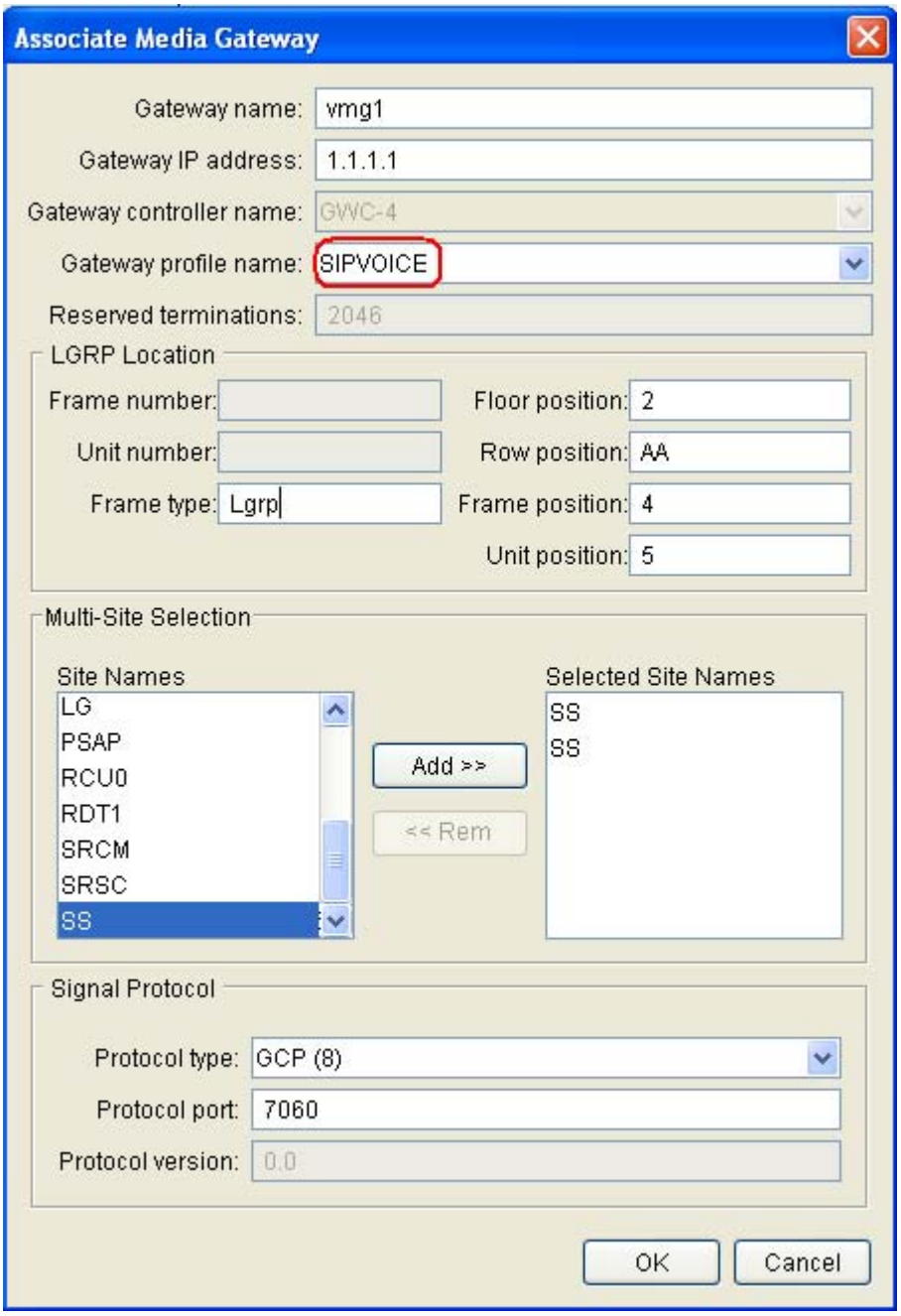


Also, the addition of these GWC profiles will update the GWC with a DPL enabled in the GWC configuration/capacity (GWC-PROFILE-MIB change).

1.1.2.2 Delete GWC

There are no changes required for this action.

1.1.2.3 Add GW



Adding a GW involves identifying a gateway name, IP address and selecting the SIPVOICE profile from the Gateway profile name list. The SIPVOICE selection causes an LGRP Location and Multi-Site Selection panel to appear.

The LGRP Location panel is used to provide the physical equipment location of the GW. LGRP_type is a string. Floor position, frame position and unit positions are all integers while row position is a char ‘A’ - ‘Z’, ‘AA’ or ‘AB’.

Below the LGRP Location panel is the Multi-Site Selection panel. Within this panel is a Site Names list and a Selected Site Names list. The Site Names list consists of all of the site names from table SITE in the CM. Site names are selected (placed in the Selected Site Name list) by simply clicking on the site name and selecting Add.

For SN09, a maximum of 12 site names can be selected. The same site name may be used multiple times by selecting Add several times.

Each site name represents one LGRP as defined by:

<site>/frame/group

Each LGRP is provisioned in table LGRPINV (CM) and represents 1023 endpoints. Each endpoint is added to table LNINV as:

<site> frame group terminal

where the terminal number ranges from 00 00 to 10 22.

The reserved termination field is updated as the Add button is selected.

The entries in the Signal Protocol panel are defaulted but can be changed.

Note: Adding a fully provisioned CS2K SS GW will require approximately 10 minutes, or 2 minutes per LGRP.

Note: Provisioning SIP GWs can only be performed one at a time. Attempts to provision multiple SIP GWs at the same time may cause all provisioning sessions to fail.

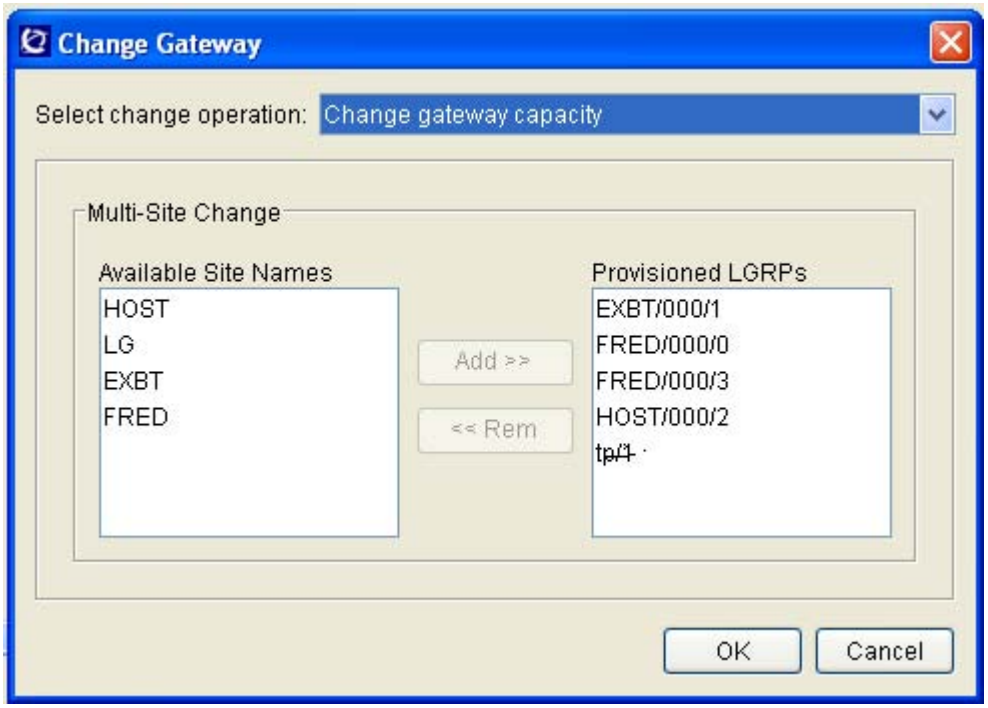
1.1.3 Design Solution / Module Flow Diagram

Addition of a GW includes (in order)

1. adding the GW to the GWC
2. adding one LGRP to LGRPINV (CM)
3. adding the associated endpoint groups (TN’s) for that LGRP to the GWC
4. adding the LENs to LNINV
5. Repeat steps 2-4 until all LGRPs have been added

1.1.3.1 Change GW

Figure 2 Change Gateway Capacity - Multi Site Dialog box



A gateway using the SIPVOICE profile will have the dialog box in figure 2 displayed. Similar to the AssocGW dialog box, this box contains two lists, Available Site Names on the left, which is a list of site names from the table SITE in the CM.

The second list, “Provisioned LGRPs”, is a list of site names already used and assigned. These site names have LGRPs and LENs assigned to it, therefore they show up with there respective frame and group numbers.

From this dialog box, the user can add additional site names (a maximum of 12 LGRP/Site names) are permitted in the Provisioned LGRPs list.

Additionally, the user can select to remove LGRP/Site names from the provisioned list simply by selecting them and the remove button.

Once the site names have been added, and OK selected, this diialog box will close and another panel will appear to display the progress and responses. The first item to display is the timeout value.

Cancel will close the box without executing any operation.

Note: Only single operations may be performed from the Change Gateway dialog; in other words, the user cannot add one site and remove another site in the same operation.

1.1.4 Configure

In the SESM, the /opt/nortel/NTsesm/admin/bin/configure tool should be used to configure SESM access to the Session Server Element Manager (SS-EM).

The configuration tool will prompt the user to enter the following:

- Transport protocol to SS-EM server (http/https - default is https). In SN09, only HTTPS is supported by the SS-EM, however flexibilty to choose HTTP is still provided to meet possible future needs.
- IP address / host name of primary SS-EM server
- IP address / host name of secondary SS-EM server. Some configurations may not include a secondary SS EM server. If so, configure the same information provided for the primary server (by default this should be the case).
- HTTP/HTTPS communication port to SS EM server (default 8080 for http, 8443 for https).
- The OPIClient version. This is mapped to the SS EM load version. In SN09, the appropriate value will be “9.0”. The OPIClient version should be incremented each release in steps of 1.0 i.e, 9.0, 10.0...15.0
- SS-EM Provisioning Manager administrator user name
- SS-EM Provisioning Manager administrator password

The IP address and port will be used to generate the SS-EM Provisioning Manager URL which in turn will be added to sesm.properties file.

As part of the configuration, the IP address will be validated for format, range and reachability. Other user entered data will be validated for format, range, values etc.

The user name will be added to sesm.properties as clear text.

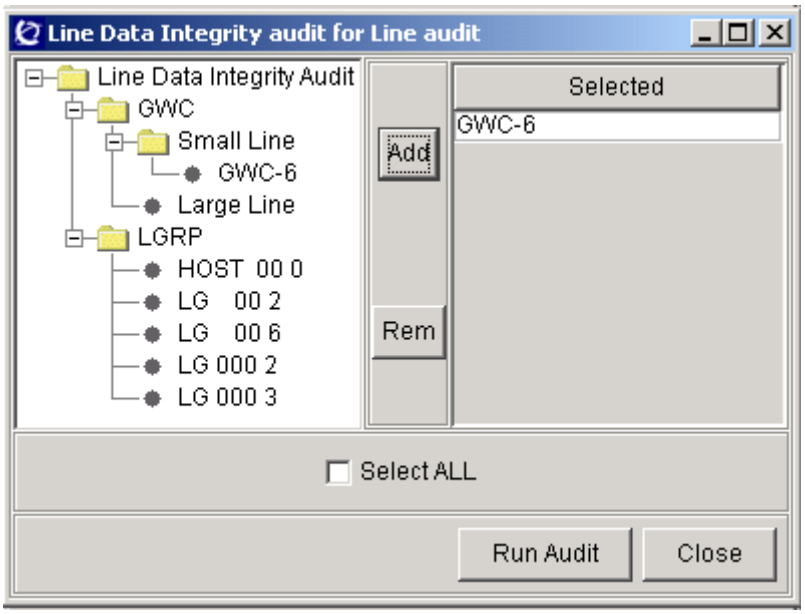
The password will be stored separately and accessible only to the root user.

All configuration information (url, username, etc.) except password can be displayed by using the SESM “/opt/nortel/NTsesm/admin/bin/configure” tool.

1.1.5 Audits

- Add a new gui to provide support for audit by GWCs, GWs or LGRPs. Only support Line Data Integrity audit now.

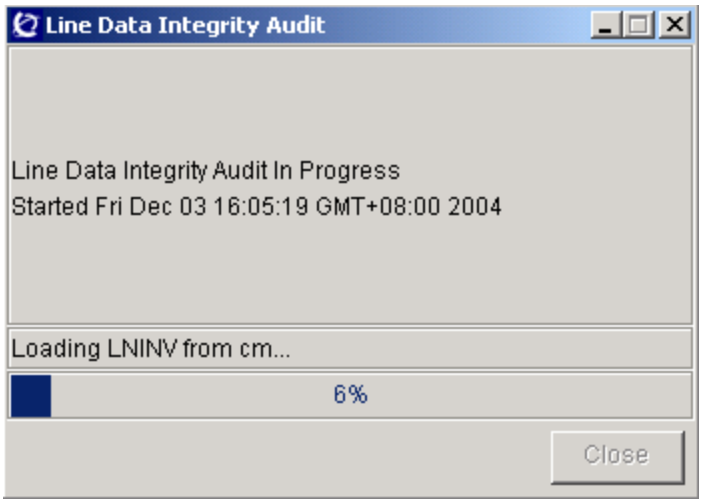
When users select “Line Data Integrity Audit” and press the “Run Audit” button in Audit System gui, the following gui will be displayed.



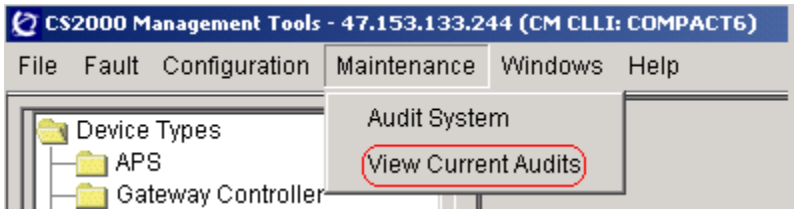
- User can select the gwc, gw or lgrp in the left tree and add them to the selected table by press the “Add” button.
- User can select the gwc, gw or lgrp in the right table and delete them from the table by press the “Rem” button.
- User can select all datas to do audit by select checkbox “Select All”. When user select the datas to do audit, the “Run Audit” button will be highlight.
- After user selected the data and press “Run Audit” button, the audit will be run as before.

- Add a progress bar in “Run Audit” gui to indicate the progress of the running audit.

Add a label to show current operation.

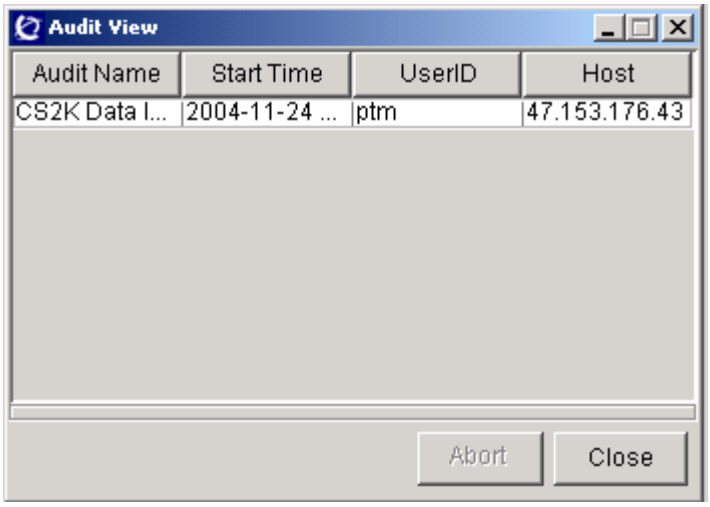


- Add a new menu in Maintenance of Cs2kmt to provide the new function “Abort Audit”.



When user selected the menu “View Current Audits”, another new gui will be displayed.

- Add a new gui to provide the new function “Abort Audit”.



The running audits will be displayed in this gui. The data of the audits include: Audit Name, Start Time, UserID, Host.

User can selected a running Audit and press the “Abort” button to abort the audit.

1.2 Hardware Requirements or Dependencies

Not applicable.

1.3 Software Requirements or Dependencies

This actrivity requires that the following components are loaded with SN09 or equalivalent loads.

CM, XAC or 3PC

GWC

MSM

1.4 Limitations and restrictions

None.

1.5 Interactions

This feature will integrate the SIP client provisioning with the existing Succession SERVORD+ system. SIP client commands/data are distributed to the SS-EM from the SERVORD+ system within the SESM. The following commands will trigger data distribution to the SS-EM from SESM SERVORD+ when SS vmgs/endpoints are found within the command: NEW, OUT, CHF

NOTE: CHF requires the use of gateway/termination names (or the equivalent LEN) in order to trigger flow through for SS lines. Use of DN will result in the command being processed only by the CM.

Query commands QLEN/QTP and QDN (which return formatted line/service information) will include the SIP_DATA options provisioned via the NEW/CHF commands in their output. The SIP_DATA option information will be appended to the end of the existing QLEN/QDN output, but prior to the dashed line (eg. “----------”) query output terminator line.

New data tags presented in query output with sample values:

END POINT DATA: *(This is the endpoint data header, no info/value associated with this tag)*

SIP_CLIENT_TYPE: SIP Line

SIP_EP_NAME: SCOT/000/0/0000

SIP_VMG_NAME: vmg1

SIP_DN: 6195209998

SIP_LOCATION: Nortel Networks.RTP.NC0

SIP_PACKAGE: SIP Lines

SIP_URI: slynch@mordor.com

See query examples in the next section for details on presentation and positioning within query output.

1.5.1 SERVORD+ Command Examples

See Configuration Section for SIP_DATA option format details and provisioning rules.

1.5.1.1 NEW command Examples:

NEW $ 6195209998 1FR LATA1 0 **SCOT 00 0 00 00** dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI slynch@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD scott11 $ DPL Y 10 $

NEW $ 6195209998 1FR LATA1 0 **vmg1 SCOT/000/0/0000** dgt SIP_DATA SIP_PACKAGE SIP Lines SIP_URI slynch@mordor.com SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD scott11 $ DPL Y 10 $

1.5.1.2 CHF Command Examples

CHF $ SCOT 00 0 00 00 SIP_DATA SIP_PACKAGE siplines SIP_PASSWD scott11 SIP_CLIENT_TYPE IBN SIP_LOCATION IBM.RTP $ $

CHF $ **vmg1 SCOT/000/0/0000** SIP_DATA SIP_PACKAGE siplines SIP_PASSWD scott11 SIP_CLIENT_TYPE IBN SIP_LOCATION IBM.RTP $ $

1.5.1.3 OUT Command Examples

OUT $ 6195209998 SCOT 00 0 00 00 BLDN

OUT $ 6195209998 **vmg1 SCOT/000/0/0000** BLDN

1.5.1.4 Query Examples

```
> QLEN SCOT  00 0 00 00

------------------------------------------------------------------------------

LEN:     SCOT  00 0 00 00

END POINT: vmg1  SCOT/000/0/0000
```

```
TYPE: SINGLE PARTY LINE
SNPA: 619
DIRECTORY NUMBER:     5209998
LINE CLASS CODE:      1FR
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     0
LINE ATTRIBUTE INDEX:     0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: Y
PM NODE NUMBER     :    87
PM TERMINAL NUMBER :    1
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA
END POINT DATA:
SIP_CLIENT_TYPE: SIP Line
SIP_EP_NAME: SCOT/000/0/0000
SIP_VMG_NAME: vmg1
SIP_DN: 6195209998
SIP_LOCATION: Nortel Networks.RTP.NC0
SIP_PACKAGE: SIP Lines
SIP_URI: slynch@mordor.com
--------------------------------------------------------------------------------

> qdn 5209998
--------------------------------------------------------------------------------
DN:     5209998
TYPE: SINGLE PARTY LINE
SNPA: 619   SIG: DT    LNATTIDX: 0
LINE EQUIPMENT NUMBER:     SCOT  00 0 00 00
END POINT: vmg1  SCOT/000/0/0000
LINE CLASS CODE:      1FR
LINE TREATMENT GROUP:     0
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: Y
PM NODE NUMBER     :    87
PM TERMINAL NUMBER :    1
OPTIONS:
DGT DPL Y 10
OFFICE OPTIONS:
SRA

END POINT DATA:
SIP_CLIENT_TYPE: SIP Line
SIP_EP_NAME: SCOT/000/0/0000
```

```
SIP_VMG_NAME: vmg1
SIP_DN: 6195209998
SIP_LOCATION: Nortel Networks.RTP.NC0
SIP_PACKAGE: SIP Lines
SIP_URI: slynch@mordor.com
--------------------------------------------------------------------------------
```

1.6 Glossary

Term	Description
New term	Definition

2: Configuration for A00008522

2.1 Hardware and Software Requirements

This feature requires the 905-240 GWC card, pec code NTRX51DL. It also requires that the CM, GWC SESM and MCS gateways are on a SN09 load.

2.2 Initial Configuration

2.2.1 SESM-CS2K Prov Mgr EM Server Configuraion

In the SESM, the /opt/nortel/NTsesm/admin/bin/configure tool should be used to configure SESM access to the Session Server Element Manager (SS-EM).

The configuration tool will prompt the user to enter the following:

- Transport protocol to SS-EM server (http/https - default is https). In SN09, only HTTPS is supported by the SS-EM, however flexibilty to choose HTTP is provided to meet possible future needs.
- IP address / host name of primary SS-EM server
- IP address / host name of secondary SS-EM server. Some configurations may not include a secondary SS EM server. If so, configure the same information provided for the primary server (by default this should be the case).
- HTTP/HTTPS communication port to SS EM server (default 8080 for http, 8443 for https).
- The OPIClient version. This is mapped to the SS EM load version. In SN09, the appropriate value will be “9.0”. The OPIClient version should be incremented each release in steps of 1.0 i.e, 9.0, 10.0...15.0
- SS-EM Provisioning Manager administrator user name

- SS-EM Provisioning Manager administrator password

The IP address and port will be used to generate the SS-EM Provisioning Manager URL which in turn will be added to sesm.properties file.

As part of the configuration, the IP address will be validated for format, range and reachability. Other user entered data will be validated for format, range, values etc.

The user name will be added to sesm.properties as clear text.

The password will be stored separately and accessible only to the root user.

All configuration information (url, username, etc.) except password can be displayed by using the SESM "/opt/nortel/NTsesm/admin/bin/configure" tool.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not Applicable.

2.4 Upgrade Considerations

TBD.

2.4.1 Dump and Restore (CM)

Not Applicable.

2.4.2 Element Management Upgrade

The MSM gateway is new to SN09. Upgrading from SN08 or fresh install of SN09 will add the required fields necessary to support the MSM Gateway.

2.4.3 Downgrade impact

No impact - works as per current process.

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
SERVRINV	CHANGED	N/A
LGRPINV	CHANGED	N/A
LNINV	CHANGED	N/A
GWC-PROFILE_MIB	CHANGED	N/A
NORTEL-GWC-COMMON-TC	CHANGED	N/A

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name: SERVRINV

Server Inventory

2.5.2.1.1 Functional description

In SN09, the field TERM_EXEC_TC_TAB of the table SERVRINV includes DPLEX with a DLP termtype for GWCs defined with Large_LineNA_v2 and Large_LineINTL_v2 GWC profiles.

2.5.2.1.2 Usage sequence and implications (CM Only)

The table SERVRINV is provisioned by the SESM. No manual datafill or change is allowed. Manual changes to this table will cause data corruption.

2.5.2.1.3 Size

Not applicable.

2.5.2.1.4 Fields/OIDs

Not applicable. This feature will use an already defined and supported field.

2.5.2.1.5 Datafill example

The following example shows sample datafill for table SERVRINV:

GWC 167 IP 47 4 4 4 DPL DPLEX POTS POTSEX KEYSET KSETEX $ NORTHAA $ NET_IP Y $ $

2.5.2.1.6 Table release history update

Not applicable.

2.5.2.1.7 Supplementary information
Not applicable.

2.5.2.1.8 Translation verification other tools
Not applicable.

2.5.2.2 Name: LGRPINV
Logical Group Inventory

2.5.2.2.1 Functional description
In SN09, the field GRPTYPE of the table LGRPINV is set to “SSDPL” for SIP; logical groups will be used to indicate that the logical group is assigned to a CS2K SS gateway.

2.5.2.2.2 Usage sequence and implications (CM Only)
The table LGRPINV is provisioned by the SESM. No manual datafill or change is allowed. Manual changes to this table will cause data corruption.

2.5.2.2.3 Size
Not applicable.

2.5.2.2.4 Fields/OIDs
Not applicable. This feature will use an already defined and supported field.

2.5.2.2.5 Datafill example
The following example shows sample datafill for table LGRPINV.

Preprovisioned SIP Lines : SITE 00 0 GWC 3 DPL_GRP $

Where SITE represents an entry from the table SITE in the CM.

2.5.2.2.6 Table release history update
Not applicable.

2.5.2.2.7 Supplementary information
Not applicable.

2.5.2.2.8 Translation verification other tools
Not applicable.

2.5.2.3 Name: LNINV
Line Inventory

2.5.2.3.1 Functional description
There are no software/functional changes to table LNINV. This section will describe the datafill.

```
(GRPTYPE SITE)  SITE                        4 char name

(GRPTYPE DPL_GRP) FRAME NUMBER              {0 TO 511}

(GRPTYPE DPL_GRP) LINE SUBGROUP             {0 TO 9}

(GRPTYPE DPL_GRP) SLOT                      {00 TO 10}

(GRPTYPE DPL_GRP) CIRCUIT                   {00 TO 99}*

*00 - 23 when SLOT = 10
```

2.5.2.3.2 Usage sequence and implications (CM Only)

Entries will be automatically configured by SESM at MSM gateway provisioning time.

2.5.2.3.3 Size

Not applicable.

2.5.2.3.4 Fields

Not Applicable.

2.5.2.3.5 Datafill example

The following example shows sample datafill for table LNINV.

Preprovisioned SIP line (North American):

SITE 00 0 21 31 RDTLSG PKLNL HASU N NL N NIL

Preprovisioned SIP line (International):

SITE 00 0 21 31 GWLPOT PKLNL HASU N NL N NIL

2.5.2.3.6 Table release history update

Not applicable.

2.5.2.3.7 Supplementary information

Not applicable.

2.5.2.3.8 Translation verification other tools

Not applicable.

2.6 Service Orders (SO) (CM & SESM)

No new service orders are created under this activity, however several new options are defined which can be used in NEW/CHF commands applicable to SIP lines hosted off of MSM VMGs.

All listed may also be used via the Bulk Provisioning Tool.

2.6.1 Service order change details

LCC and options

(SESM)
A new SIP_DATA option is introduced by this feature. The SIP_DATA option is a SERVORD+ option which is not presented to XACore SERVORD (it is removed from the command prior to XACore SERVORD command processing).

2.6.1.1 Option Format:

SIP_DATA sub-options-and-values $

where

sub-options = SIP_CLIENT_TYPE, SIP_URI, SIP_PASSWD, SIP_PACKAGE, SIP_LOCATION

The SIP_DATA option and sub-option **tags** (but not their values, see later restrictions) may be entered in either lower or upper case transparently.

Note: sub-option values have external case restrictions. See "Usage/Format Validation and Rules" in a subsequent section.

2.6.1.2 Sub-option value formats:

SIP_CLIENT_TYPE option value format = {one or more token_string_values}

SIP_URI option value format = {token_string_value, format uservalue@domainnamevalue}

SIP_PASSWD option value format = {token_string_value}

SIP_PACKAGE option value format = {one or more token_string_values}

SIP_LOCATION option value format = {one or more token_string_values}

2.6.1.3 SIP_DATA Sub-option and Value Examples:

"SIP_DATA SIP_PACKAGE test package $"

"SIP_DATA SIP_PACKAGE test package SIP_URI someone@somecompany.com $"

"SIP_DATA SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP.NC0 SIP_PASSWD test1password $"

2.6.1.4 Usage/Format Validation and Rules

OSSGate/SERVORD+ SIP_DATA validation will be limited. SessionServer-EM will be responsible for validating the actual value contents.

2.6.1.4.1 Rules Enforced for SIP Data by OSSGate/SERVORD+

Breaking these rules causes immediate command failure/rejection by OSSGate/SERVORD+:

- One or more sub-options are REQUIRED when the SIP_DATA option is specified.
- Sub-option tags are reserved words and may not be used as values for other sub-options or for any non-related types (eg. CM customer group, gateway names, etc.). For example, “SIP_PASSWORD sip_password” is an invalid option and value pair. “sip_password” may not be used as the value specified for the SIP_PASSWORD sub-option. “sip_password” may not be used as a part or whole value for any other sub-option (e.g. “SIP_LOCATION sip_passwd” will be rejected).
- The SIP_DATA terminator, “$”, is a reserved token and may not be used as a value of any SIP_DATA sub-option. If a sub-option is present in the SIP_DATA options list, then it must have a valid value other than “$”.
- The tag-value pair relationship for the options/sub-options will be enforced from a simple format perspective. All sub-options must have associated values. The overall SIP_DATA option must be terminated by a “$”.
- Multiple/extraneous SIP_DATA options or sub-options found in a single NEW/CHF/etc command, will result in rejection of the command by OSSGate/SERVORD+.
- SIP_URI must be of the format user@domain. The domain information is parsed from the URI value. A missing domain (e.g. missing @ delimiter or domain information) will cause immediate command failure. An invalid domain name specified will be rejected by the Session Server Provisioning Manager.
- SIP_LOCATION must be included in the SIP_DATA option when the command issued results in the creation of a new user on the Session Server. In SN09, this applies only to the NEW command.

2.6.1.4.2 Rules NOT Explicitly Enforced for SIP Data by OSSGate/SERVORD+

These rules are not explicitly enforced by OSSGate/SERVORD+. Breaking these rules may cause command failures or other unintended consquences:

- SIP_DATA and the associated sub-option tags are reserved words and may not be used as values for any non-related types (eg. CM customer group, gateway names, etc.). Use of the reserved keywords in this manner may cause unexpected problems when attempting to use OSSGate/SERVORD+ for provisioning ANY type of line.

- CHF commands affecting SIP_DATA on SIP lines requires that gateway/termination names (or associated LEN) be used in the command instead of DN. Use of DN will result in the command being processed only by the CM, which is undesirable when SIP_DATA is present in the command.
- Use of the SIP_DATA option is not supported in commands which do not affect SIP lines or in commands which are not supported for flowthrough **for** SIP lines. Use of the SIP_DATA option in these commands may cause unintended command failures.
- The SIP_DATA option may fall anywhere in the command string except as the first token (which is reserved for the command name), however it is ***highly recommended*** that the SIP_DATA option be placed in the normal option field range of the command.
- The values assigned to sub-options SIP_CLIENT_TYPE, SIP_PACKAGE, and SIP_LOCATION are ***automatically normalized to lower case by OSSGate/SERVORD+*** (e.g. SIP_CLIENT_TYPE value "SIP Line" received at OSSGate will be normalized to "sip line" prior to transfer to the Session Server Provisioning Manager). **When commissioning these associated values on the Session Server Provisioning Manager, you MUST use lower case text.** Failure to commission these values in the Session Server Provisioning Manager using lower case text will result in command failures at OSSGate/SERVORD+.
- SIP_URI is normalized to lower case by the Session Server Provisioning Manager when received from OSSGate/SERVORD+. Caseless comparisons are performed by the Session Server Provisioning Manager when determining if a URI entered at OSSGate is already in use (e.g. "Slynch@Nortel.com" is considered identicle to "slynch@nortel.com" from the Session Server Provisioning Manager's perspective). Only the normalized/lower-case URI is stored by the Session Server Provisioning Manager (e.g. "USERname1@Domain1.net" received from OSSGate/SERVORD+ would be stored as "username1@domain1.net" in the Session Server Provisioning Manager).

2.6.1.5 Data Mapping Example

In the following command,

LEN: MSM1 00 0 00 00

is mapped to

VMG: TestMSMVMG.1

termination/endpoint: MSM1/000/0/0000

OSSGate command:

NEW $ 9195200500 IBN PRADEFAULT 0 0 LATA1 0 MSM1 00 0 00 00 + DPL Y 10 SIP_DATA SIP_PACKAGE test package SIP_PASSWD + test1Password SIP_URI someone@somecompany.com + SIP_CLIENT_TYPE SIP Line SIP_LOCATION Nortel Networks.RTP $ $

XACore SERVORD command derived from OSSGate command:

NEW $ 9195200500 IBN PRADEFAULT 0 0 LATA1 0 MSM1 00 0 00 00 + DPL Y 10 $

Data sent to SS-EM:

VMG: TestMSMVMG.1

termination: MSM1/000/0/0000

Domain: somecompany.com

User: someone

Password: test1Password

firstName: SIPLineUser (default value)

lastName: SIPLineUser (default value)

Package: test package

locale: English (default value)

timezone: Eastern Standard Time (default value)

clientType: SIP Line

DN: 9195200500

location: Nortel Networks.RTP

status: ACTIVE (default value)

2.6.2 New commands

Not Applicable.

2.6.3 Line equipment format changes

2.6.3.1 LEN

No LEN format changes are introduced by this feature. Typical LEN format for SS LENs:

SITE FFF G TT tt

SITE = SITE name

FFF = frame number, 0-511

G = group number, 0-9

TT tt = terminal, 00 00 - 10 23

2.6.3.2 Media gateway endpoint format

No gateway/endpoint format changes are introduced by this feature. Typical SS VMG and endpoint formats:

VMG = 64 character free-form string (eg. TestSSVMG.1)

endpoint/termination = SITE/FFF/G/TTtt

where SITE, FFF, G, and TTtt value are as specified in the SS LEN format.

- The LEN's individual TT tt values will always be zero-padded to 2 digits when converted to an endpoint/termination name (e.g. TT tt value "2 7" would be converted to an endpoint/termination TTtt value of "0207").
- The LEN's FFF value will always be zero-padded to 3 digits (e.g. FFF value "6" would be converted to endpoint/termination FFF value "006").

2.7 Software optionality control (SOC)

2.8 Element Management

SESM

2.8.1 New/modified GUIs

Table 2 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Associate Gateway	**CHANGED**
Change Gateway	**CHANGED**
View Current Audits	**NEW**

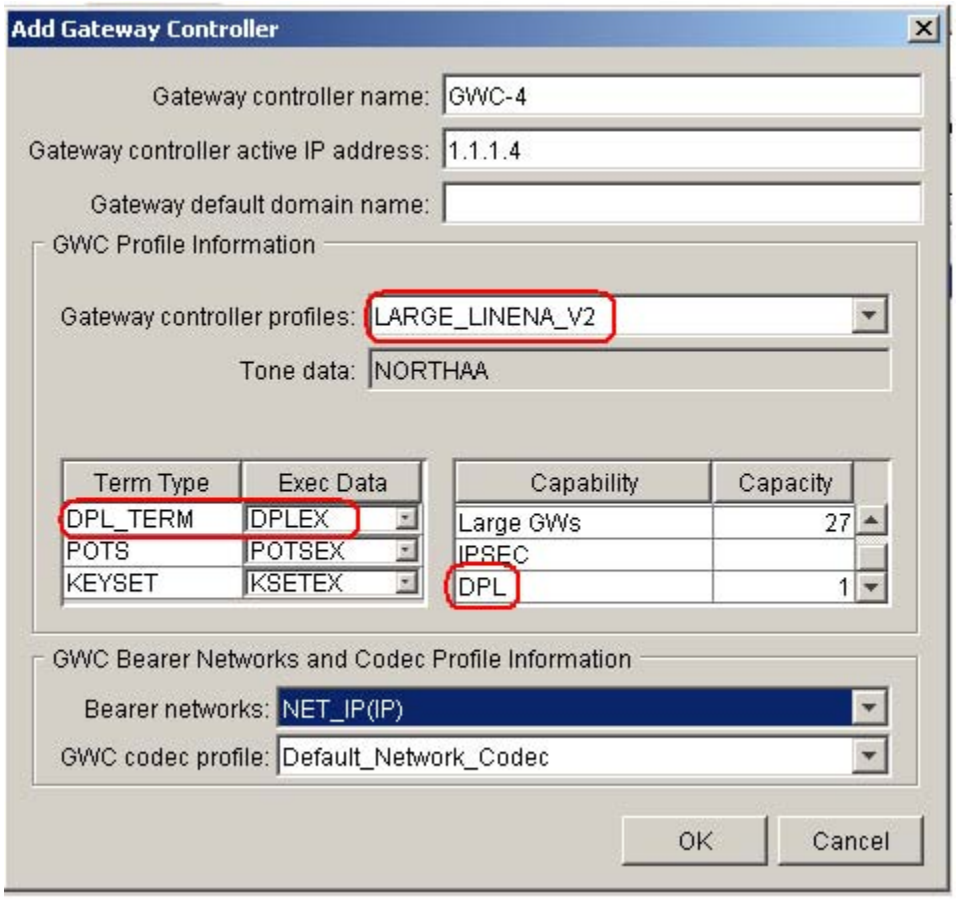
Table 2 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Line Data Integrity Audit	**NEW**
Run Audit	**CHANGED**

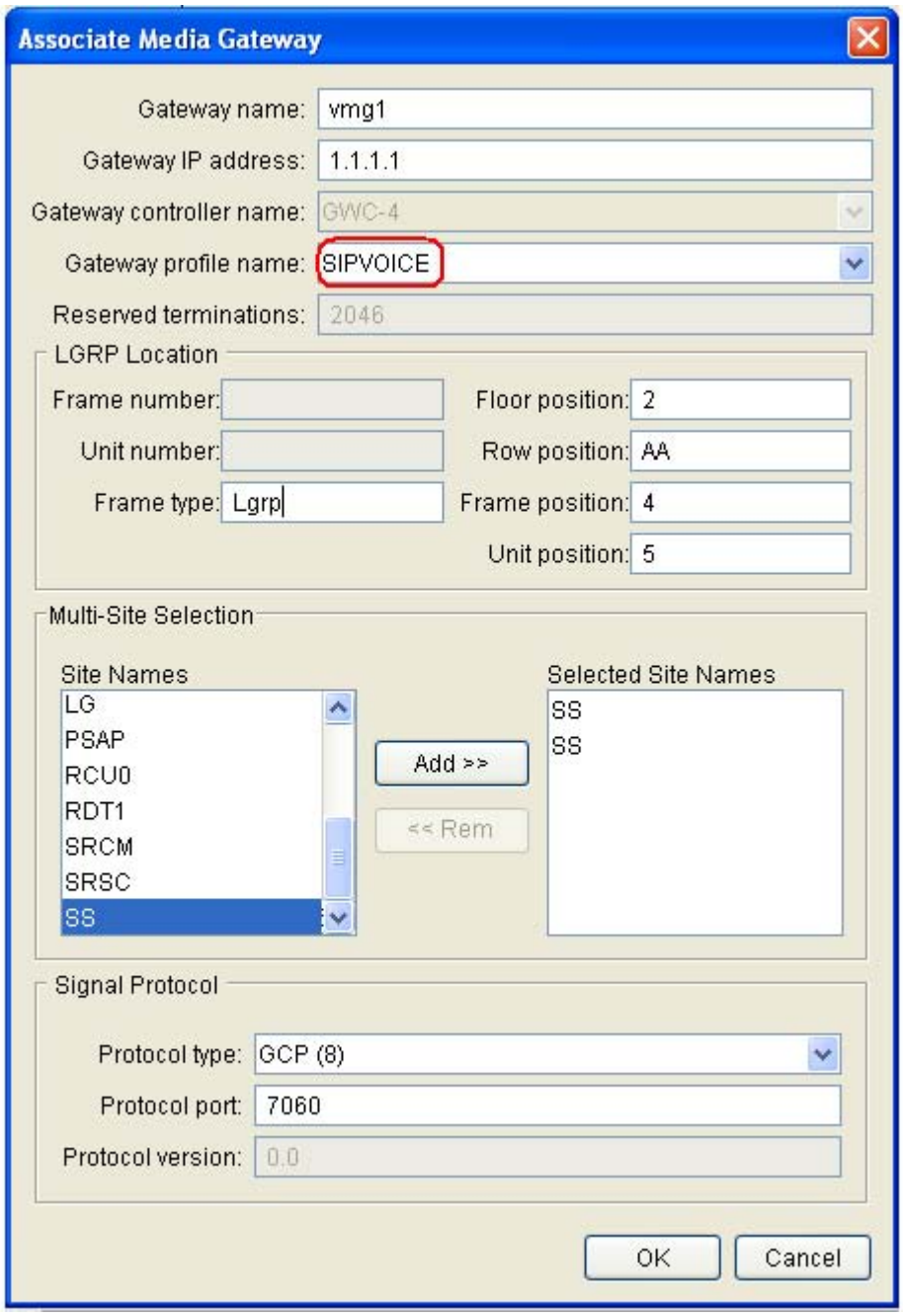
2.8.2 GUI information

2.8.2.1 GUI Name: Add GWC

GWCs for CS2K Session Server gateways are provisioned using either the Large_LineNA_v2 or Large_LineINTL_v2 GWC profile. These GWC profiles will cause a GWC to be added to the CM, table SERVRINV, with the exec lineup of DPLEX/DPL, POTSEX/POT and KSETEX/KEYSET)refer to diagram below).



2.8.2.2 GUI name: Associate Gateway



2.8.2.2.1 Functional description

Adding a GW involves identifying a gateway name, IP address and selecting the MSM profile from the Gateway profile name list. The MSM selection causes a Multi-Site Selection panel to appear.

The LGRP Location panel is used to provide the physical equipment location of the GW. LGRP_type is a string. Floor position, frame position and unit positions are all integers while row position is a char ‘A’ - ‘Z’, ‘AA’ or ‘AB’.

Below the LGRP Location panel is the Multi-Site Selection panel. Within this panel is a Site Names list and a Selected Site Names list. The Site Names list consists of all of the site names from table SITE in the CM. Site names are selected (placed in the Selected Site Name list) by simply clicking on the site name and selecting Add.

For SN09, a maximum of 12 site names can be selected.

Each site name represents one LGRP as defined by:

<site>/frame/group

Each LGRP is provisioned in table LGRPINV (CM) and represents 1023 endpoints. Each endpoint is added to table LNINV as:

<site> frame group terminal

where the terminal number ranges from 00 00 to 10 22.

The Root Zone Selection panel is used to provision middleboxes.

The reserved termination field is updated once the OK button is selected. The entries in the Signal Protocol panel are fixed (cannot be changed).

Note: Adding a fully provisioned CS2KSS GW will take about 45 mins (12 LGRPs).

Note: Provisioning SIP GWs can only be performed one at a time. Attempts to provision multiple SIP GWs at the same time may cause all provisioning sessions to fail.

2.8.2.2.2 GUI usage and implications

This GUI is used only to add an MSM gateway.

2.8.2.2.3 GUI size

Not applicable.

2.8.2.2.4 GUI fields

The Multi site Selection panel is only visible if the MSM profile is selected from the Gateway Profile list.

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Site Names	New	none	Site name values from the CM	Site Names	None
Selected Site Names	New	none	Site names selected from the Site Name list	Selected Site Names	None

2.8.2.2.5 Usage example

There are two ways to access the above Associate Gateway GUI:

- From the CS2000 Management Tools GUI, select Configuration from the top menu and select Associate Media Gateway from the pull down
- From the Gateway tab, in the lower portion of the GUI, select the "Associate.." button

From the Associate Gateway panel:

1. Add the gateway name - up to 64 characters, can be "." or "/" delineated,
2. Input the IP address of the MSM Service Manager,
3. If the Associate Gateway panel was opened via the CS2000 Management Tools menu bar then the Gateway Controller name will need to be entered,
4. Select MSM from the Gateway profile name. The Site name box will disappear and will be replaced with a Multi Site Selection panel.
5. From the list of Site Names on the left, select a site name then clich on the "Add" button. This will add the site name to the Selected Site Name list on the right. For SN09, a maximum of 6 entries can be on the right side. These entries can be the same or different (same site name can be used multiple times). These site names will be used to name the line groups (LGRPs).
6. If a site name was selected in error, from the list on the right, select the site name and the "Rem" button. This will remove the site name from the list on the right.
7. The protocol, version and port have been defaulted, no changes are needed

8. Select OK to start the process. The association process may take up to 15 minutes. This process includes adding a GW to the GWC, adding a LGRP to table LGRPINV in the CM, adding the endpoints to the GWC, then adding the LENs to LNINV in the CM. The LGRP addition process is repeated until all selected LGRPs have been added.

2.8.2.2.6 GUI release history update
Modification to the Associate Gateway GUI

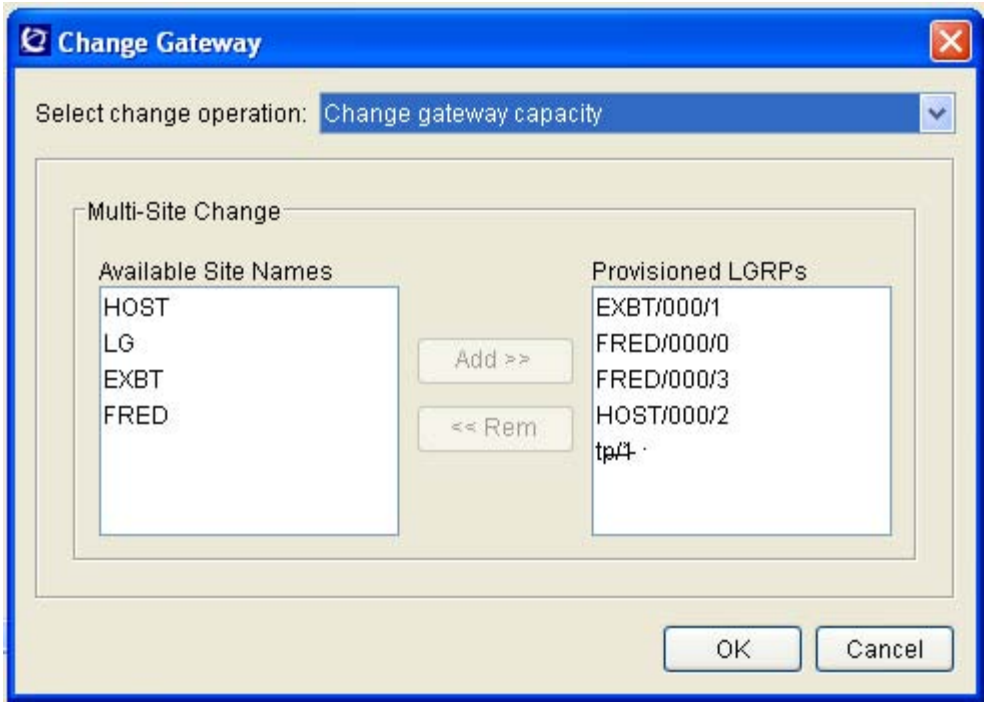
2.8.2.2.7 Context sensitive launching information
Not impacted, no changes

2.8.2.2.8 Supplementary information
None

2.8.2.2.9 CLUI Interface
No impact.

2.8.2.3 GUI name: Change Gateway

2.8.2.3.1 Functional description
This GUI allows the user to change the capacity of a gateway - this capability currently exists. Should the gateway be a MSM, a different Change Gateway GUI is presented.



A gateway using the MSM profile will have the dialog box in figure 2 displayed. Similar to the AssocGW dialog box, this box contains two lists, Available Site Names on the left, which is a list of site names from the table SITE in the CM.

The second list, “Provisioned LGRPs”, is a list of site names already used and assigned. These site names have LGRPs and LENs assigned to it, therefore they show up with there respective frame and group numbers.

From this dialog box, the user can add additional site names (a maximum of 6 LGRP/Site names) are permitted in the Provisioned LGRPs list.

Additionally, the user can select to remove LGRP/Site names from the provisioned list simply by selecting them and the remove button.

Once the site names have been added, and OK selected, this diialog box will close and another panel will appear to display the progress and responses. The first item to display is the timeout value.

Cancel will close the box without executing any operation.

Note: currently only single operations may be performed from thie Change Gateway dialog; in other words, the user cannot add one site and remove another site in the same operation.

2.8.2.3.2 GUI usage and implications

2.8.2.3.3 GUI fields

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Site Names	New	none	Site name values from the CM	Site Names	None
Selected Site Names	New	none	Site names selected from the Site Name list	Selected Site Names	None

2.8.2.3.4 Usage example - Removing an LGRP

Reference the above figure, if the user wishes to remove HOST/000/2 from the currently configured, the following steps are performed:

1. From the Provisioning panel, Gateway Tab, click on the MSM gateway (there should only be one).
2. Select the Change button from the bottom of the Gateway Tab. A Change dialog box opens.
3. From the Change Dialog, the pull down, select Change Gateway Capacity
4. The above dialog box opens.
5. The user selects HOST/000/2 from the Provisioned LGRPs List, then selects the Rem. This will remove the HOST/000/2 from the Provisioned LGRPs List and place in the Available Site Names List.
6. Click on the OK and the operation will begin.
7. A Status box will open and indicate the expected time that the operation may take. This box will also indicate any success or error encountered during this operation.

2.8.2.3.5 Usage example - Adding an LGRP

Reference the above figure, if the user wishes to add another FRED LGRP/site name, the following steps are performed:

1. From the Provisioning panel, Gateway Tab, click on the MSM gateway (there should only be one).
2. Select the Change button from the bottom of the Gateway Tab. A Change dialog box opens.
3. From the Change Dialog, the pull down, select Change Gateway Capacity
4. The above dialog box opens.
5. The user selects FRED from the Available Site Names List, then selects the Add. This will add FRED from the Provisioned LGRPs List.
6. Click on the OK and the operation will begin.
7. A Status box will open and indicate the expected time that the operation may take. This box will also indicate any success or error encountered during this operation.

2.8.2.3.6 Usage example - Cancel

At any time, the user may cancel the pending operation without executing the operation. Simply select Cancel.

2.8.2.3.7 GUI release history update

Not Applicable.

2.8.2.3.8 Context sensitive launching information

Not impacted, no changes.

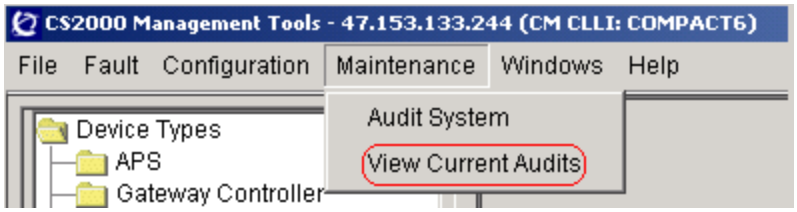
2.8.2.3.9 Supplementary information
Not Applicable.

2.8.2.3.10 CLUI Interface No Impact.

2.8.2.4 GUI name: View Current Audits

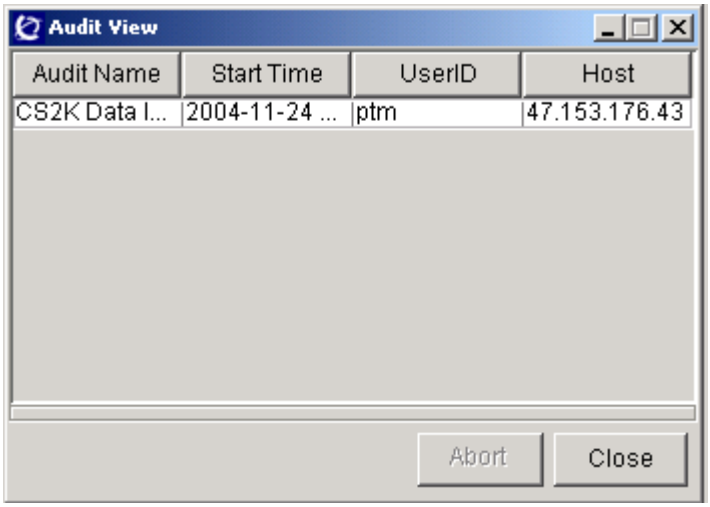
2.8.2.4.1 Functional description

- Add a new menu in Maintenance of Cs2kmt to provide the new function “Abort Audit”.



When user selected the menu “View Current Audits”, another new gui will be displayed. Detail info refer to the following gui.

- Add a new gui to provide the new function “Abort Audit”.



The running audits will be displayed in this gui. The datas of the audits include: Audit Name, Start Time, UserID, Host.

User can selected a running sudit and press the “Abort” button to abort the audit.

2.8.2.4.2 GUI usage and implications
This GUI is used only to view and abort the running audits.

2.8.2.4.3 GUI size
Not applicable

2.8.2.4.4 GUI fields
Not applicable

2.8.2.4.5 Usage example
From the CS2000 Management Tools GUI, select Maintenance from the top menu and select Audit System from the pull down.

2.8.2.4.6 GUI release history update
Add a new gui to view and abort the running audits.

2.8.2.4.7 Context sensitive launching information
Not impacted.

2.8.2.4.8 Supplementary information
None

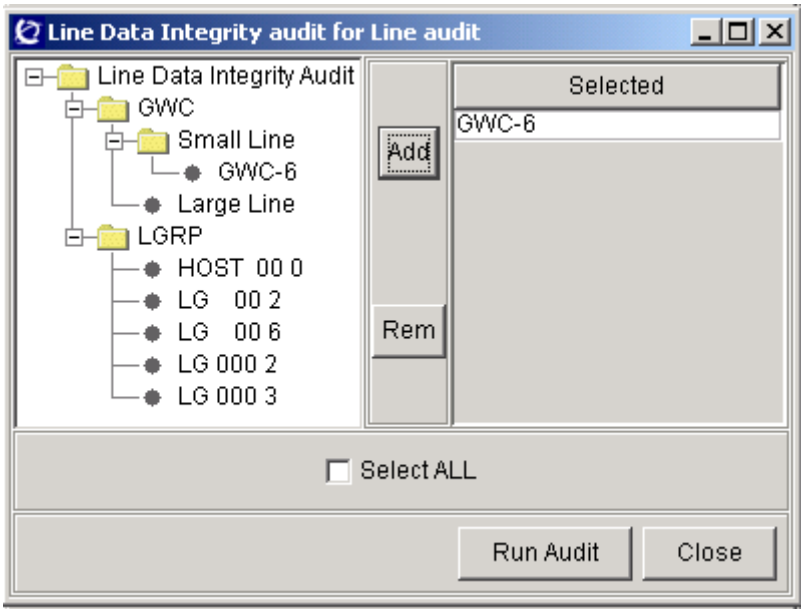
2.8.2.4.9 CLUI Interface Not Impacted

2.8.2.5 GUI name: Line Data Integrity Audit

2.8.2.5.1 Functional description

- Add a new gui to provide support for audit by GWCs, GWs or LGRPs. Only support Line Data Integrity audit now.

When user select “Line Data Integrity Audit” and press the “Run Audit” button in Audit System gui, the following gui will be displayed.



User can selected the GWCs, GWs or LGRPs in the left tree and add them to the right table by press the “->” button.

The button “<-” is used to delete the data that user selected in the right table.

User can select all datas to do audit by select checkbox “Select All”.

After user selected the data and press “Run Audit” button, the audit will be run as before.

2.8.2.5.2 GUI usage and implications

This GUI is used only to provide support for running line audit per GWCs, GWs, or LGRPs.

2.8.2.5.3 GUI size

Not Applicable.

2.8.2.5.4 GUI fields

Not Applicable.

2.8.2.5.5 Usage example

From the CS2000 Management Tools GUI, select Maintenance from the top menu and select Audit System from the pull down.

2.8.2.5.6 GUI release history update
Add a new gui to provide support for running line audit per GWCs, GWs, or LGRPs.

2.8.2.5.7 Context sensitive launching information
Not impacted.

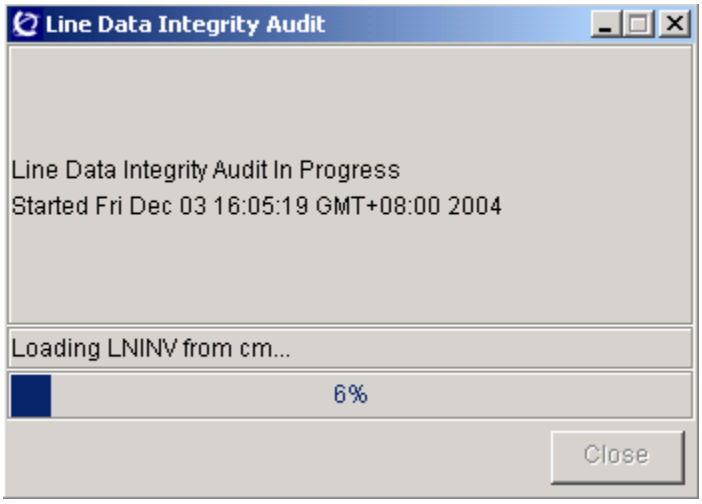
2.8.2.5.8 Supplementary information
None

2.8.2.5.9 CLUI Interface Not Impacted

2.8.2.6 GUI name: Run Audit

2.8.2.6.1 Functional description

2.8.2.6.2 GUI usage and implications
This GUI is used only to provide support for indicating process of running audit.



The progress bar was used to indicate the progress of the running audit.

The label was used to show the current operation.

2.8.2.6.3 GUI size
Not Applicable

2.8.2.6.4 GUI fields
Not Applicable

2.8.2.6.5 Usage example
From the CS2000 Management Tools GUI, select Maintenance from the top menu and select Audit System from the pull down.

2.8.2.6.6 GUI release history update
Add a new gui to provide support for indicating process of running audit.

2.8.2.6.7 Context sensitive launching information
Not impacted.

2.8.2.6.8 Supplementary information
None

2.8.2.7 CLUI Interface
Not Impacted

2.9 User interface changes
Not Applicable

Product = CS 2000 Management Tools

A00008916 -- Gateway Controller Lines Density Increase
Functional Description

1: Applicable Solution(s)
PT-IP, UA-IP, IAC

1.1 Description
With the introduction of the N905 Gateway Controller hardware there is now increased CPU speed and memory capacity. This enables increased port density and combined profiles. The new profiles introduced by this feature are only compatible with N905 GWC hardware and will not operate with MCP750 GWC hardware, therefore both GWC units MUST be loaded with N905 hardware before the GWC profile is migrated to one of the new N905 profiles.

The new profiles are forward compatible with certain existing profiles, allowing for in-service profile migrations. However, the new profiles are not backward compatible with previous profiles. In other words, once a N905 GWC is migrated to a new profile it cannot be migrated back to a previous profile. The only way to migrate backwards from high-density profile is to

delete the GWC provisioning from the SESM database and re-provision the GWC.

1.1.1 Small Gateway Lines High Density Profiles

The High Density small line gateway profiles support 25,600 lines and small gateways without IPSEC turned on. If IPSEC is to be supported then the engineering limit is 12,800 gateways and lines. This is an engineering rule and is not enforced by the software, the software will allow up to 25,600 lines and gateways to be provisioned regardless of IPSEC. As noted above, once a GWC has been migrated to the high density profile it cannot be downward migrated to the previous profile without deleting the provisioning and re-provisioning with desired profile.

PROFILE NAME: SMALL_LINENA_V2

This profile is a high density version of the SMALL_LINENA profile. It enhances SMALL_LINENA by increasing line and gateway capacity from 6,400 to 25,600. This profile is compatible with SMALL_LINENA as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	NORTHAA
KEYSET	KSETEX	

CAPABILITY	CAPACITY
Lines	25,600
Small Gateways	25,600
IPSEC	
Kerberos	
DQOS	80

PROFILE NAME: **SMALL_LINEINTL_V2**

This profile is a high density version of the SMALL_LINEINTL profile. It enhances SMALL_LINEINTL by increasing line capacity from 6,400 to 12,800 lines and gateways. This profile is compatible with SMALL_LINEINTL as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	UKADSI
KEYSET	KSETEX	

CAPABILITY	CAPACITY
Lines	25,600
Small Gateways	25,600
IPSEC	
Kerberos	
DQOS	80

1.1.2 Large Gateway Lines High Density Profiles

The High Density large line gateway profiles support 12,800 lines and small gateways with or without IPSEC. This profile also supports SIP Lines [DPL] (see feature A00008522 for details). As noted above, once a GWC has been migrated to the high density profile it cannot be downward migrated to the previous profile without deleting the provisioning and re-provisioning with desired profile.

PROFILE NAME: **LARGE_LINENA_V2**

This profile is a high density version of the LARGE_LINENA profile. It enhances LARGE_LINENA by increasing line capacity from 6,400 to 12,800 lines. This profile is compatible with LARGE_LINENA as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	NORTHAA
KEYSET	KSETEX	
DPL_TERM	DPLEX	

CAPABILITY	CAPACITY
Lines	12,800
Large Gateways	27
IPSEC	
DPL	

PROFILE NAME: **LARGE_LINEINTL_V2**

This profile is a high density version of the LARGE_LINEINTL profile. It enhances LARGE_LINEINTL by increasing line capacity from 6,400 to 12,800 large lines. This profile is compatible with LARGE_LINEINTL as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	UKADSI
KEYSET	KSETEX	

CAPABILITY	CAPACITY
Lines	12,800
Large Gateways	27
IPSEC	
DPL	

1.1.3 Combined Lines, Trunks, and Audio Profiles

These profiles combine the SMALL_LINE, LARGE_LINE, TRUNK, and AUDCNTL profiles into one combined profile at MCP750 capacities. This profile also supports SIP Lines [DPL] (see feature A00008522 for details). All gateway types and capabilities that are supported on the individual profiles are supported in this combined profile with the following exceptions:

- 250 PTS and PRI trunk types are not supported on the combined profile (250 ISUP trunks are supported). 250 PTS and PRI trunks must be removed before migrating to the combined profile.

As noted above, once a GWC has been migrated to this profile it cannot be downward migrated to the previous profile without deleting the provisioning and re-provisioning with desired profile.

PROFILE NAME: **LINE_TRUNK_AUD_NA**

This profile is a combination of the SMALL_LINENA, LARGE_LINENA and TRUNK_NA profiles. This profile is compatible with SMALL_LINENA, LARGE_LINENA, and TRUNK_NA as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	NORTHAA
KEYSET	KSETEX	
PRAB	DTCEX	
ABTRK	GWCEX	
DPL_TERM	DPLEX	

CAPABILITY	CAPACITY
Lines	6400
Trunks	4094
Audio	4096
DQOS	20
Small Gateways	6400
Large Gateways	51
Audio Gateways	16
BCT	
IPSEC	
KERBEROS	
Conferences	
Announcements	
DPL	

PROFILE NAME: **LINE_TRUNK_AUD_INTL**

This profile is a combination of the SMALL_LINEINTL, LARGE_LINEINTL and TRUNK_INTL profiles. This profile is compatible with SMALL_LINEINTL, LARGE_LINEINTL, and TRUNK_INTL as part of an in-service upgrade.

TERM TYPE	EXEC DATA	TONEDATA
POTS	POTSEX	UKADSI
KEYSET	KSETEX	

CAPABILITY	CAPACITY
Lines	6400
Trunks	4094

PRAB	DTCEX	
ABTRK	GWCEX	
DPL_TERM	DPLEX	

Audio	4096
DQOS	20
Small Gateways	6400
Large Gateways	51
Audio Gateways	16
BCT	
IPSEC	
KERBEROS	
Conferences	
Announcements	
DPL	

1.1.4 Profile Compatibility

The following table lists which new profiles are compatible with existing profiles. As noted above, once a GWC has been migrated to a N905 supported profile it cannot be downward migrated without deleting the provisioning and re-provisioning with desired profile.

Figure 1 Profile Compatibility Table

Existing Profile (SN08)	Compatible In-Service Upgrade To (SN09 Profile)
SMALL_LINENA	SMALL_LINENA_V2, LINE_TRUNK_AUD_NA
SMALL_LINEINTL	SMALL_LINEINTL_V2, LINE_TRUNK_AUD_INTL
LARGE_LINENA	LARGE_LINENA_V2, LINE_TRUNK_NA
LARGE_LINEINTL	LARGE_LINEINTL_V2, LINE_TRUNK_INTL
TRUNK_NA	LINE_TRUNK_AUD_NA
TRUNK_INTL	LINE_TRUNK_AUD_INTL
SIP_LINES_NA	LARGE_LINENA_V2, LINE_TRUNK_NA
SIP_LINES_INTL	LARGE_LINEINTL_V2, LINE_TRUNK_INTL

1.1.5 GWC Profile Migration Instructions

Once both GWC units have been upgrade to N905 hardware, the GWC profile can be migrated to one of the new N905 profiles using the SESM GUI. Following a successful GWC Profile change, both units of the Gateway Controller must be reloaded before the change takes affect, the GWC units are still running on previous profile until a lock/unlock is performed. An alarm is raised for each unit to indicate a data mismatch exists between the SESM server and the Gateway Controller. The alarm condition is displayed by the **Alarm Manager** accessed via the **Fault** menu. The alarm will be cleared once the GWC units have been reloaded.

1. Verify that both GWC units are N905 hardware.
2. Change Profile from SESM GUI (alarm will be generated).
3. (SESM GUI) **Busy** the inactive unit.
4. (SAM21 GUI) **Lock** and **Unlock** the associated card. The card is booted and provisioned data is downloaded following the unlock operation. The data mismatch alarm condition is cleared for this unit.
5. (SESM GUI) **RTS** the inactive unit.
6. (SESM GUI) **Warm Swact** the Gateway Controller.
7. Repeat steps 3 through 6 for the mate unit.

1.2 Hardware Requirements or Dependencies

This feature is dependent on the N905 GWC hardware.

1.3 Software Requirements or Dependencies

SN09 SESM, SAM-21 and GWC loads.

1.4 Limitations and restrictions

The new profiles are only supported on the N905 hardware. An MCP750 GWC will not come into service if it is provisioned with one of the new profiles. If the GWC card is pre-provisioned with a N905 profile and then loaded with MCP750 hardware and booted, an alarm will generated. This is an unsupported configuration, both GWC units must be loaded with N905 hardware.

If an MCP750 profile is already in service (not a pre-provisioning case) the software will verify that N905 hardware exists before allowing the GWC profile change.

The new profiles are not backward compatible with any other profile. Therefore, the new N905 profile must be chosen carefully. Once the N905 GWC is in service on the new profile it cannot be changed without deleting provisioning on the GWC.

250 PTS and PRI trunk types are not supported on the combined profile (250 ISUP trunks are supported). 250 PTS and PRI trunks must be removed before migrating to the combined profile.

The N905 Small Gateway Lines profiles support 25,600 lines WITHOUT IPSEC. With IPSEC turned on 12,800 is the engineered limit. The limit is not enforced in provisioning however.

1.5 Interactions

1.6 Applicable customer facing sections

Fault Management:

- Logs _____
- Alarms _____

Configuration:

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

Glossary

Term	Description
New term	definition

Product = CS 2000 Management Tools

A00009189 -- USP - SESM Support for 64 Character FQDN. Related feature: A00008043 CS2K Support for 64 Character FQDN

Functional Description

1: Applicable Solution(s)

IAW, IAC

1.1 Description

This feature makes enhancements on SESM & CS2K to make the whole system fully support Gateway FQDN up to 64 characters.

In SN07/SN08, FQDN support was introduced into CS2K system. But the solution had a number of limitations. The size of the gateway FQDN and domain name were restricted. Only a single domain name was supported per GWC, and only the hostnames were used in the CS2K-MT GUI, OSSGATE, TMM, and LMM.

This SN09 feature is intended to remove those limitations while still maintaining backwards compatibility:

- Multiple gateway domain names are supported per GWC as part of the Gateway Name field as long as default gateway domain name is not provisioned on the GWC. In this case, the Gateway Name represents a gateway FQDN and can be up to 64 characters.
- Only one default gateway domain name (up to 62 characters) can be provisioned per GWC. If provisioned, then the Gateway Name represents the gateway hostname. The FQDN is the concatenation of the Gateway Name and the default domain name, which together can contain up to 64 characters.
- The customer can use the Gateway Name as a hostname or a FQDN in all user interfaces, includes CS2K-MT GUI, OSSGate, TMM and LMM.
- Use of a gateway name containing the default domain name assigned to a GWC is not allowed in any OSSGate SERVORD+ commands. Use of such a name will result in a command failure (eg. “Gateway not found”).
- This feature allows Small Lines, TGCP trunks and third party Large Lines gateway to use a free-format, up to 64 characters gateway FQDN.
- Only cable solution gateways support usage of default gateway domain name.

Table 1 Gateway profiles which support default gateway domain name

Gateway Profile Name	Gateway Profile Name	Gateway Profile Name
MOTOROLAMTA_1	ARRIS_TOUCHTONE_NN01_4	TOUCHTONE_NN01_2
MOTOROLAMTA_2	ARRIS_TOUCHTONE_NN02_4	TOUCHTONE_NN01_3
MOTOROLAMTA_4	TOUCHTONE_NN01_1	TOUCHTONE_NN01_4

1.2 CS2K-MT GUI functionality modifications

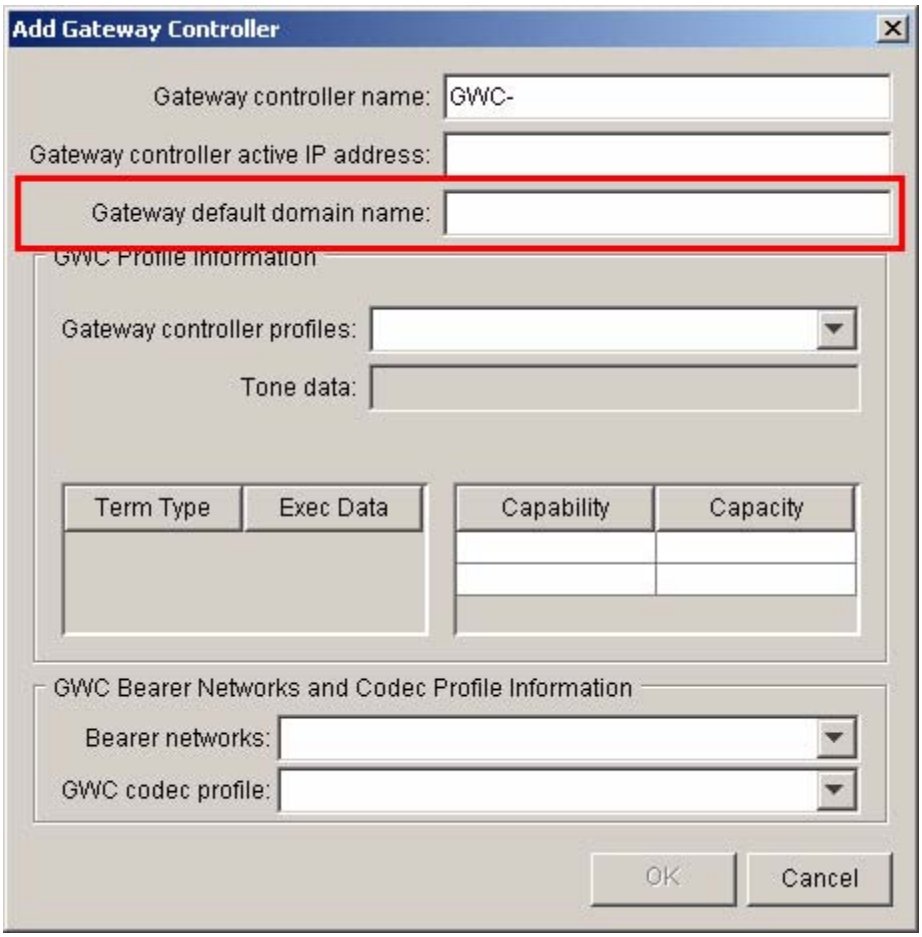
1.2.1 Add GWC node dialog

When adding GWC node, customer could set default gateway domain name. This name only can be used for cable solution gateways (refer to Table 1 o n the preceding page).

If default gateway domain name is provisioned, only cable solution gateways can be associated on this GWC node. Any other gateway association will be rejected. Then the default gateway domain name will be applied to all associated cable solution gateways.

This field can be left empty if user don't want to set default gateway domain name. In this case, not only cable solution gateways, but also other solution gateways can be associated.

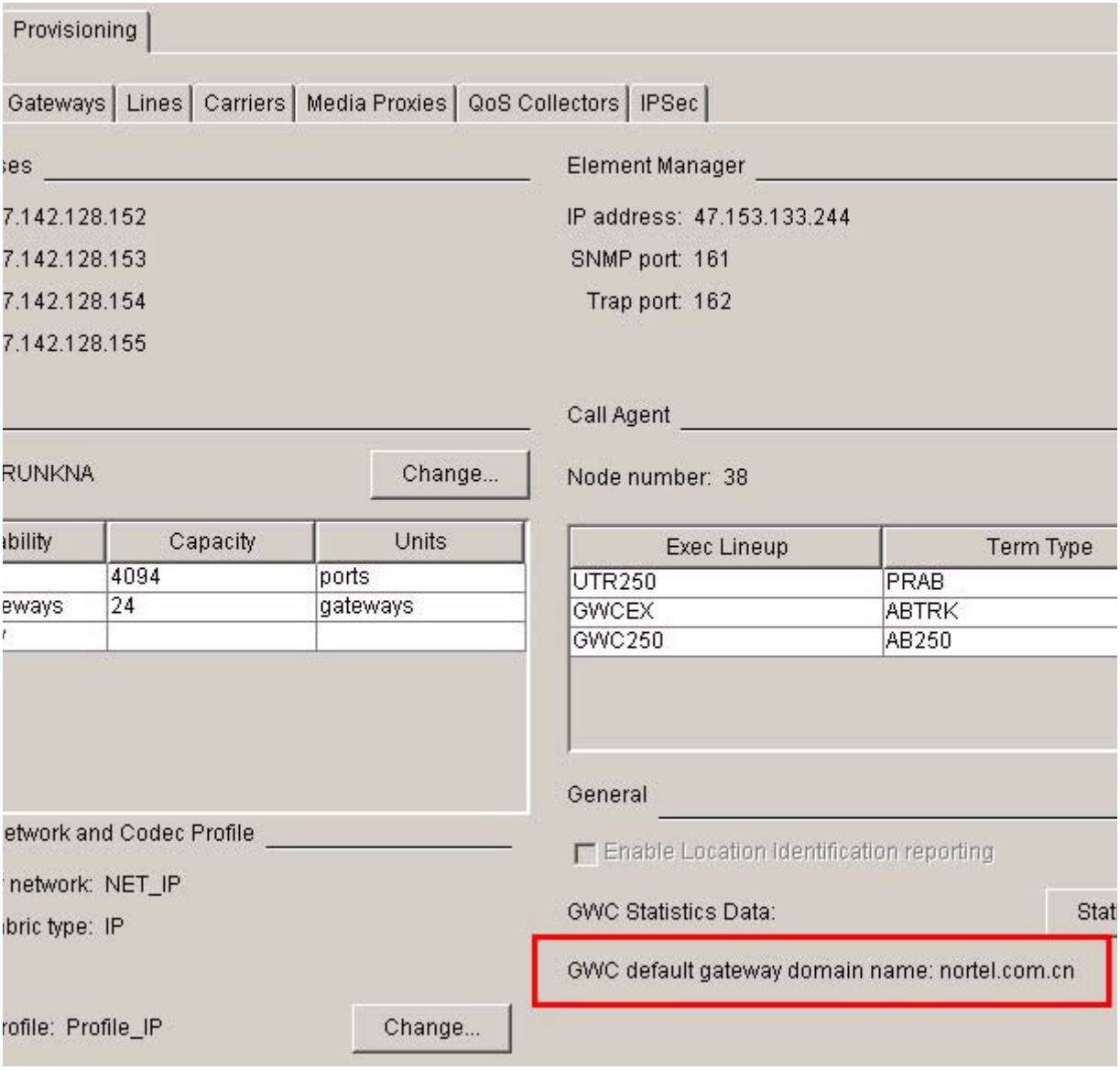
Figure 1 Add GWC node dialog



1.2.2 GWC provisioning display panel

If a default gateway domain name was provisioned when adding GWC node, the domain name will be displayed on GWC provisioning display panel. If not provisioned, "<Not Configured>" will be displayed.

Figure 2 GWC provisioning display panel



1.2.3 Associate Media Gateway dialog

GUI layout of Associate Media Gateway dialog is not changed. But the usage of “Gateway Name” field is different than before.

1.2.3.1 Has default gateway domain name provisioned

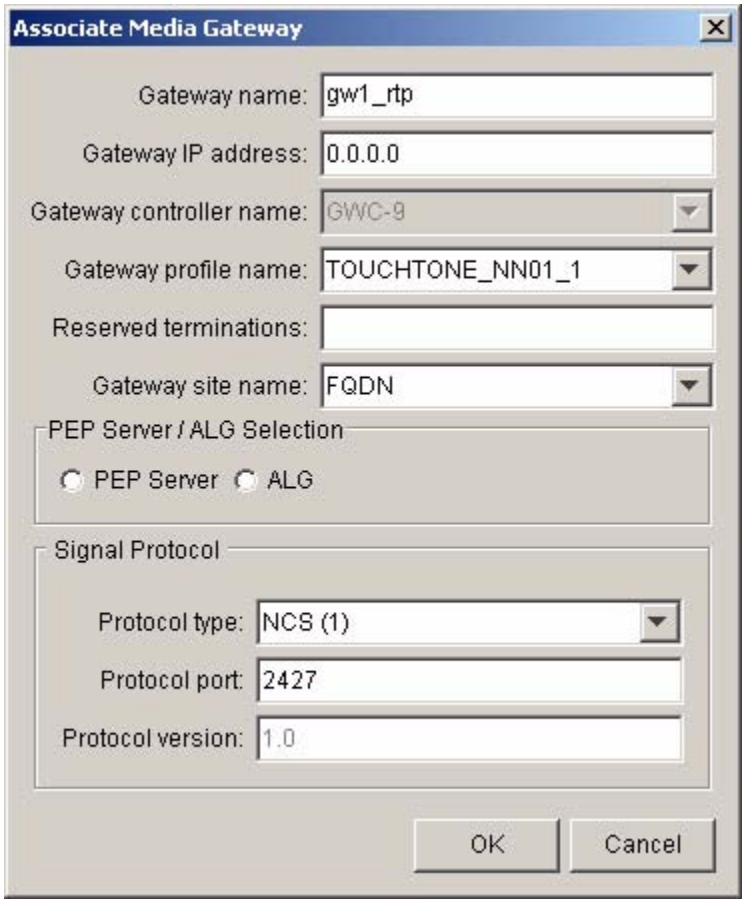
Since SN09, if a default gateway domain name is provisioned on the GWC, only cable solution gateways can be associated on this GWC (refer to Table 1 on page 1935). Then the Gateway Name represents the gateway hostname. The FQDN is the concatenation of the Gateway Name and the default domain name, which together can contain up to 64 characters.

For example:

If the default domain name is “**nortel.com**”, And the user needs to provision a gateway with FQDN “**gw1_rtp.nortel.com**”, then input the Gateway Name field as the hostname “**gw1_rtp**”.

In this case, if the gateway is a PacketCable gateway, the Gateway Name "**gw1_rtp**" is downloaded to table LNENDPT on the Core, and it is also used for QoS record.

Figure 3 Associate Media Gateway Dialog



1.2.3.2 No default gateway domain name provisioned

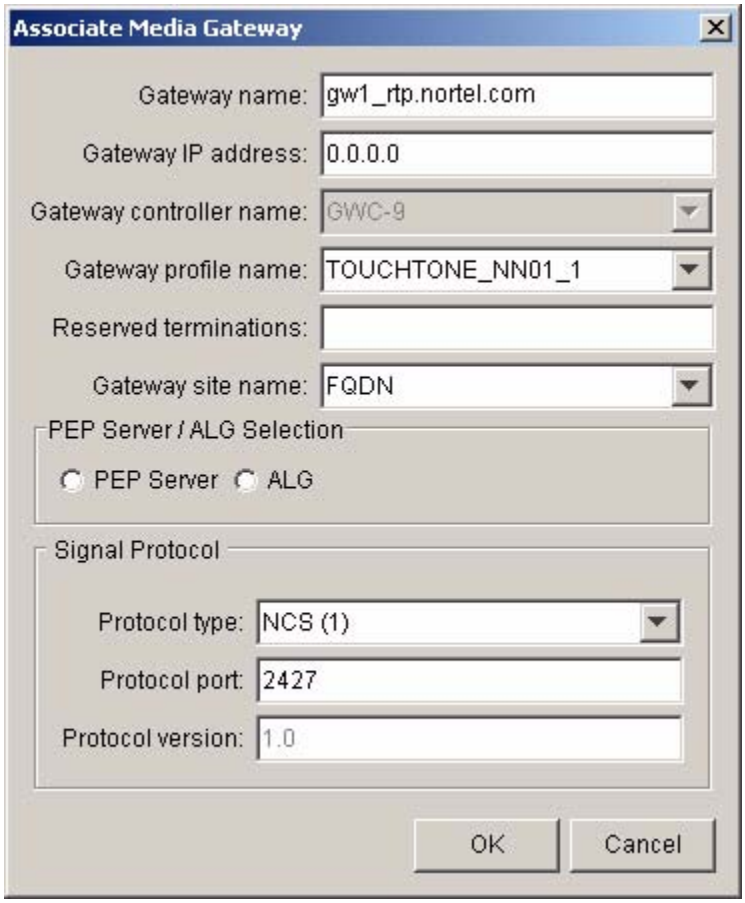
Since SN09, if default gateway domain name is not provisioned, then the Gateway Name represents the gateway FQDN, which can be free-format, up to 64 characters.

For example:

If the default domain name is not set and the user needs to provision a gateway with FQDN "**gw1_rtp.nortel.com**", then input the Gateway Name field as the FQDN "**gw1_rtp.nortel.com**".

In this case, if the gateway is a PacketCable gateway, the Gateway Name "**gw1_rtp.nortel.com**" is downloaded to table LNENDPT on the Core, and it is also used for QoS record.

Figure 4 Associate Media Gateway Dialog



1.2.4 Gateways display panel

On gateways display panel, gateway domain name or part of gateway FQDN can be used as retrieval criteria when querying gateway information. And gateway domain name will be displayed in separate column if provisioned.

1.2.4.1 Use default domain name

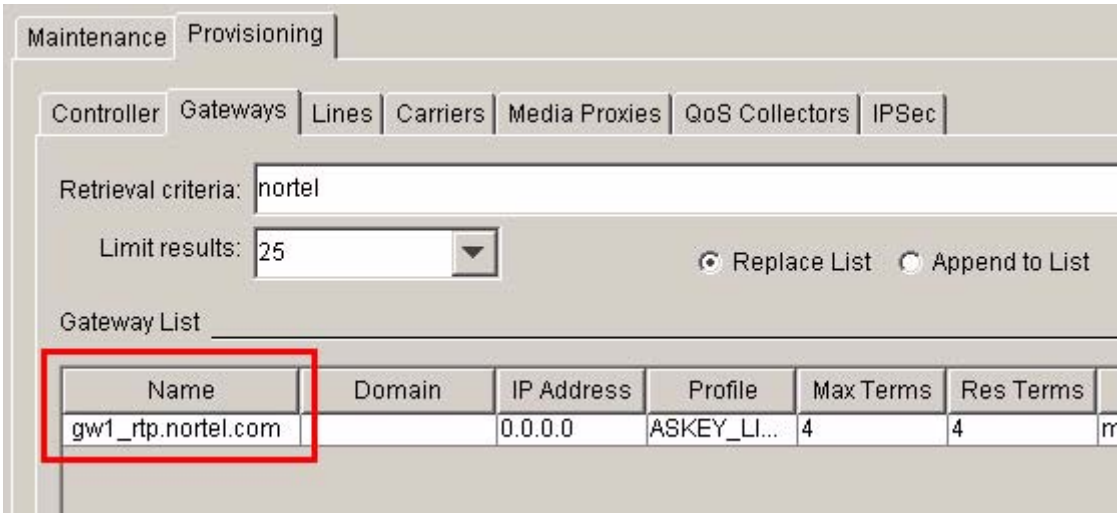
For those gateways using default gateway domain name, the gateway information will be displayed as following figure.

Figure 5 Gateways display panel - Case 1

1.2.4.2 No default domain name

For those gateways do not use default gateway domain name, the gateway information will be displayed as following figure.

Figure 6 Gateway display panel - Case 2



1.2.5 Lines display panel

On lines display panel, gateway domain name or part of gateway FQDN can be used as retrieval criteria when querying line information. And gateway domain name will be displayed in separate column if provisioned.

Figure 7 Lines display panel

1.2.6 CS2K Audit

In all CS2K audit components (CS2K Data Integrity Audit, Line Audit and Trunk Audit), gateway FQDN can be recognized when running audit process.

If gateway domain name was provisioned, gateway FQDN will be displayed in audit report and possible correct action.

Figure 8 CS2K Data Integrity Audit report window

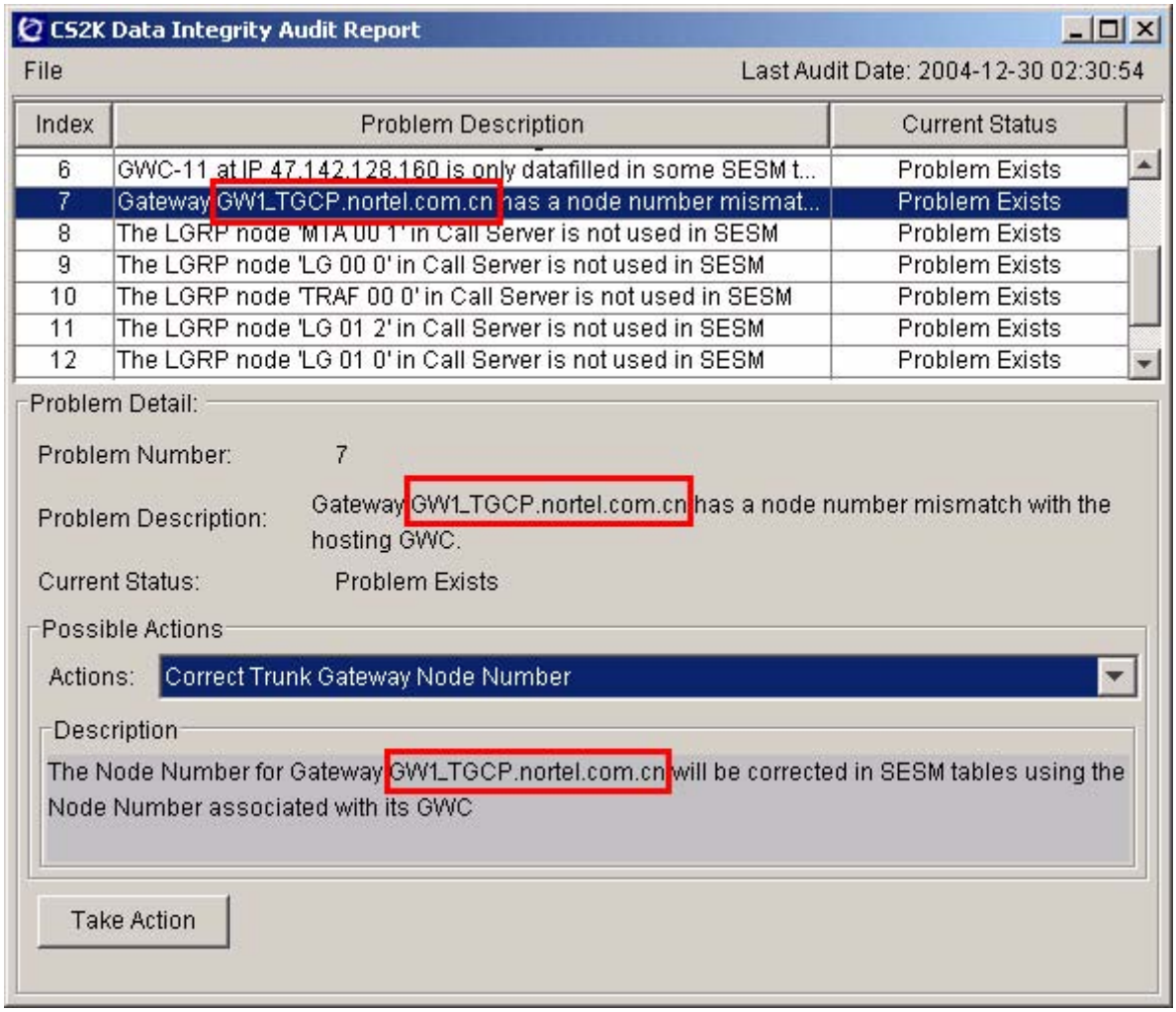


Figure 9 Line Data Integrity Audit report window

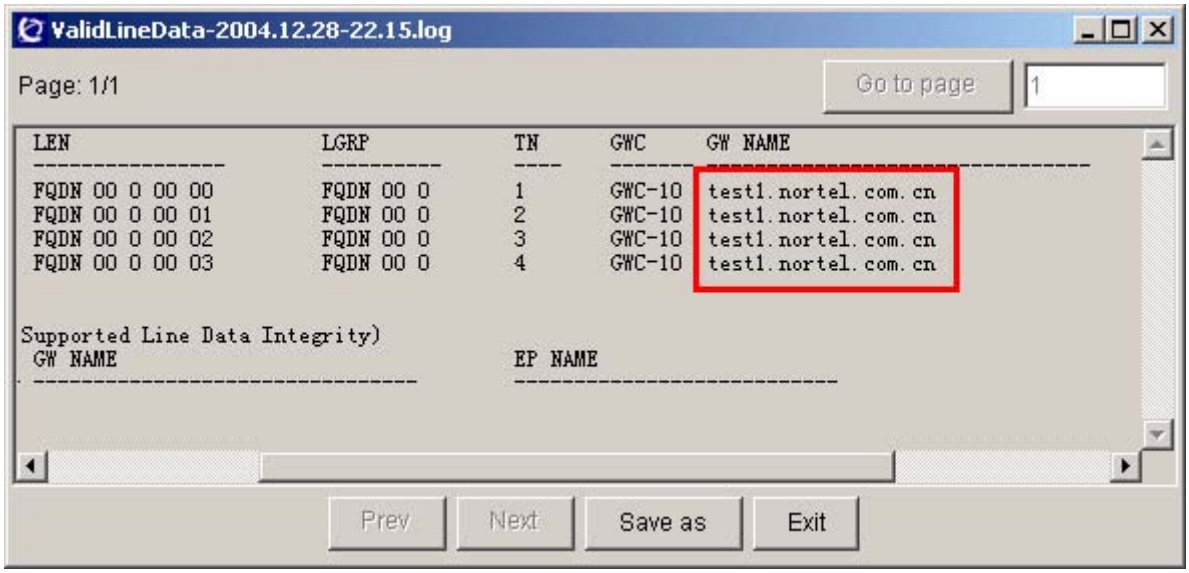
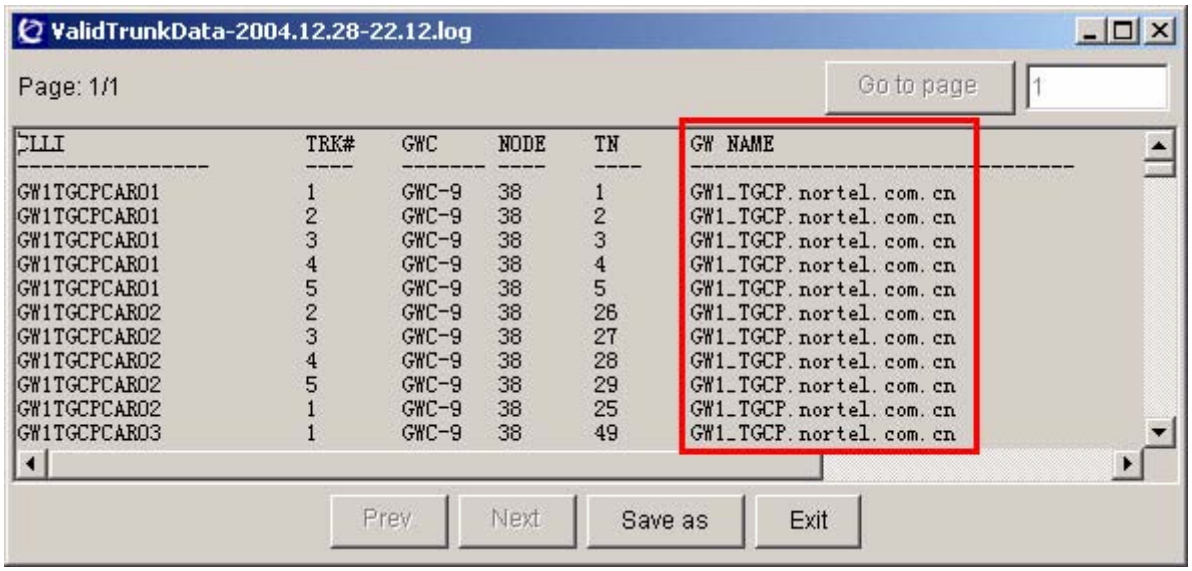


Figure 10 Trunk Data Integrity Audit report window



1.3 OSSGate functionality modifications

1.3.1 Nodes Provisioning interface

There are some changes on OSSGate Nodes Provisioning interface:

1.3.1.1 Add GWC node

A new parameter, gwDefaultDomainName, is added in the AddGWC xml command which is allowed user to input the gateway domain name if needed.

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addGWCtoCS usn="1" version="1.0">
        <Parameters>
          <csUIName>COMPACT6</csUIName>
          <gwcUIName>GWC-10</gwcUIName>
          <profileName>LARGE_LINENA</profileName>
          <gwcActvIp>47.128.142.156</gwcActvIp>
          <gwcSnmpPort>161</gwcSnmpPort>
          <bearerNetworkName>NET_IP</bearerNetworkName>
          <bearerFabricType>IP</bearerFabricType>
          <codecProfileName>Profile_IP</codecProfileName>
          <termType>POTS</termType>
          <termType>KEYSET</termType>
          <execLineup>POTSEX</execLineup>
          <execLineup>KSETEX</execLineup>
          <gwDefaultDomainName>nortel.com.cn</gwDefaultDomainName>
        </Parameters>
      </addGWCtoCS>
    </Methods>
  </Command>
</CommandList>
```

1.3.1.2 Query GWC

The Query GWC OSSGate xml command doesn't need to be changed, but the response will be changed to include the gateway domain name, if the queried GWC has no domain name, this field will be null.

The QueryGWC response will be like following:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Response>
  <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <queryGWC usn="1" version="1.0">
      <ReturnData>
```

```
            <Row>
              <gwcUIList>GWC-10</gwcUIList>
              <gwcIpList>47.142.128.156</gwcIpList>
              <callServerId>COMPACT6</callServerId>
              <nodeName>GWC 10</nodeName>
              <typeList>1</typeList>
              <typeList>6</typeList>
              <typeList>7</typeList>
              <typeList>15</typeList>
              <typeList>16</typeList>
              <xacNodeNumber>27</xacNodeNumber>
              <actvIpAddress>47.142.128.156</actvIpAddress>
              <snmpPort>161</snmpPort>
              <mktTones>NORTHAA</mktTones>
              <termTypes>POTS</termTypes>
              <termTypes>KEYSET</termTypes>
              <pmExecs>POTSEX</pmExecs>
              <pmExecs>KSETEX</pmExecs>
              <capacity>6400</capacity>
              <externalIP>NOT_YET_SUPPORTED</externalIP>
              <externalPort>0</externalPort>
              <bearerNetworkName>NET_IP</bearerNetworkName>
              <bearerFabricType>IP</bearerFabricType>
              <codecProfileName>Profile_IP</codecProfileName>
              <gwDefaultDomainName>nortel.com.cn</gwDefaultDomainName>
            </Row>
            <RC>0</RC>
            <MsgTxt>Query of a Single GWC was successful</MsgTxt>
          </ReturnData>
          </queryGWC>
        </Methods>
      </Response>
    </CommandList>
```

1.3.1.3 Query Media Gateway

Although the gateway might be associated with a default domain name, but in the OSSGate QueryMG response, only the gateway host name will be returned.

So no changes was made on QueryMG operation.

1.3.2 Other OSSGate interfaces

For all of other OSSGate interfaces, format of request/response messages are not modified. The only changes are:

- If gateway name is required in the request message, both of gateway name and gateway FQDN can be used.
- If gateway name is filled in request message, the same gateway name will be returned in the response message, no matter if default gateway domain name is provisioned.
- If gateway FQDN is filled in request message, the same gateway FQDN will be returned in the response message (excepts Query Media Gateway interface).

This applies to following OSSGate interfaces:

1.3.2.1 Nodes Provisioning

- disAssocGWC
- disAssocMG
- changeMG
- deleteGWCfromCS

1.3.2.2 Trunk Provisioning

- AddTuple
- DelTuple
- ReplaceTuple
- GetRange
- GetTuple

1.3.2.3 Carrier Provisioning

- AddCarrier
- DeleteCarrier
- GetCarrier
- GetEndpoint
- ListAllCarriers

1.3.2.4 Trunk Maintenance

- PostByGatewayName
- QESByGatewayName
- BSYByGatewayName
- RTSByGatewayName
- INBByGatewayName

- FRLSByGatewayName
- PostByCarrier
- QESByCarrier
- BSYByCarrier
- RTSByCarrier
- INBByCarrier
- FRLSByCarrier
- PostByTrunkClli
- BSYByTrunkClli
- RTSByTrunkClli
- INBByTrunkClli
- FRLSByTrunkClli
- PostGroupDChannelByTrunkClli
- GetTrunkCllisByGatewayName
- GetGatewayNames
- GetCarriers

1.3.2.5 Line Provisioning

All SERVORD+ commands which support GW/endpoint names will NOT support the use of a gateway name which contains the default domain name assigned to the gateway's hosting GWC. If the gateway is provisioned on a GWC which has a default gateway domain name assigned, only the gateway hostname (specified at gateway creation time) may be used in the SERVORD+ command. Examples of commands for such a gateway are as follows:

Gateway "testgwname" is provisioned on a GWC which has a default gateway domain name of "us.nortel.com" assigned.

Supported Hostname only:
EST $ DLH 5200999 1FR Lata1 0 ***testgwname*** aaln/1 ***testgwname.1*** aaln/1 $ DGT $ 3

QTP ***testgwname*** aaln/1

Unsupported FQDN:
EST $ DLH 5200999 1FR Lata1 0 ***testgwname.us.nortel.com*** aaln/1 ***testgwname.1.us.nortel.com*** aaln/1 $ DGT $ 3

QTP ***testgwname.us.nortel.com*** aaln/1

Query output will always provide FQDN information if available in the GWCEM if the gateway is initially provisioned with a FQDN (ie. does not use the a GWC's default gateway domain name). If the gateway is provisioned on a GWC which has a default gateway domain name assigned, then only the hostname entered at gateway provisioning time will be returned in the query output.

1.3.2.5.1 Limitations

Gateways which are provisioned with domain information imbedded within the user provided hostname and assigned to GWCs without a default gateway domain name, will always return the user-assigned, domain-imbedded name in queries and will always require the user-assigned, domain-imbedded name in non-query commands (eg. NEW, OUT, etc..).

Example 1:

A user associates gateway ***"testgwname.us.nortel.com"*** to GWC-0. GWC-0 is *not configured* with a default gateway domain name. When the gateway is provisioned in this manner, all SERVORD+ queries (QLEN/QDN/QTP/etc) will return ***"testgwname.us.nortel.com"*** in ouput and all SERVORD+ non-query commands (NEW/EST/OUT/etc) will require ***"testgwname.us.nortel.com"*** in the relevant command string.

Query command and output format:

```
> QTP testgwname.us.nortel.com aaln/4
------------------------------------------------------------------
---
LEN:     UAIP  00 0 00 03
END POINT: testgwname.us.nortel.com  aaln/4
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:     6210003
LINE CLASS CODE:      1FR
IBN TYPE: STATION
CUSTGRP:           RES1     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     77
LINE ATTRIBUTE INDEX:     77
XLAPLAN KEY :   613_PKDK_1             RATEAREA KEY :  L619_LATA1_20
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    127
PM TERMINAL NUMBER :    4
OPTIONS:
DGT PIC 250CAR Y
RES OPTIONS:
CXR CTALL N STD
OFFICE OPTIONS:
```

```
SRA
------------------------------------------------------------------------
---
>
```

NON-Query Formats allowed:

```
EST $ DLH 5200999 1FR Lata1 0 testgwname.us.nortel.com aaln/1
testgwname.us.nortel.com aaln/2 $ DGT $ 3
```

Gateways which are provisioned without domain information imbedded within the user provided hostname and assigned to GWCs which specify a default gateway domain name, will always return the user-assigned host name in queries and will always require the user-assigned host name in non-query commands (eg. NEW, OUT, etc..).

Example 2:
A user associates gateway ***"testgwname.1"*** to GWC-0. GWC-0 is *configured* with a default gateway domain name ***"ibm.com"***. When the gateway is provisioned in this manner, all SERVORD+ queries (QLEN/QDN/QTP/etc) will return ***"testgwname"*** in output. Non-query SERVORD+ commands (NEW/EST/OUT/etc) will allow only ***"testgwname.1"*** in the relevant command string.

Query command and output format:

```
> QTP testgwname.1 aaln/4
yields
------------------------------------------------------------------------
---
LEN:     UAIP  00 0 00 03
END POINT: testgwname  aaln/4
TYPE: SINGLE PARTY LINE
SNPA: 613
DIRECTORY NUMBER:     6210003
LINE CLASS CODE:      1FR
IBN TYPE: STATION
CUSTGRP:           RES1     SUBGRP: 0  NCOS: 0
SIGNALLING TYPE:  DIGITONE
LINE TREATMENT GROUP:     77
LINE ATTRIBUTE INDEX:     77
XLAPLAN KEY :   613_PKDK_1             RATEAREA KEY :  L619_LATA1_20
CARDCODE:  RDTLSG    GND: N  PADGRP: PKNIL  BNV: NL MNO: N
PM NODE NUMBER     :    127
PM TERMINAL NUMBER :    4
OPTIONS:
DGT PIC 250CAR Y
```

```
RES OPTIONS:
CXR CTALL N STD
OFFICE OPTIONS:
SRA
------------------------------------------------------------------------
---
>
```

NON-Query Formats allowed:

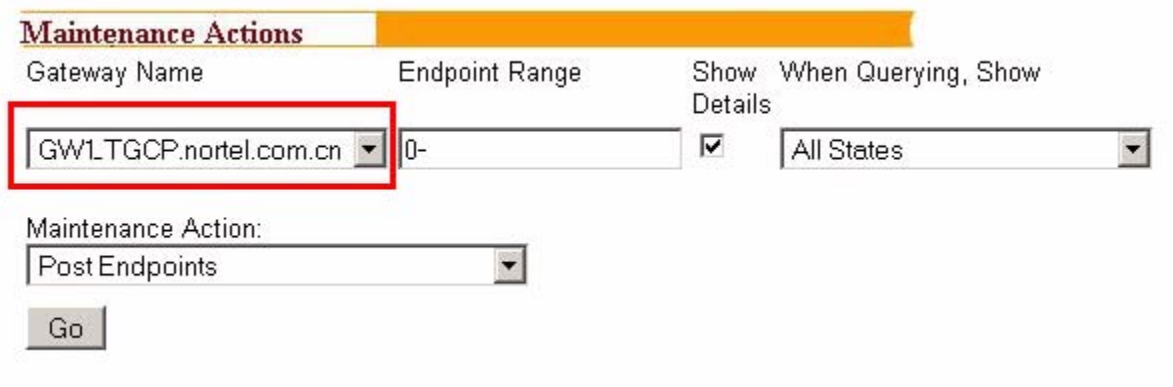
```
EST $ DLH 5200999 1FR Lata1 0 testgwname.1 aaln/1 testgwname.1 aaln/2
$ DGT $ 3
```

1.4 TMM functionality modifications

1.4.1 Maintenance By Gateway Name

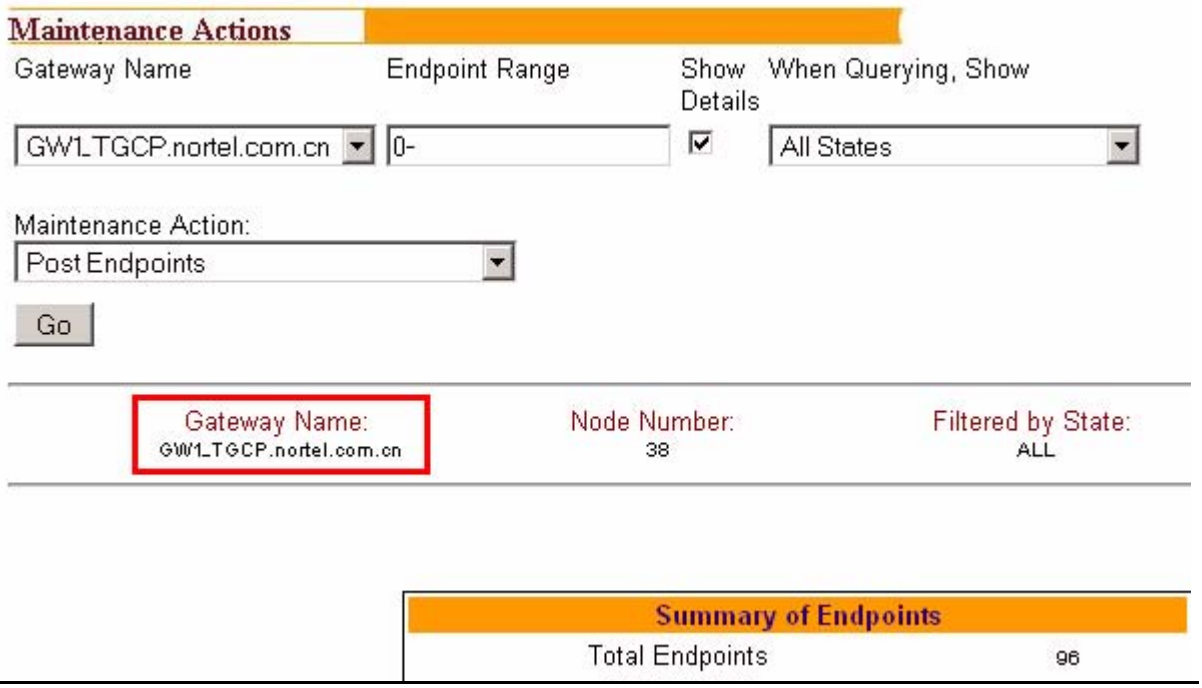
In SN09, gateway FQDN up to 64 characters will be automatically retrieved and displayed on TMM GUI.

Figure 11 FQDN gateway name retrieval - MtcByGatewayName



If user performs maintenance actions such as Post and Busy, Gateway FQDN will be displayed on state output.

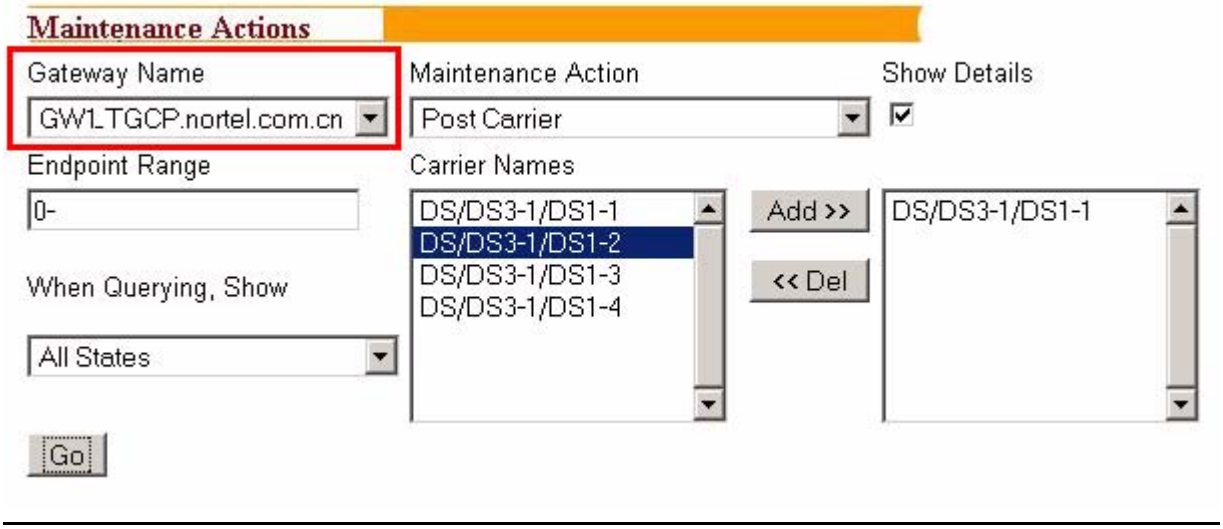
Figure 12 Mtc by Gateway Name state output



1.4.2 Maintenance By Carrier

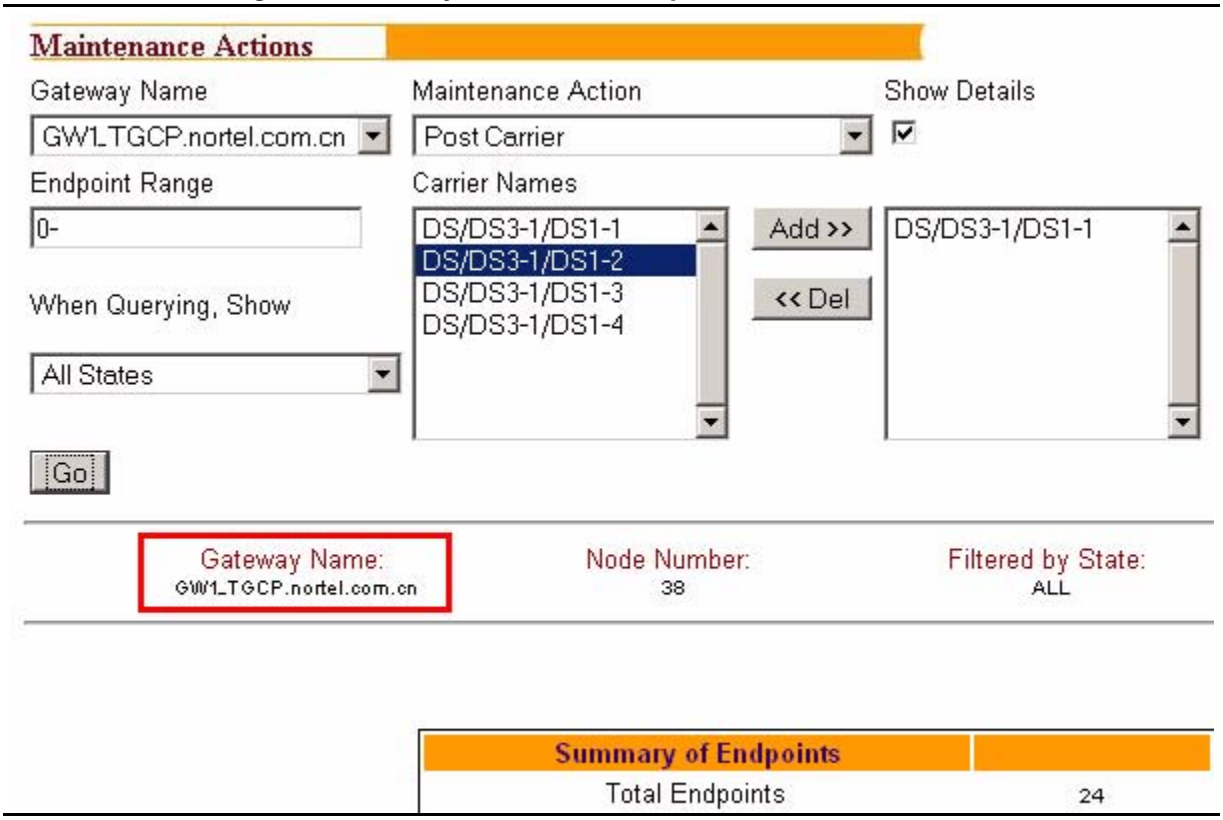
In SN09, gateway FQDN up to 64 characters will be automatically retrieved and displayed on TMM GUI.

Figure 13 FQDN gateway name retrieval - MtcByCarrier



If user performs maintenance actions such as Post and Busy, Gateway FQDN will be displayed on state output.

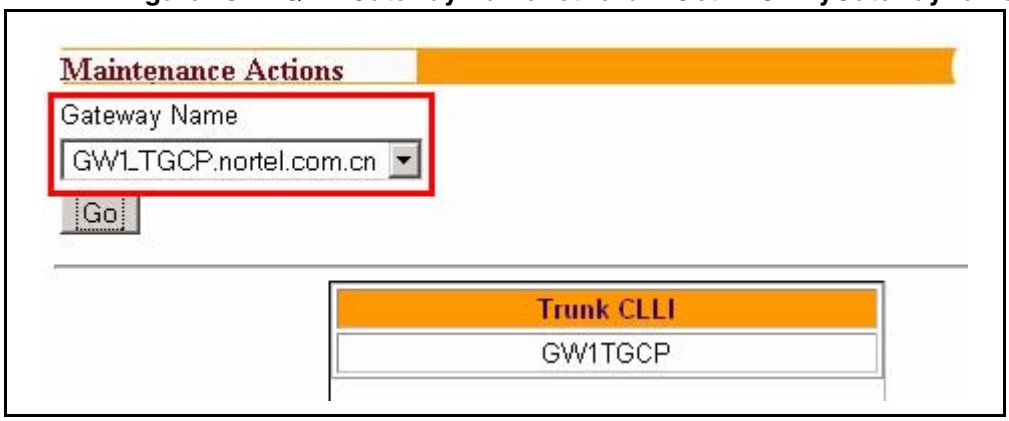
Figure 14 Mtc by Carrier state output



1.4.3 Get TrkCLLIs by Gateway Name

In SN09, gateway FQDN up to 64 characters will be automatically retrieved and displayed on TMM GUI.

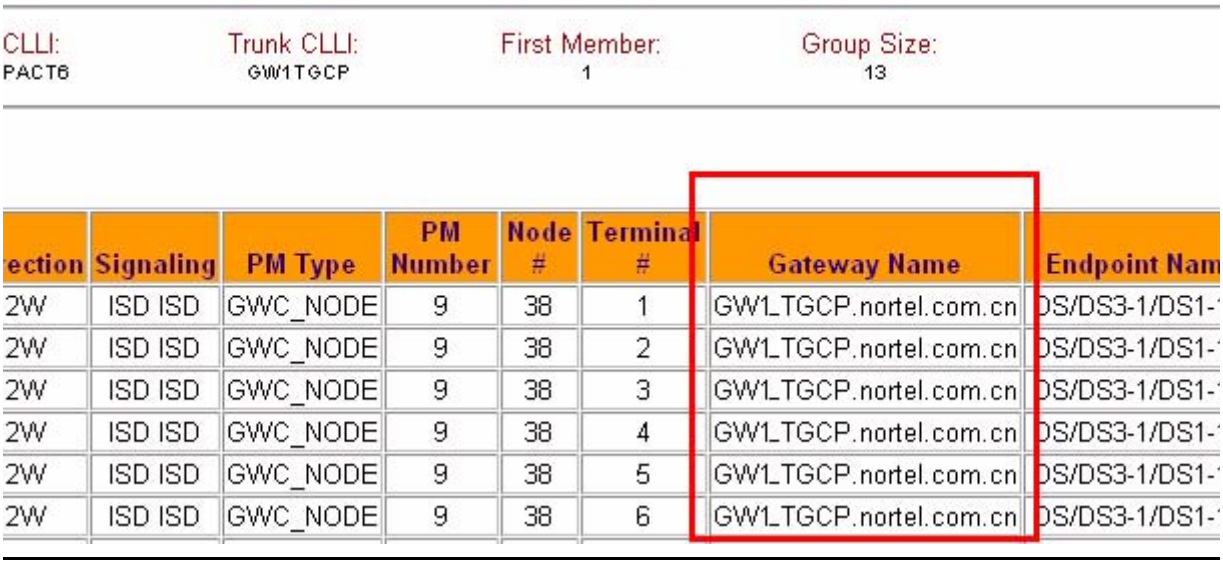
Figure 15 FQDN Gateway Name retrieval - GetTrkCIliByGatewayName



1.4.4 Maintenance By Trunk CLLI

If user performs maintenance actions such as Post and Busy, Gateway FQDN will be displayed on detailed trunk member information.

Figure 16 Mtc by Trunk CLLI



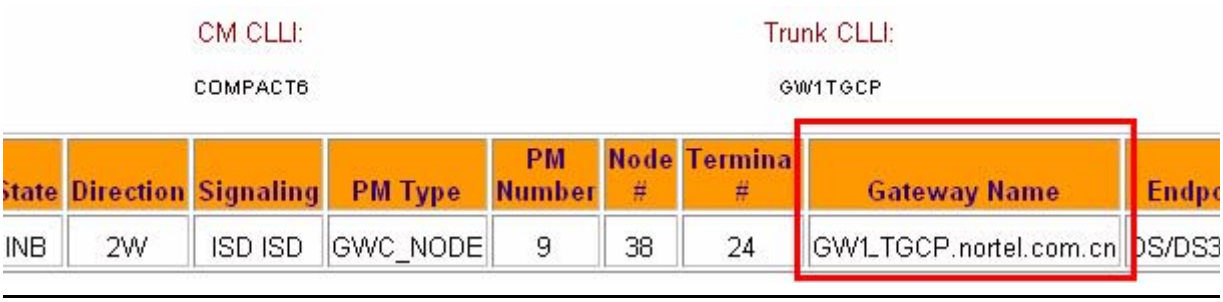
CLLI: PACT6 Trunk CLLI: GW1TGCP First Member: 1 Group Size: 13

ection	Signaling	PM Type	PM Number	Node #	Terminal #	Gateway Name	Endpoint Nam
2W	ISD ISD	GWC_NODE	9	38	1	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	2	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	3	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	4	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	5	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-
2W	ISD ISD	GWC_NODE	9	38	6	GW1_TGCP.nortel.com.cn	DS/DS3-1/DS1-

1.4.5 D-Channel Maintenance

If user post D-Channel by Trunk CLLI, Gateway FQDN will be displayed on detailed D-Channel trunk member information.

Figure 17 D-Channel Maintenance



CM CLLI: COMPACT6 Trunk CLLI: GW1TGCP

State	Direction	Signaling	PM Type	PM Number	Node #	Termina #	Gateway Name	Endpo
INB	2W	ISD ISD	GWC_NODE	9	38	24	GW1_TGCP.nortel.com.cn	DS/DS3

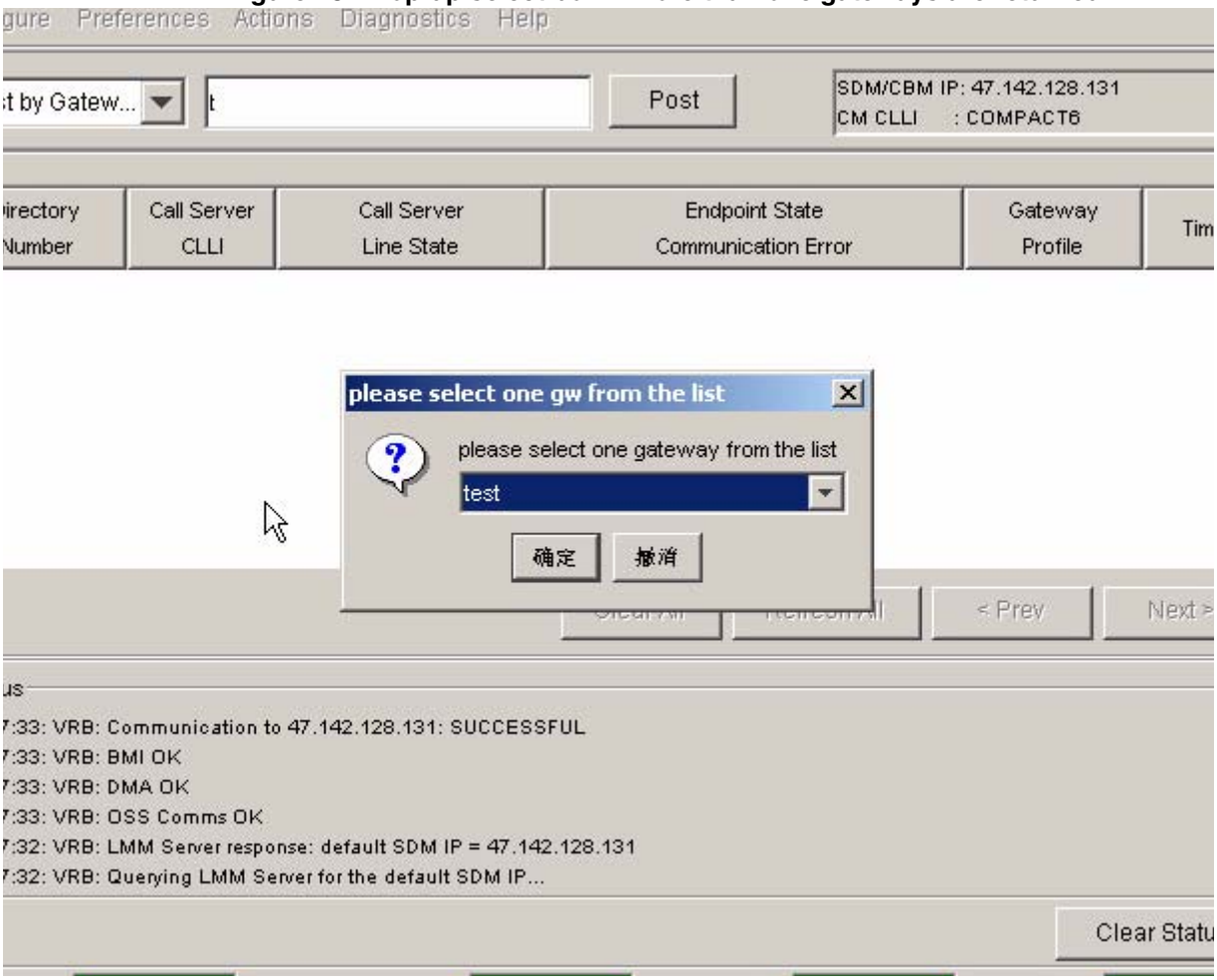
1.5 LMM functionality modifications

1.5.1 “Post by Gateways” operation

“Post By Gateways” can provide users the functionality to post all the DNs that is associated with the specific gateway, in SN08, all the gatways are hostname, but in SN09, both gateway hostname and full FQDN name are all needed to be supported to post the DN.

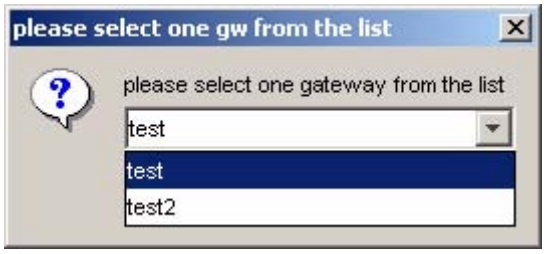
In SN09, the “Post by Gateway” can support the partial query, which means user can input only one part of the gateway name (either gateway hostname or full FQDN name), if there have more than one gateways which can match the partial string, a select box will be pop-uped to let user to choose one, if there is only one gateway to match the query string, it will be used to retrieve all the DNs and no box will be pop-uped.

Figure 18 Pop-up select box if more than one gateways are returned



User can select one gateway from the select box such like the following.

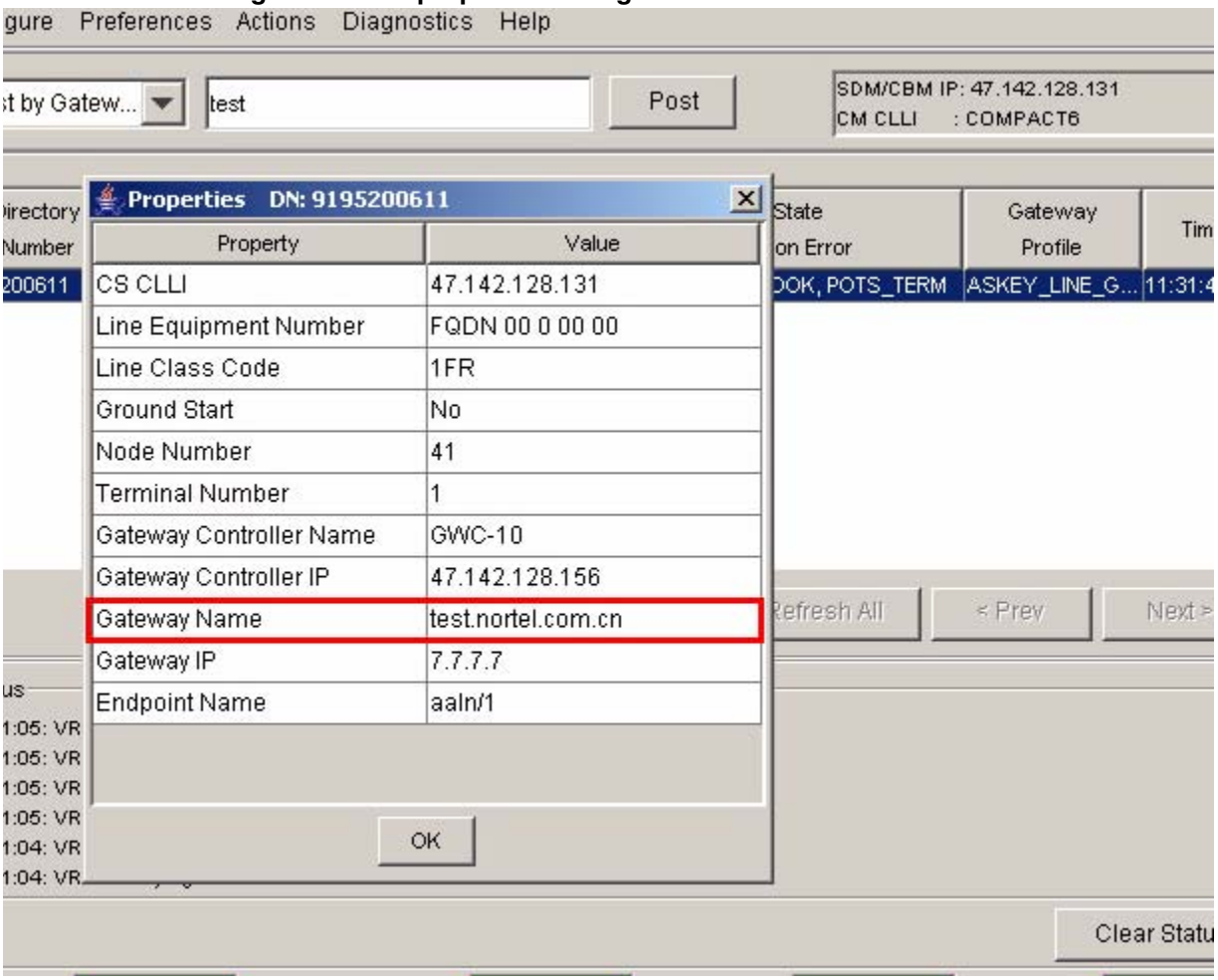
Figure 19 gateway select box



1.5.2 DN's properties dialog

When user right click on a DN and choose the "properties" menu, a DN's properties dialog will appear to show all the properties for the selected DN which includes a gateway name field. If the gateway is associated with a default domain name, the full FQDN name will be displayed in the gateway name field like following diagram.

Figure 20 DN properties dialog



1.6 Other Tools

1.6.1 QGW command on Core

Table LNENDPT is sorted by LENs and may contain up to 150,000 tuples. Therefore, finding all the LENs & Endpoints for a particular Gateway can be somewhat difficult.The Query Gateway Tool (QGW) is a tool on the CM that can be used to output all the LENs and Endpoints for the specified Gateway in table LNENDPT.

To use the command, enter the QGW command at the CM CI prompt, followed by a string denoting the Gateway name. Below is an example of the use of the command:

```
CI:
>qgw 'sbv-10.com6.net'
-------------------------------------------------------
--
LEN: LG    00 0 00 00     ENDPOINT: aaln/1
LEN: LG    00 0 00 01     ENDPOINT: aaln/2
-------------------------------------------------------
--
```

If the Gateway does not exist in table LNENDPT, the following error message is output:

```
>qgw 'sbbv-11.com6.net'
ERROR   - Gateway Name does not exist in table LNENDPT
```

1.7 Hardware Requirements or Dependencies

None.

1.8 Software Requirements or Dependencies

None.

1.9 Limitations and restrictions

1. When associating media gateway, gateway hostname and FQDN must be unique across whole office, otherwise it will be rejected.
2. If a default gateway domain name is provisioned, then together the Gateway Name and the default gateway domain name cannot exceed 64 characters. This rule only be applied to cable solution gateways. Refer to Table 1 on page 1935.
3. If no default gateway domain name provisioned, Small line gateways, TGCP trunking gateway and third party gateway's max name length can up to 64 characters.

1.10 Interactions

None.

1.11 Glossary

Term	Description
CS2K	Call Server 2000
CS2K-MT	Call Server Management Tools
FQDN	Fully Qualified Domain Name
GUI	Graphic User Interface
GW	Gateway
GWC	Gateway Controller
GWCEM	Gateway Controller Element Manager
LMM	Line Maintenance Manager
TMM	Trunk Maintenance Manager
SESM	Succession Element and Subelement Manager
OSSDI	Operations Support System Data Interface

2: Configuration for A00009189

2.1 Hardware and Software Requirements

This feature requires SN09 SESM/Core/GWC loads be installed successfully.

2.2 Initial Configuration

No additional initial configuration step is required by this feature.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

None.

2.4 Upgrade Considerations

None.

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified MIBs and database schema

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
MIB		
GWC-GW-MIB	Changed	New
GWC-ENDPOINT-MIB	Changed	New
GWC-EPID-GRP-MIB	Changed	New
GWC-RMGC-MIB	Changed	New
SESM/GWCEM Database Schema		
GWCEM.GATEWAY	Changed	New
GWCEM.GWDOMAIN	New	New
GWCEM.GATEWAYPROFILE	Changed	Old
GWCEM.GWROOTITRANSMIDDLEBOXES	Changed	Old
GWCEM.GLOBALIDS	New	New

Note: 1) For the MIBs in list above, the old table are deprecated from this release onward. 2) The gateway controller will not support the old MIB table.

2.5.2 MIB GWC-GW-MIB

2.5.2.1 Name: gateWayTableV2

.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.legacyCallServer.lcsGateWayController.gwcGwMIB.gateWayTableV2

2.5.2.1.1 Functional description

From SN09,GWC will use the new table gateWayTableV2 to do corresponding SNMP operations.The difference between new table and old table are;1, expand gateWayName size to 64 characters. 2, Add 32 bits gateWayID. 3, Remove useless columns gateWayHeartBeat and gateWayConnset.

2.5.2.1.2 Usage sequence and implications (CM Only)

Not applicable.

2.5.2.1.3 Size
Same as old table.

2.5.2.1.4 Fields/OIDs

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
gateWayID	New		1	
gateWayNameV2	New		2	
gateWayAddressV2	New		3	
gateWayTypeV2	New		4	
gateWayLgrpV2	New		5	
gateWayProtocolV2	New		6	
gateWayProtVersV2	New		7	
gateWayPortV2	New		8	
gateWayProfileV2	New		9	
gateWayAdjacentMiddleBoxIDV2	New		10	
gateWayEntryStatusV2	New		11	

2.5.2.1.5 Datafill example
Not applicable.

2.5.2.1.6 Table release history update
Not applicable.

2.5.2.1.7 Supplementary information
Not applicable.

2.5.2.1.8 Translation verification and other tools
Not applicable.

2.5.3 MIB GWC-ENDPOINT-MIB

2.5.3.1 Name: endPointTableV2
.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.legacyCallServer.lcsGateWayController.gwcEndPointMIB.endPointTableV2
Functional description

From SN09,GWC will use the new table endPointTableV2 to do corresponding SNMP operations. The difference between new table and old table is epidGWID repalces endPointGW in V2 table.

2.5.3.1.1 Usage sequence and implications (CM Only)

2.5.3.1.2 Size
Same as old table.

2.5.3.1.3 Fields/OIDs

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
epidGWID	New		1	
endPointNameV2	New		2	
endpointTNV2	New		3	
endPointNNV2	New		4	
endPointServStatusV2	New		5	
endPointEntryStatusV2	New		6	

2.5.3.1.4 Datafill example
Not applicable.

2.5.3.1.5 Table release history update
Not applicable.

2.5.3.1.6 Supplementary information
Not applicable.

2.5.3.1.7 Translation verification and other tools
Not applicable.

2.5.4 MIB GWC-EPID-GRP-MIB

2.5.4.1 Name: epidGrpTableV2

.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.legacyCallServer.lcsGateWayController.gwcEpidGrpMIB.epidGrpTableV2

2.5.4.1.1 Functional description

From SN09,GWC will use the new table epidGrpTableV2 to do corresponding SNMP operations.The difference between new table and old table is epidGrpGWID replaces gatewayName in V2 table.

2.5.4.1.2 Usage sequence and implications (CM Only)

Not applicable.

2.5.4.1.3 Size

Same as old table.

2.5.4.1.4 Fields/OIDs

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
epidGrpGWID	New		1	
epidGrpNameV2	New		2	
epidGenerationDescV2	New		3	
nodeNoV2	New		4	
firstTnV2	New		5	
noOfPortsV2	New		6	
v52InterfacesidV2	New		7	
v52LinkidV2	New		8	
v5UALinkidV2	New		9	
priInterfaceidV2	New		10	
epidGrpEntryStatusV2	New		11	

2.5.4.1.5 Datafill example

Not applicable.

2.5.4.1.6 Table release history update

Not applicable.

2.5.4.1.7 Supplementary information

Not applicable.

2.5.4.1.8 Translation verification and other tools

Not applicable.

2.5.5 MIB GWC-RMGC-MIB

2.5.5.1 Name: gwToGwcTableV2

.iso.org.dod.internet.private.enterprises.nortel.voip.ptn.serviceControl.legacyCallServer.lcsGateWayController.gwcRmgcDataMIB.gwToGwcTableV2

2.5.5.1.1 Functional description

From SN09,GWC will use the new table gwToGwcTableV2 to do SNMP operations.The difference between new table and old table is gwFQDNV2 is expanded to 64 characters.

2.5.5.1.2 Usage sequence and implications (CM Only)

Not applicable.

2.5.5.1.3 Size

Same as old table.

2.5.5.1.4 Fields/OIDs

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
gwFQDNV2	New		1	
gwcFQDNV2	New		2	
gwEntryStatusV2	New		3	

2.5.5.1.5 Datafill example

Not applicable.

2.5.5.1.6 Table release history update

Not applicable.

2.5.5.1.7 Supplementary information

Not applicable.

2.5.5.1.8 Translation verification and other tools

Not applicable.

2.5.6 Database Schema: GWCEM.GATEWAY

2.5.6.1 Functional description

This table is used to store provisioned gateway entries, 2 fields will be impacted.

2.5.6.2 Fields

Table 2 Modified/Added fields

Field	New/Changed	Entry	Explanation and action
GATEWAYNAME	Changed	VARCHAR2 (64) NOT NULL	Length will be extended to 64, used to store gateway hostname.
GATEWAYINDEX	New	INTEGER NOT NULL	Gateway index number.

2.5.6.3 Limitations

Field GATEWAYNAME is primary key, so gateway hostname must be completely unique across entire office.

2.5.7 Database Schema: GWCEM.GWDOMAIN

2.5.7.1 Functional description

This new table is used to store provisioned gateway domain name.

2.5.7.2 Fields

Table 3 Fields descriptions

Field	New/Changed	Entry	Explanation and action
GWCID	New	VARCHAR2 (32) NOT NULL	Indicates which GWC this Gateway Domain Name belongs to. Refer to table “GWCEM.GWCNODE“.
DOMAINNAME	New	VARCHAR2 (64) NOT NULL	Gateway domain name.
DOMAININDEX	New	INTEGER NOT NULL	Gateway domain global index number.

2.5.8 Database Schema: GWCEM.GATEWAYPROFILE

2.5.8.1 Functional description

This table stores all data of gateway profiles, new column will be added into this table.

2.5.8.2 Fields

Table 4 New Field

Field	New/Changed	Entry	Explanation and action
FQDN_SUPPORTED	New	VARCHAR2 (5)	Indicate whether the default gateway domain name is supported by this profile. Available values are “true” and “false”. String “false” indicates “not support”, string “true” indicates “support”. The default value is “false”.

2.5.9 Database Schema: GWCEM. GWROOTITRANSMIDDLEBOXES

2.5.9.1 Functional description

Expand gatewayname from 32 charaters to 64 characters.

2.5.9.2 Fields

Table 5 New Field

Field	New/Changed	Entry	Explanation and action
GATEWAYNAME	Changed	VARCHAR2 (64)	To support 64 character FQDN.

2.5.10 Database Schema: GWCEM. GLOBALIDS

2.5.10.1 Functional description

This new added table stores global id of different device.

2.5.10.2 Fields

Table 6 New Field

Field	New/Changed	Entry	Explanation and action
IDTYPE	New	NUMBER NOT NULL	Indicate 8 bits device type that the GID belongs to.
CALLAGENTID	New	NUMBER NOT NULL	Indicate 8 bits CallAgent ID.
KEY	New	NUMBER NOT NULL	Indicate 16 bits key which is unique on IDTYPE and CALLAGENTID.
GLOBALID	New	NUMBER NOT NULL	Indicate 32 bits GID which is unique accross all device type and call agent id.

2.6 Service Orders (SO) (CM & SESM)

None.

2.7 Software optionality control (SOC)

None.

2.8 Element Management

FQDN support was introduced in SN07/SN08, a “dummy” gateway need to be added which created the suffix or domain name for all the gateways on a GWC. The remaining gateways were provisioned using its unique prefix, or hostname. The domain of the ‘dummy’ gateway then could be appended to the end of all NCS and DNS signaling at call processing time.

In SN09, the procedure of domain name configuration is changed. Customer could set a default gateway domain name when adding GWC node. If provisioned, the default gateway domain name will be applied to all the gateways on this GWC (if the gateway profile supports FQDN). The name which customer filled when associating media gateway will be gateway hostname. The gateway FQDN will be concatenation of gateway hostname and default gateway domain name.

In SN09, if customer does not fill default gateway domain name when adding GWC node. No default gateway domain name will be used, customer can fill in FQDN-liked name when associating media gateway (if the gateway profile supports FQDN). The gateway hostname and FQDN will be the same, as the name user filled.

2.8.1 New/modified GUIs

Table 7 New or modified GUIs

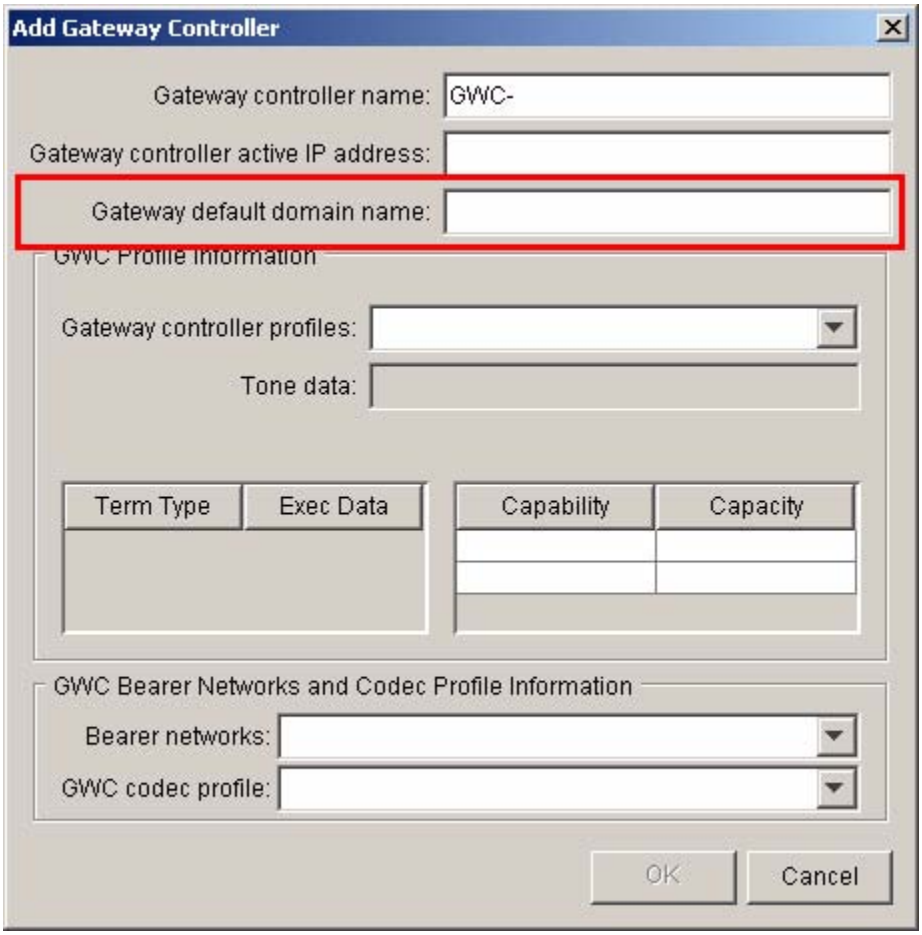
GUI name	NEW, CHANGED, or DELETED
GWCEM	Changed

2.8.2 GUI information

2.8.2.1 GUI name: Add GWC node

This dialog is used to add GWC node by customer. New field “Gateway default domain name” is added in SN09. This field is optional, customer could fill in if default gateway domain name is required. If customer does not fill it when adding GWC node, no default gateway domain name will be set.

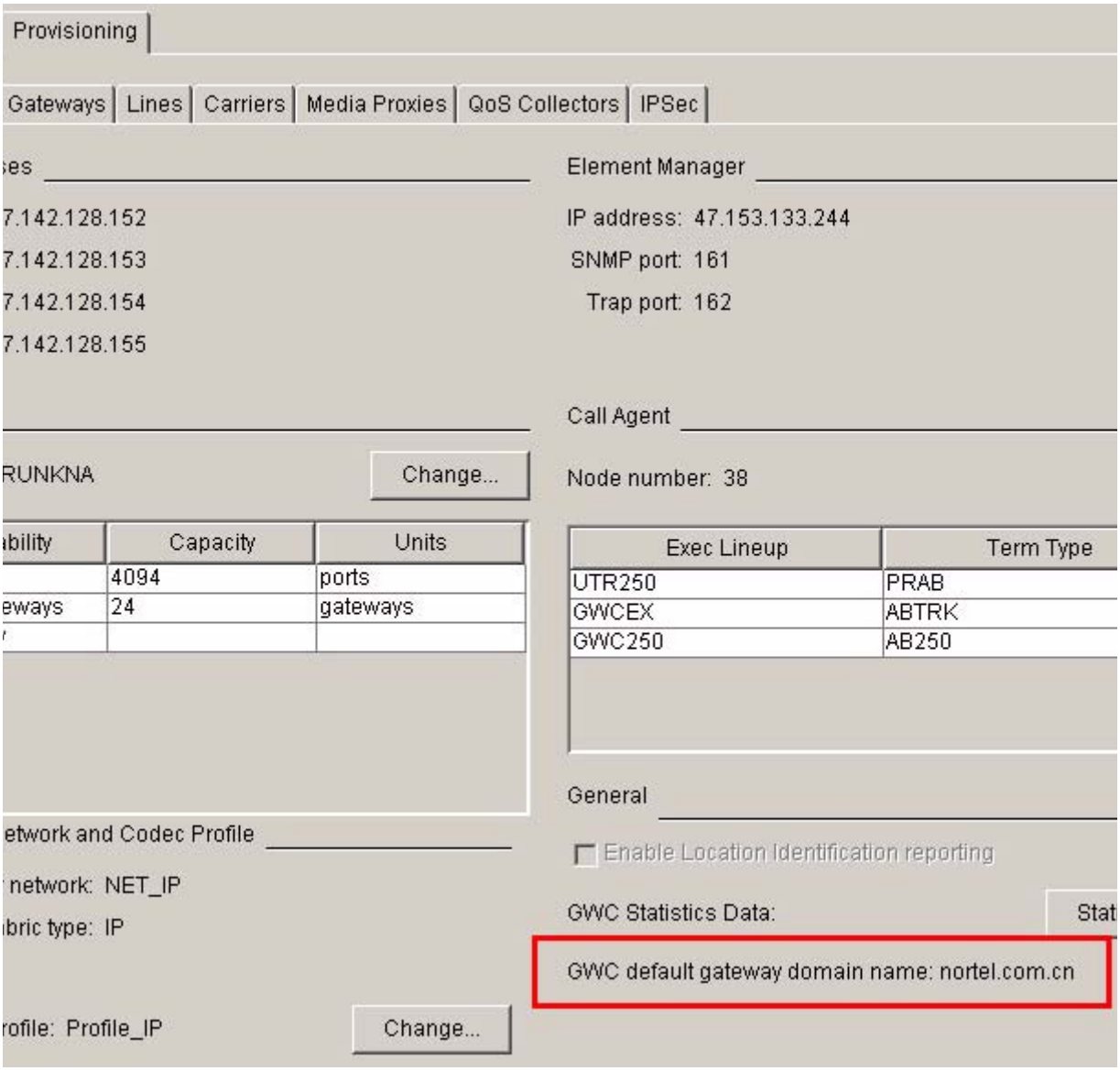
Figure 1 Add GWC node GUI



2.8.2.2 GUI name: GWC provisioning panel

The GWC default gateway domain name will be displayed on right bottom corner of GWC provisioning panel. If no default gateway domain name provisioning on this GWC, it will be displayed as “<Not Configured>”.

Figure 2 GWC provisioning panel GUI



2.8.3 CLUI Interface

None.

2.9 User interface changes

2.9.1 Directory: N/A

2.9.2 Command: QGW

2.9.2.1 Command type: NON-MENU

2.9.2.2 Command target: All

2.9.2.3 Command availability: RES

2.9.2.4 Command description

Table LNENDPT is sorted by LENs and may contain up to 150,000 tuples. Therefore, finding all the LENs & Endpoints for a particular Gateway can be somewhat difficult.The Query Gateway Tool (QGW) is a tool on the CM that can be used to output all the LENs and Endpoints for the specified Gateway in table LNENDPT.

2.9.2.5 Command syntax

Table 8 <CommandName> command parameters and variables

Command	Parameters and variables
QGW	Parms: <GATEWAY> STRING
Parameters and variables	Description
GATEWAY	Displays LENs & Endpoints for the specified Gateway.

2.9.2.6 Qualifications and warnings

None.

2.9.2.7 Responses

Table 9 Command outputs with associated meanings and actions

Command
Command: qgw <Gateway name listed in table LNENDPT> Response: ---------- LEN: LG 00 0 00 00 ENDPOINT: aaln/1 LEN: LG 00 0 00 01 ENDPOINT: aaln/2 ---------- **Meaning:** This response means that the specified Gateway has 2 LENs/Endpoints in table LNENDPT and they are displayed in the response. **System or user actions:** No actions required.
Command: help qgw Response: COMMAND: Query Gateway Outputs all the LENs & Endpoints in table LNENDPT associated with the Gateway. Parms: <GATEWAY> STRING Meaning: This response displays help information for QGW. System or user actions: No actions required.
Command: qgw Response: Next par is: <GATEWAY> STRING Enter: <GATEWAY> Meaning: This response is prompting the user for the GATEWAY name. System or user actions: Enter a Gateway name.

Table 9 Command outputs with associated meanings and actions

Command
Command: qgw <Gateway name not listed in table LNENDPT> Response: ERROR - Gateway Name does not exist in table LNENDPT **Meaning:** This response means that the specified Gateway does not exist in table LNENDPT. **System or user actions:** Check to see if the Gateway name is spelled correctly and re-enter command. If still not found, then check for the Gateway existence in SESM.

2.9.2.8 Example

Table 10 Usage examples for QGW command

Description of task:	
Description of task	qgw 'sbv-10.com6.net'
Command: Command response:	---------- LEN: LG 00 0 00 00 ENDPOINT: aaln/1 LEN: LG 00 0 00 01 ENDPOINT: aaln/2 ----------

2.10 OSSGate Interface Changes

2.10.1 XML Command Changes

When user specify a gateway operation, such as assocMG, disAssocMG, changeMG or addGWCtoCS, system will allow user to input either gateway host name only or the full FQDN name.

2.10.1.1 Command XML

2.10.1.1.1 Add GWC command

A new parameter, gwDefaultDomainName, will be added into the Add GWC xml command which is like the following:

Add GWC to CS XML command

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <addGWCtoCS usn="1" version="1.0">
        <Parameters>
          <csUIName>COMPACT6</csUIName>
          <gwcUIName>GWC-10</gwcUIName>
          <profileName>LARGE_LINENA</profileName>
          <gwcActvIp>47.128.142.156</gwcActvIp>
          <gwcSnmpPort>161</gwcSnmpPort>
          <bearerNetworkName>NET_IP</bearerNetworkName>
          <bearerFabricType>IP</bearerFabricType>
          <codecProfileName>Profile_IP</codecProfileName>
          <termType>POTS</termType>
          <termType>KEYSET</termType>
          <execLineup>POTSEX</execLineup>
          <execLineup>KSETEX</execLineup>
          <gwDefaultDomainName>nortel.com.cn</gwDefaultDomainName>
        </Parameters>
      </addGWCtoCS>
    </Methods>
  </Command>
</CommandList>
```

2.10.1.1.2 disAssocMG XML command

Both gateway hostname and gateway full FQDN name are allowed to input when user want to delete the gateway from system.

disAssocMG XML command with full FQDN name

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <disAssocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>test1.nortel.com.cn</mgUIName>
        </Parameters>
      </disAssocMG>
    </Methods>
  </Command>
</CommandList>
```

disAssocMG XML command with gateway host name

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
    <Methods>
      <disAssocMG usn="1" version="1.0">
        <Parameters>
          <mgUIName>test1</mgUIName>
        </Parameters>
      </disAssocMG>
    </Methods>
  </Command>
</CommandList>
```

2.10.1.1.3 Change MG XML command

Similar with other OSSGate interface, the change gateway interface also changed to support both gateway hostname and full FQDN name.

The xml command is like the following:

Change MG XML command with full FQDN name

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CommandList >
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
      <Methods>
        <changeMG usn="1" version="1.0">
          <Parameters>
            <mgUIName>test1.nortel.com.cn</mgUIName>
            <reservedTerminations>16</reservedTerminations>
          </Parameters>
      </changeMG>
    </Methods>
  </Command>
</CommandList>
```

Change MG XML command with only hostname

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<CommandList >
  <Command>
    <Interface>cs2kCfgMgrIf</Interface>
      <Methods>
        <changeMG usn="1" version="1.0">
          <Parameters>
            <mgUIName>test1</mgUIName>
            <reservedTerminations>16</reservedTerminations>
          </Parameters>
      </changeMG>
    </Methods>
  </Command>
</CommandList>
```

2.10.1.2 Response XML

2.10.1.2.1 QueryGWC response

The gateway domain name that is added with the GWC will be included in the response when user perform a QueryGWC request.

Example:

```
<?xml version="1.0" encoding="UTF-8" ?>
<CommandList>
 <Response>
 <Interface>cs2kCfgMgrIf</Interface>
  <Methods>
   <queryGWC usn="1" version="1.0">
   <ReturnData>
    <Row>
     <gwcUIList>GWC-10</gwcUIList>
     <gwcIpList>47.142.128.156</gwcIpList>
     <callServerId>COMPACT6</callServerId>
     <nodeName>GWC 10</nodeName>
     <typeList>1</typeList>
     <typeList>6</typeList>
     <typeList>7</typeList>
     <typeList>15</typeList>
     <typeList>16</typeList>
     <xacNodeNumber>27</xacNodeNumber>
     <actvIpAddress>47.142.128.156</actvIpAddress>
     <snmpPort>161</snmpPort>
     <mktTones>NORTHAA</mktTones>
     <termTypes>POTS</termTypes>
     <termTypes>KEYSET</termTypes>
     <pmExecs>POTSEX</pmExecs>
     <pmExecs>KSETEX</pmExecs>
     <capacity>6400</capacity>
     <externalIP>NOT_YET_SUPPORTED</externalIP>
     <externalPort>0</externalPort>
     <bearerNetworkName>NET_IP</bearerNetworkName>
     <bearerFabricType>IP</bearerFabricType>
     <codecProfileName>Profile_IP</codecProfileName>
     <gwDefaultDomainName>nortel.com.cn</gwDefaultDomainName>
    </Row>
    <RC>0</RC>
    <MsgTxt>Query of a Single GWC was successful</MsgTxt>
   </ReturnData>
   </queryGWC>
  </Methods>
 </Response>
</CommandList>
```

2.10.2 Additional OSSGate Changes

None.

2.11 Security

None.

2.12 Configuration Walkthrough

Provisioning/configuring component software and services.

Product = CS 2000 Management Tools

A00009310-- SSPFS Restricted Access Shell

Functional Description

1: Applicable Solution(s)

UA-IP

1.1 Description

This feature's intention is to provide a hardened restricted shell for non-administrative CLUI functions on the SSPFS platform. It is expected that customers will use this environment when giving users access to CLUIs residing on SSPFS servers. The users will have a restricted command set and shell environment, unlike today where the user is given an unrestricted shell to run the CLUI utilities.

The restricted shell will use the Solaris resident rksh (restricted Korn shell). With a restricted Korn shell, the user cannot:

- Change the working directory.
- Set the value of SHELL, ENV, or PATH variables.
- Specify the pathname of a command with a '/' in it.
- Redirect output of a command with '>', '>|', '<>', or '>>'.

The only commands available to the user will be those in the PATH variable defined by the user's default .profile. The PATH variable will be made up of the restricted access shell bin directories. The default .profile will be contained in the restricted access shell skeleton directory (/etc/skel.rash).

The application CLUIs (i.e. npm, gwcadmin.sh) currently provide their own level of authentication via the existing login servlet when accessing the CLUI. Within the application, an additional level of command authorization may be used based on the group(s) of the CLUI user. This authorization/ authentication mechanism used by the application CLUIs is functionality that has been in use prior to SN09 and will not be changed by this new content.

At times, a restricted access shell user will need to perform system administrative tasks, which will require root (or other user) access. The restricted access shell user will be required to 'su' to the new user. This feature provides an 'su' wrapper that verifies the user invoking su is a member of either emsadm or secadm group before gaining access to the Solaris resident 'su' command.

1.1.1 Creating Local Restricted Shell User Accounts

To obtain the functionality of this feature, specify the shell to be '/usr/bin/rash' and the skeleton directory to be./etc/skel.rash'. Restrcited access shell users wil lhave their home directory created in /export/home/<user id>. If the user is to be created in the restricted shell environment using the Solaris 'useradd' command, specify the '-s' option for shell, '-d' option for home directory, and '-k' option for skeleton directory. The following is an example of creating restricted access user 'test6' using the Solaris useradd command:

useradd -gsuccssn -Gmgcadm,emsadm -s /usr/bin/rash -d /export/home/test6 -m -k /etc/skel.rash test6

From the example above, user id 'test6' will:

- Have a SHELL equal to restricted access shell (rash) which is ultimately rksh.
- Have a home directory at: /export/home/test6
- Home directory will contain the contents of /etc/skel.rash. This is where the user's .profile is obtained which will contain the limited PATH variable containing only restricted bin directories (i.e. /usr/rbin/basebin)..
- User's primary group is succssn.
- User's secondary groups are mgcadm and emsadm.

1.1.2 Creating Central Restricted Shell User Accounts

To grant restricted shell access to a central user account, the users's shell must be set to '/usr/bin/rash' and user's home directory to '/export/home/<usrname>'. If IEMS Security Server is used to manage the central user account, this is done by setting the user's login shell to 'restricted'.

The creation of user home directory /home/export/<usrname> and copying of user shell profile from skeleton directory /etc/skel.rash are automatically handled by a specialized PAM-MKHOMEDIR SPI.

1.1.3 Registering Restricted Access Shell Executables

Applications will use the Servman utility to register restricted access shell executables. Option '-rash' has been added to Servman which will handle creating the links and removing the links within servman.

To add single files, use the restricted access shell option as follows:

servman register -group newapp *-rash "fullpath;name"*

Note: Where *name* is the symbolic link name in the restricted shell bin directory and *fullpath* is the path to the actual executable. Servman will create a symbolic link in the application restricted bin directory (i.e. /usr/rbin/appbin).

To add multiple files, us a similar command but delimit the entries with the '*' character:

servman register -group oldapp -rash "fullpath1;name*fullpath2;name2"

1.1.4 Restricted Command Set

Much of what makes the restricted access shell restrictive is the limited command set. This command set will be split into base level commands and application level commands. Base level commands include Solaris resident commands and SSPFS delivered commands. Application commands includes commands installed after SSPFS, such as application CLUIs (i.e. gwcem, sam21em).

Table 1: Solaris and SSPFS Commands

Command	Comment/Usage
awk	pattern scanning
cat	concatenate and display files
cli	SSPFS command line interface, mainly for configuration changes.
cut	cut out selected fields of each line of a file
df	displays number of free disk blocks and files
grep	search a file for a pattern
iostat	report I/O statistics
ipcs	report inter-process communication facilities status
kill	terminate or signal processes
less	browse or page through a text file (
ls	list contents of directory
more	browse or page through a text file
netstat	show network status
ps	report process status
servquery	Query the status of SSPFS applications
sort	sort, merge, or sequence check text files

Table 1: Solaris and SSPFS Commands

Command	Comment/Usage
su	Wrapper that only allows users in group emsadm or secadm to access Solaris su.
top	provide system and process status
head	display first few lines of files
tail	display the last part of a file
vmstat	report virtual memory statistics

Table 2: Application (other) Commands

Command	Comment/Usage
npm	Network Path Manager CLUI
gwcad-min.sh	GatweWay Controller Element Manager CLUI
bpt	Bulk Provisioning Tool
sam21em	SAM21 Element Manager CLUI
?	SNMP Poller - executables needed not provided at this time.
?	OMPUSH - executables needed not provided at this time

Note: Currently, IEMS exposes the following commands to be executed on the SSPFS element in an unrestricted shell, logging in as root user via ssh: *servquery -status all, swact, servstart IEMS, init 6*. IEMS will continue to function in this manner for SN09 as the scope of this feature does not include changing existing “root only” commnads and having them execute in a restricted shell environemnt.

1.2 Hardware Requirements or Dependencies

Not applicable.

1.3 Software Requirements or Dependencies

Not applicable.

1.4 Limitations and restrictions

Not applicable.

1.5 Interactions

First interaction is the change to the shell environment users may get when they are given access to the SSPFS server to invoke maintenance CLUIs. Today, the user is granted an unrestricted shell to access the CLUIs, which gives the user access to other server resources which may not be the desired. This feature restricts the user's environment, limiting the server's exposure to only the user's home directory. In addition, the users PATH will also be limited to directories which contain a subset of available server executables.

1.6 Glossary

Term	Description
CLUI	Command Line User Interface
PAM	Pluggable Authentication Module
SSPFS	Succession Solution Platform Foundation Server

Product = CS 2000 Management Tools

A00009339 -- Packet Cable T.38 Support

Functional Description

1: Applicable Solution(s)

IAC

1.1 Description

This activity provides packet cable support for T.38 Fax based on PacketCable1.5 Specifications. It adds T.38 fax element into the LCO (for NCS and TGCP) which is sent to the gateway at the start of a call. The presence of this information triggers the gateway to include the T.38 into its SDP response. This is then used by the far end gateway to ensure that both gateways support T.38 before the functionality is used.

This activity provides T.38 support which is compliant with the PacketCable 1.5 Specifications.

The switch-over to T.38 is performed based on the MTA or MG sending a detection of the “t38 start” event. If the T.38 codec is supported by both gateways, the call switches to T.38 mode once the switching sequence completes.

This feature will implement T.38 strict and loose modes, as described in the PacketCable 1.5 Specifications. If strict mode is active, the attempt to switch to T.38 codec will only occur if both gateways in the call advertise T.38 capabilities in their SDP (refer to the CS2000 T.38 Gateway Interoperability Specification for details). If loose mode is active, the CS2000 will attempt to switch to T.38 even if one side does not advertise T.38 capabilities. In loose mode, when the codec switch is rejected by either end, an attempt will be made to preserve the call by switching back to G.711 codec.

Prior to SN09, the only choice for T.38 was enabled or disabled. The equivalent for “enabled” is “strict” mode in SN09.

Strict Mode is recommended to be used if all Gateways in a customer network support T.38. Due to increased messaging, Loose Mode is only recommended when there are gateways in the network that (1) support the T.38 codec, and (2) do not advertise this support in the SDP. This scenario is common when SIP trunks are being used, but is unlikely when a customer has exclusively PacketCable 1.5-compliant devices and/or a T.38-capable PVG.

Loose Mode is not recommended to be used during an SN09 upgrade while Gateways are being upgraded to T.38-capable loads. Instead, it is recommended to leave T.38 off until all Gateways have been upgraded, then turn it to “strict” or “loose” as appropriate.

The customer must configure T.38 in either “strict”, “loose”, or “off” mode via the GWC Element Manager in CS2M. Since this setting can be different for each GWC, there is a possibility of different modes being applied to each Gateway involved in a FAX call. It is recommended that customers choose the same T.38 mode across all GWC’s. If different modes must be used, the customer must select either “strict” or “loose” across all profiles. T.38 calls are not supported and will fail if any profiles have T.38 configured to the “off” setting.

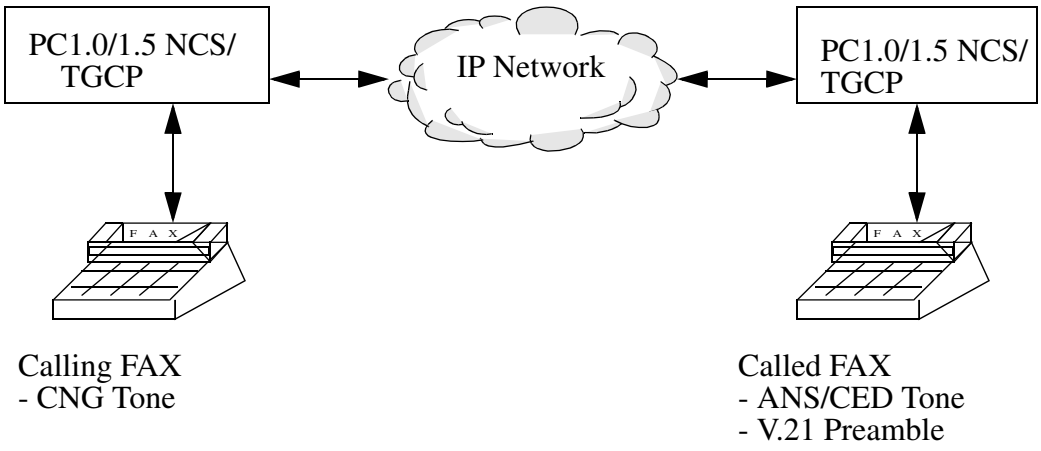
This feature requires that a non-compression codec (G.711) must always be an alternative in the codec list when one or more compression codecs are used. This provides an alternative to allow the FAX call to succeed in the event that one Gateway does not support T.38. If T.38 loose mode is active, one of the gateways in a call does not support T.38, and a compression codec is in use, the gateways must autonomously switch to G.711 without direction from the CS2K.

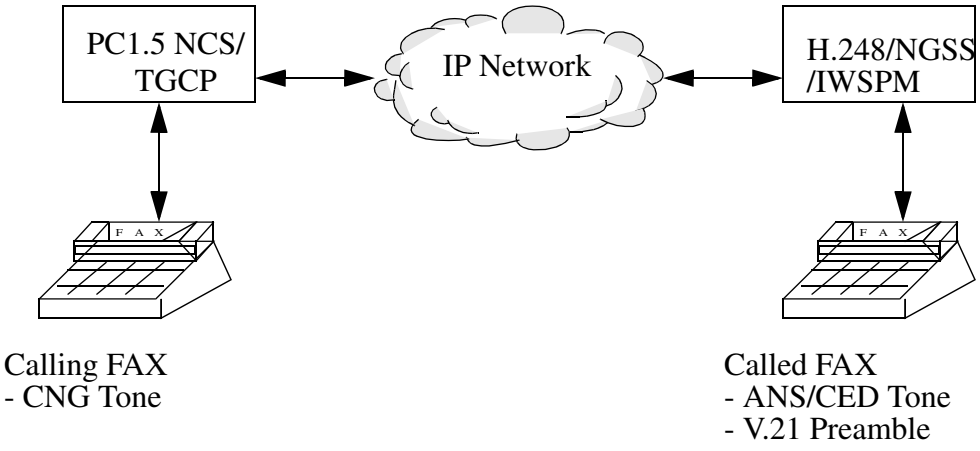
This feature is dependent on SN09 activity A00009294 and A00009443 for SIP/NGSS interworking.

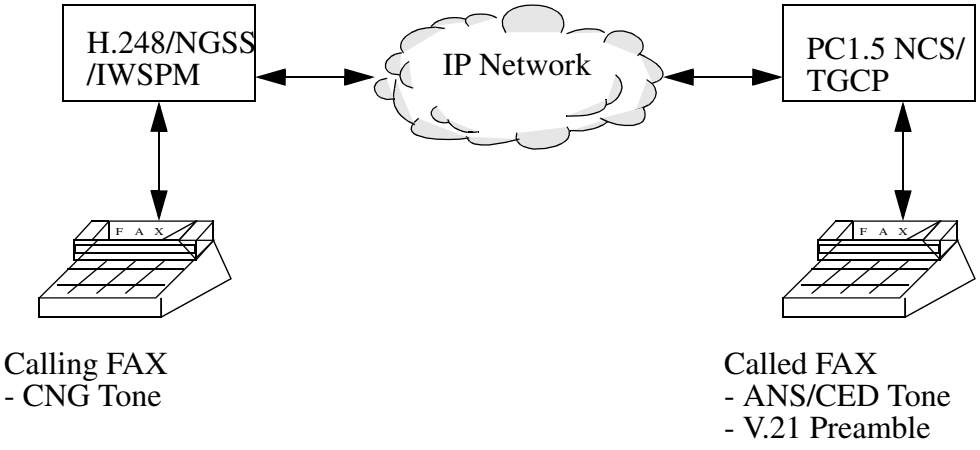
1.2 Interworking and Scenarios

The feature covers FAX interworking between the following GWs in the Cable Solution:

- PacketCable 1.5 GW (MTA or MG)
- PacketCable 1.0 GW (MTA or MG)
- PVG (T.38 Annex D only)
- M2000 (T.38 Annex D only)
- SIP/SIPT
- IWSPM (G.711-only)







1.3 Software Requirements or Dependencies

The feature requires the following items in place for successful T.38 functionality:

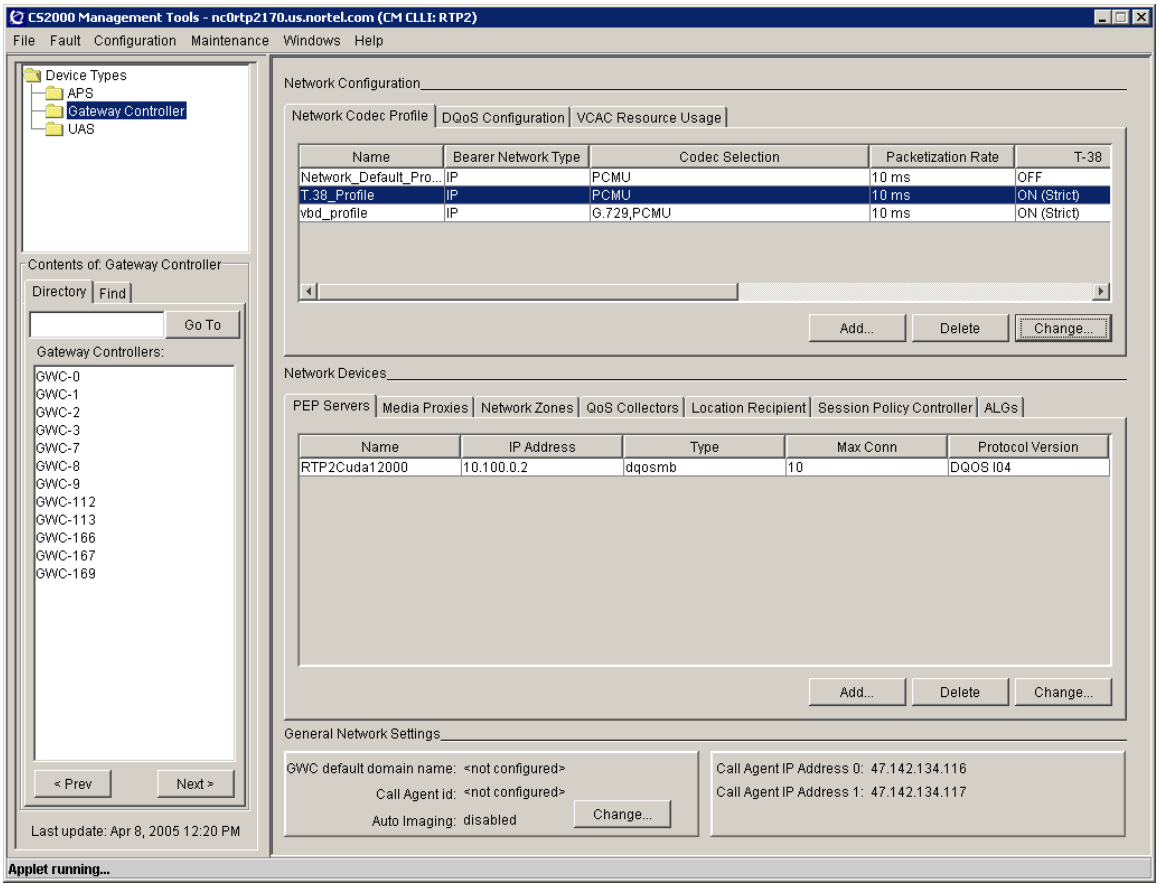
- SN09 SESM for setting up T.38 mode
- PacketCable 1.5 compliant GWs

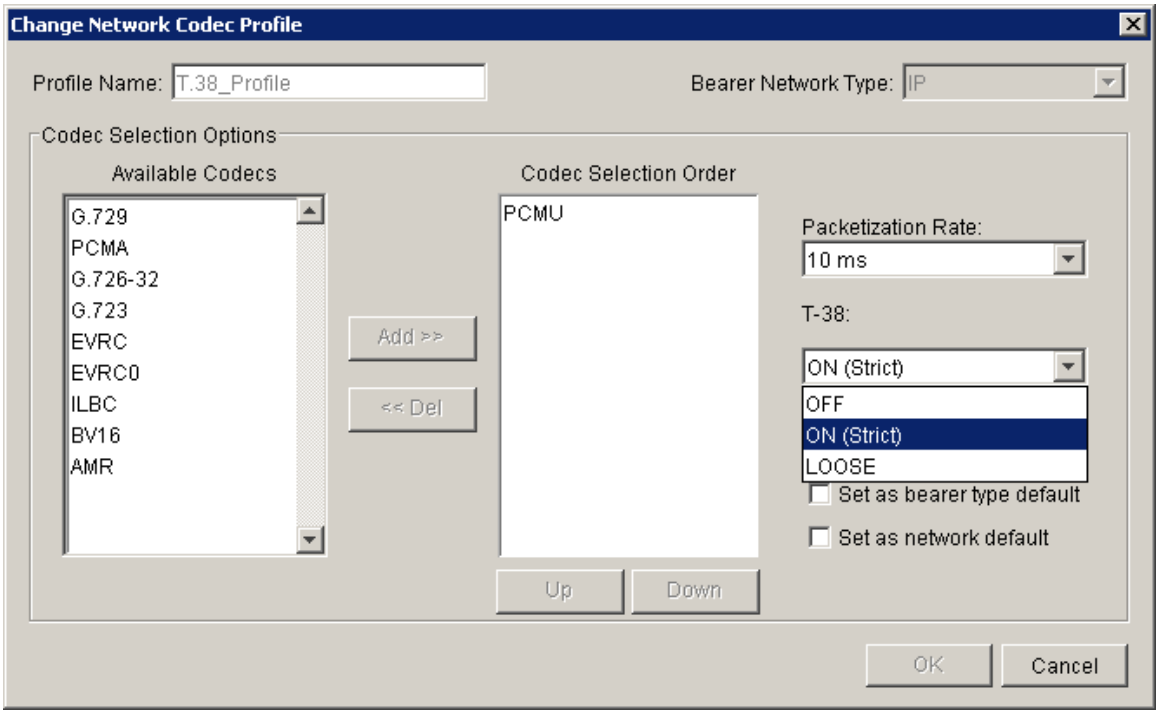
  Note: PacketCable GW's MUST advertise support for the FXR package in the Capabilities Audit response in order to use T.38.
- GWC load with all the feature related changes (including A00009294 and A00009443 content)

1.3.1 T.38 Provision from SESM

When adding a new network profile, the user could choose from one of three T.38 options currently provided on the CS2M GUI. The options are: “OFF, “ON (STRICT)”, and “LOOSE”. Prior to SN09, OFF was represented by disabled and ON (STRICT) was represented by enabled. The option “LOOSE” is used for packet cable. The figure below shows the T.38 options that the user may select from.

Figure one: Add network Codec Profile interface



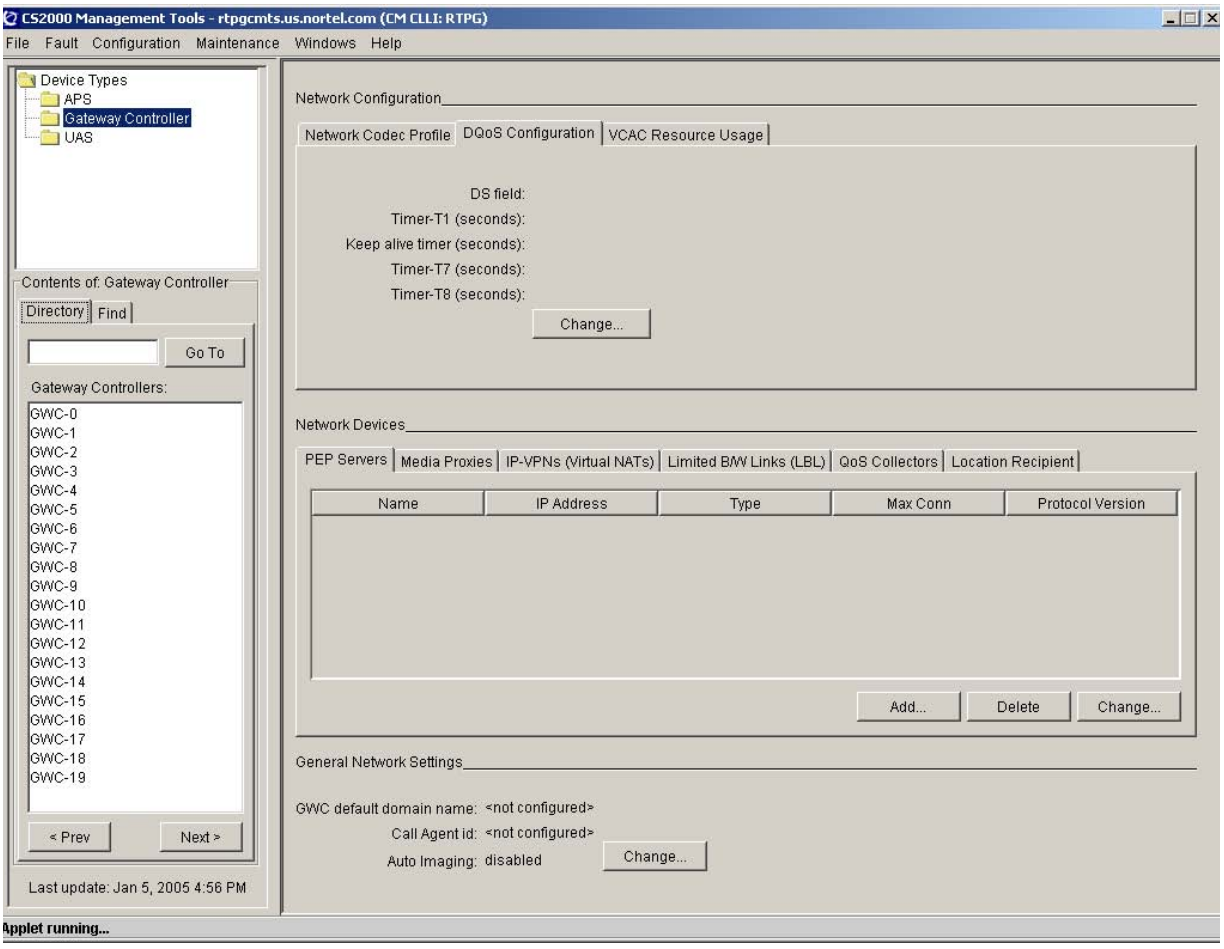


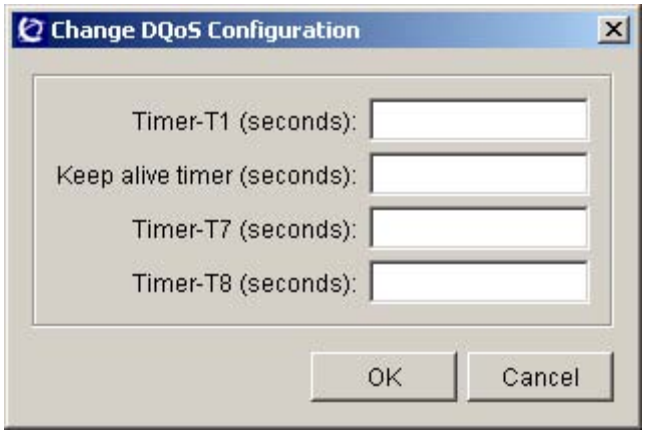
1.3.2 DSCP Provision in SESM

DS field is a fundamental value used for classification and marking of IP packets to achieve end-to-end QoS. This is an 8-bit value sent to CMTS from GWC via DQoS Signaling. This value will overwrite the TOS field in the IP header set by MTA. The media packet forwarding will then be prioritized according to the given DSCP, which is the most significant 6-bit value of the DS field. Prior to this feature, the DS field is hardcoded and set to 10111000 (184 in decimal) in SESM DQoS configuration GUI and it is displayed as “Expedited Fwding” after the user provisions the other DQoS values via “Change DQoS Configuration” dialog.

Figure 1 shows the DQoS configuration GUI display prior to this feature.

Figure 1 DQoS configuration GUI prior to this feature

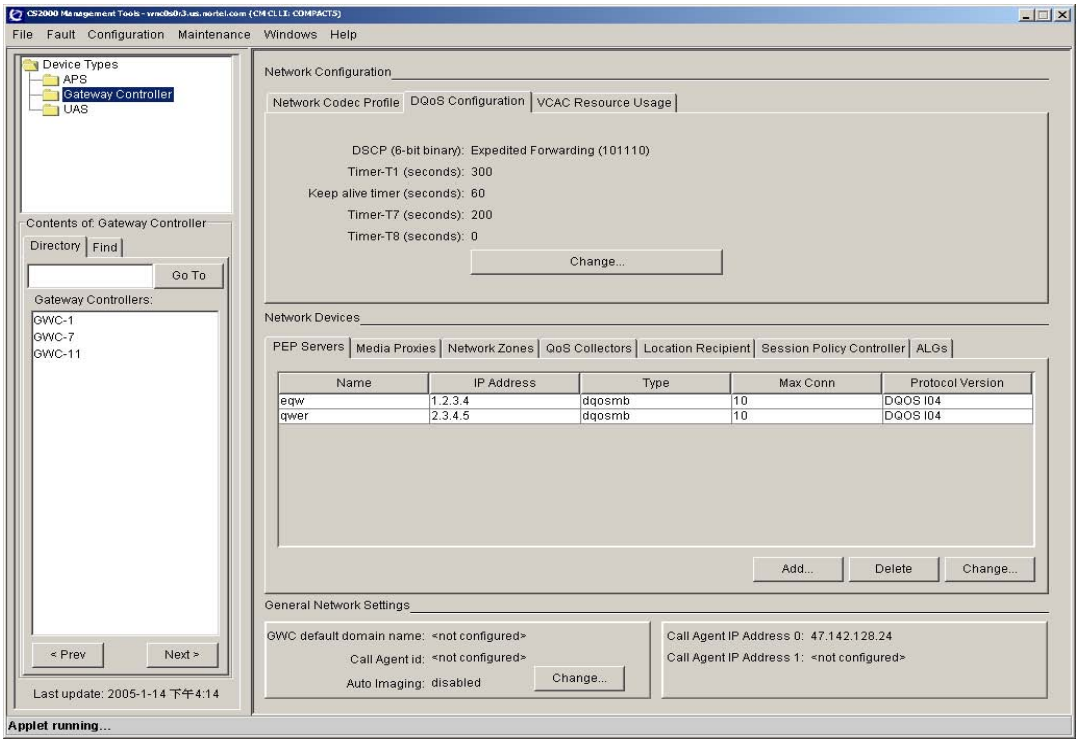




Change from “DS field” to “DSCP (6-bit binary)” will be made to avoid any confusion between the 6-bit DSCP and an 8-bit DS Field value. On the “Change DQoS Configuration” dialog GUI, the “DSCP (6-bit binary)” field will be added. The pulldown menu containing predefined IP Service Class

names will be provided for the selection (please refer to Table 1, “DiffServ Code Point Allocation,” on the following page). User could also input 6-bit binary stream. If the DSCP stream input is not in the pulldown menu, the raw binary stream will be displayed. For example, in the second figure below, the default value is EF (101110).

Changed DQoS Configuration GUI



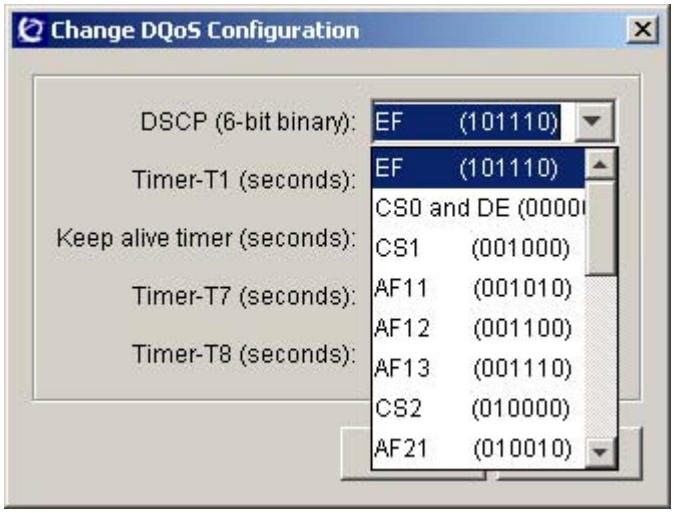


Table 1: DiffServ Code Point Allocation

DSCP	PHB	Status - Reference
000 000	CS0 and DE	RFC 2474
000 001	---	EXP/LU
000 010	---	UASS
000 011	---	EXP/LU
000 100	---	UASS
000 101	---	EXP/LU
000 110	---	UASS
000 111	---	EXP/LU
001 000	CS1	RFC 2474
001 001	---	EXP/LU
001 010	AF11	RFC 2597
001 011	---	EXP/LU
001 100	AF12	RFC 2597
001 101	---	EXP/LU
001 110	AF13	RFC 2597
001 111	---	EXP/LU
010 000	CS2	RFC 2474
010 001	---	EXP/LU
010 010	AF21	RFC 2597
010 011	---	EXP/LU
010 100	AF22	RFC 2597
010 101	---	EXP/LU
010 110	AF23	RFC 2597
010 111	---	EXP/LU
011 000	CS3	RFC 2474
011 001	---	EXP/LU

DSCP	PHB	Status - Reference
100 000	CS4	RFC 2474
100 001	---	EXP/LU
100 010	AF41	RFC 2597
100 011	---	EXP/LU
100 100	FA42	RFC 2597
100 101	---	EXP/LU
100 110	FA43	RFC 2597
100 111	---	EXP/LU
101 000	CS5	RFC 2474
101 001	---	EXP/LU
101 010	---	UASS
101 011	---	EXP/LU
101 100	---	UASS
101 101	---	EXP/LU
101 110	EF	RFC 2598
101 111	---	EXP/LU
110 000	CS6	RFC 2474
110 001	---	EXP/LU
110 010	---	UASS
110 011	---	EXP/LU
110 100	---	UASS
110 101	---	EXP/LU
110 110	---	UASS
110 111	---	EXP/LU
111 000	CS7	RFC 2474
111 001	--	EXP/LU

Table 1: DiffServ Code Point Allocation

DSCP	PHB	Status - Reference
011 010	AF31	RFC 2597
011 011	---	EXP/LU
011 100	AF32	RFC 2597
011 101	---	EXP/LU
011 110	AF33	RFC 2597
011 111	---	EXP/LU

DSCP	PHB	Status - Reference
111 010	--	UASS
111 011	--	EXP/LU
111 100	--	UASS
111 101	--	EXP/LU
111 110	--	UASS
111 111	--	EXP/LU

This function has no impact to GWC because the DSCP value is converted to DS field (8-bit) by left-shift 2. This guarantees that bit 6 and 7 are set to zero.

1.4 Limitations and restrictions

In order to interworking with NGSS/SIP or SIPT, the NGSS software containing A00009443 content needs in place so that T.38 can be set properly. And for interworking with H.248 PVG, A00009294 GWC-related content is also required.

This feature will not support T.38 interworking with Gateways not included in the Cable Solution. This includes (but is not limited to) H.323 gateways, MGCP gateways, and other H.248-based gateways such as MG9K.

A PVG with a VSP3 card is required for T.38 interworking with PacketCable devices.

This feature will NOT support T.38 interworking with the IWSPM. G.711 will be used for all FAX calls involving the IWSPM.

This feature will only perform T.38 integration testing with Gateway vendors that can provide a T.38-capable load during the design phase of this feature. At the time of this FN, this only includes the Arris TTM. Currently, Motorola MTAs and Nuera Media Gateways are not planned for integration testing.

This feature will not make use of the fax tone "ft" or modem tone "mt" events in NCS or TGCP.

There is no impact to PacketCable Event Messaging due to T.38 behavior, with the exception of Electronic Surveillance. This feature will not support PacketCable 1.5 Electronic Surveillance, since there is other work required beyond the scope of this feature for full PC 1.5 ES compliance.
If the customer chooses to interwork with a Gateway (or SIP Client on the far end of a SIP trunk) that supports neither G.711 nor T.38, FAX calls will fail regardless of whether strict or loose mode is active.

T.38 functionality will not be supported for TGCP PTS trunks.

T.38 Annex D functionality is not supported between VRDN-based SIP Trunks and H.248 gateways (e.g. PVG). Therefore, if a PacketCable MTA/MG originates a call through a VRDN SIP trunk, terminating to a PVG, FAX calls will not be successful. This scenario will work with NGSS SIP trunks configured for T.38 support. Also, PacketCable MTA/MG to VRDN SIP to PacketCable MTA/MG calls will be supported using T.38.

1.5 Interactions

Not Identified.

1.6 Glossary

Term	Description
CS2K	Call Server 2000
CMTS	Cable Modem Termination System
MTA	Multimedia Terminal Adapter
GWC	Gateway Controller
MGC	Media Gateway Controller - refers to GWC/CS2K for trunks
PVG	Passport Packet Voice Gateway (Passport15000)
SDP	Session Description Protocol (IETF RFC 3266)
G3FE	Group 3 Facsimile Equipment G3FE refers to any entity which presents a communication interface conforming to ITU- T Recommendation T. 30, T. 4, and optionally T. 6. A G3FE may be a traditional G3 facsimile machine, an application with a T. 30 protocol engine or any other possibility mention in the network model for IP Facsimile mentioned in Recommendation T. 38.
SIP	Session Initiation Protocol (IETF RFC 3261)
SIP-T	Session Initiation Protocol - Telephony ITU-T based standard, that encapsulates ISUP messaging as payload within SIP messages.
UDP	User Datagram Protocol (IETF RFC 768)
UDPTL	Facsimile UDP Transport Layer protocol (ITU T.38)
CED	Called terminal identification answer tone of Fax device (2100 +/- 15 Hz, continuous tone, duration 2.6-4.0 sec.) see T.30 chapter 4.1

Term	Description
CNG	Calling tone of Fax device (1100 +/- 38 Hz, 0.5 sec. on, 3.0 sec. off, duration 60-120 sec.) see T.30 chapter 4.2.
V.21 Preamble	Series of flag sequences 01111110 for 1 sec +/- 15%.

Product = CS 2000 Management Tools

A00009890 -- Provisioning for Media Proxy insertion for SIP lines

Functional Description

1: Applicable Solution(s)

CHS

1.1 Description

In SN09 SIP lines will be supported on the CS2k via a new component, the Session Server (aka 'Phoenix'), which is based on re-use of various MCS components. It is necessary to allow SIP Lines to reside in private VPNs, as is already provided for fixed VOIP line gateways and CICM terminals. This is achieved by appropriate Media Proxy insertion by the CS2K. This feature provides the provisioning necessary to support Media Proxy insertion for SIP lines.

During a call, the VPN ID of a SIP line will be determined by the Session Server (via a mapping of 'Location ID' to 'Routability Group'), while the VPN ID of a fixed VOIP/CICM line is determined by the GWC, via SESM provisioned IP-VPN(NAT) Network Zones and 'Distributed VPNs'. Hence in order to allow correct comparison if the VPN IDs at the two ends of a call and Media Proxy insertion if required, the VPN IDs in GWC and Session Server must be consistent. This feature ensures that both the GWC and the Session Server have the same VPN ID information to allow the correct insertion of Media Proxies, by flow-through provisioning of IP-VPN(NAT) network zones and Distributed VPNs from SESM to the Session Server.

Data synchronisation is managed by the CS2K Audit, for cases in which the SESM and Session Server data are inconsistent and for commissioning support.

Example flow-through case: To create a IP-VPN(NAT) Zone.

- Use the SESM GUI to add a new IP-VPN(NAT) Zone named “maidenhead.com”.
- If a Session Server(MCS-EM) is configured into the SESM an add Routability Group request is sent to the Session Server via the OPI interface.
- On a successful response from the Session Server, the SESM will allow the IP-VPN(NAT) Zone to be created and displayed to the user.

Related activities are:

- ACTID xxxxx MP insertion for SIP lines OPI changes on Session Server(MCS-EM)
- SN09 feature A00008522, SESM Support for SIP Lines, which implements the SIP Proxy on SESM
- SN09 feature A00007217, OAM-Itrans Media Proxy Selection

1.2 Hardware Requirements or Dependencies

Not applicable

1.3 Software Requirements or Dependencies

Session Server OPI version 9.0 software (OPI version allows Routability Group ID’s)

1.4 Limitations and restrictions

Multiple CS2M Configuration managers should not connect to a single Session Server(MCS-EM). The result of this would mean that a shared IP-VPN(NAT) Zone would not be allowed to be provisioned into the 2nd to nth CS2M Configuration managers and hence omit the 2nd...nth CS2Ks from having gateways/endpoints provisioned within the shared IP-VPN(NAT). This is not a supported configuration for SN09 release.

1.5 Interactions

For customer deployments where a Session Server is introduced into the CS2k for SIP Lines functionality, this feature will enforce data synchronisation between the SESM and Session Server. Where data synchronisation fails, an alarm will be generated to inform the customer.

The existing funtionality of creating a IP-VPN(NAT) Zone and creating a Distributed IP-VPN (NAT) Zone will only succeed if the Session Server accepts the flow-through provisioning data from the SESM.

e.g. If the flow-through provisioning of the IP-VPN (NAT) Zone information to the Session Server fails this will cause the creation of the IP-VPN (NAT) Zone to fail on the SESM.

The existing funtionality of the CS2K data audit, will also attempt to synchronise the data between the SESM and the Session Server.

1.6 Glossary

Term	Description
NAT	Network Address Translation
IP-VPN	Internet Protocol - Virtual Private Network

2: Configuration for A00009890

2.1 Hardware and Software Requirements

The Session Server :MCS-EM OPI v9.0 or above provisioning interface.
The Session Server :MCS-EM Admin user name and password available to CS2K(SESM) configuration engineer.

2.2 Initial Configuration

See the Session Server(MCSEM) configuration that has been documented under activity A00008522.

As documented by the above acivity the SESM (CS2M) needs to be pre-configured to add connectivity information for the Session Server(MCSEM).

e.g. IP Address, Port, Username and Password for the Session Server(MCSEM).

2.3 Upgrade Considerations

2.3.1 Element Management Upgrade

For CS2M upgrade from versions 6.2 , 7.0 and 8.0 to SN09.

If there has been any IP-VPN(NAT)s provisioned in the CS2M configuration manager, these will need to be synchronised with the Session Server(MCSEM). Before the syncronisation can take place the Call Agent ID is required to be entered. If the Call Agent ID is not already provisioned a prompt will ask the user to enter the Call Agent ID, this should be a number that uniquly qualifies the call agent within the customer domain. e.g. If a carrier has 5 CS2Ks then they should be numbered 1..5 in each CS2K Configuration manager.

The CS2K Audit will attempt to perform a regular synchronisation. If the user wishes to commission this information prior to the scheduled audit, then a

manual audit request will synchronise the data to allow correct Media Proxy insertion for SIP lines.

2.3.2 Downgrade impact

None

2.4 Element Management

The CS2M configuration manager :GWCEM has been modified to flow-through IP-VPN (NAT) Zone information to the Session Server(MCSEM). This is only visible to the user if there is an error condition. The error sent to the user may inform them that the Session Server(MCSEM) has failed to add the IP-VPN(NAT) Zone and therefore the current operation has failed.

The CS2K Audit GUIs have been modified to allow the user to audit the Session Server(MCSEM) provisioning data.

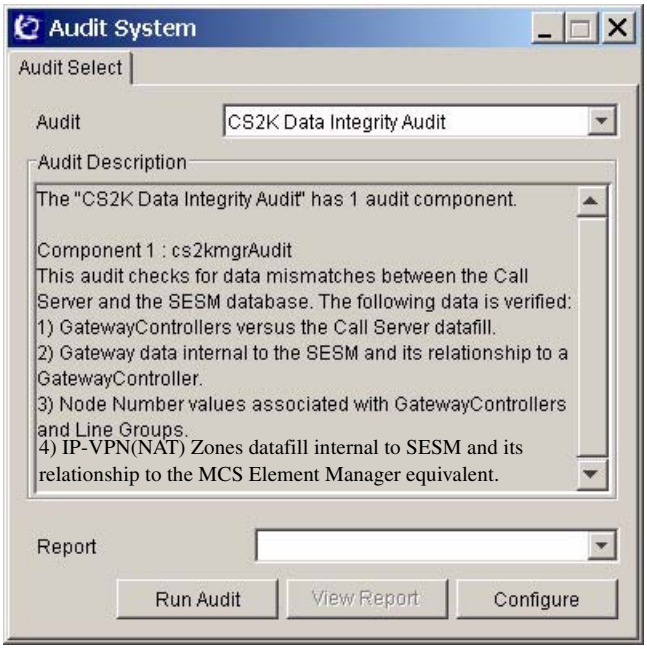
2.4.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
Audit System	Changed
CS2K Data Integrity Audit Configuration	New
CS2K Data Integrity Audit Report	Changed

2.4.2 GUI information

2.4.2.1 GUI name: Audit System



2.4.2.1.1 Functional description

Functionality is unchanged, however when selecting the “CS2K Data Integrity Audit” from the pull down selector, the Audit Description text is enhanced to describe the introduction of new audit functionality related to the audit of IP-VPN(NAT) Zones data fill against the Session Server(MCSEM).

2.4.2.1.2 GUI usage and implications

Unchanged.

2.4.2.1.3 GUI size

Table 2 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
Audit System	0	1	Minimal impact

2.4.2.1.4 GUI fields

Unchanged.

2.4.2.1.5 Usage example

No change in usage.

2.4.2.1.6 GUI release history update

2.4.2.1.7 Context sensitive launching information
None.

2.4.2.1.8 Supplementary information
None.

2.4.2.2 GUI name: CS2K Data Integrity Audit Configuration

2.4.2.2.1 Functional description
This GUI allows the user to selectively run the existing CS2K data integrity audit, the new CS2K SIP Media Proxy Data Integrity Audit or both audit components.

The GUI is accessed from the Audit System GUI upon selecting the “CS2K Data Integrity Audit” and pressing the “Run Audit” button.

2.4.2.2.2 GUI usage and implications
This GUI allows the user to select which sub components of the CS2K data integrity audit to run. This is done by selecting the check boxes for the 2 sub components.

The user is able to restrict the audit run to only those areas of interest. By selecting the “CS2K Call Server Data Integrity Audit” the exisiting audit functionality is exercised whereas by selecting the “CS2K SIP Media Proxy Data Integrity Audit”, the integrity of network zone datafill provisioned jointly at the CS2K and the MCS element manger is exercised.

Where the MCS element manager is not provisioned at the CS2M, the “CS2K SIP Media Proxy Data Integrity Audit” option will be disabled.

By selecting the “Run Audit” button, the required audit components will be run. Where no audit components have been selected, the “Run Audit” button will be disabled.

The “Close” button cancels the run of the audit components and closes the GUI.

2.4.2.2.3 GUI size

Table 3 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
CS2K Audit Config	0	1	Minimal

2.4.2.2.4 GUI fields

The following table lists fields for GUI CS2K Audit Config.

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
CS2K Call Server Data Integrity Audit	New	-	check box	Selects if the CS2K Call Server Data Integrity Audit will be executed	-
CS2K SIP Media Proxy Data Integrity Audit	New	-	Check box	Selects if the CS2K Media Proxy Data Integrity Audit should be executed	-
Run Audit	New	-	Button	Run the selected audit sub components	-
Close	New	-	Button	Close the GUI without running the selected audit sub components	-

2.4.2.2.5 Usage example

See Main screen shot for an example of both audit sub components selected.

2.4.2.2.6 GUI release history update

New functionality

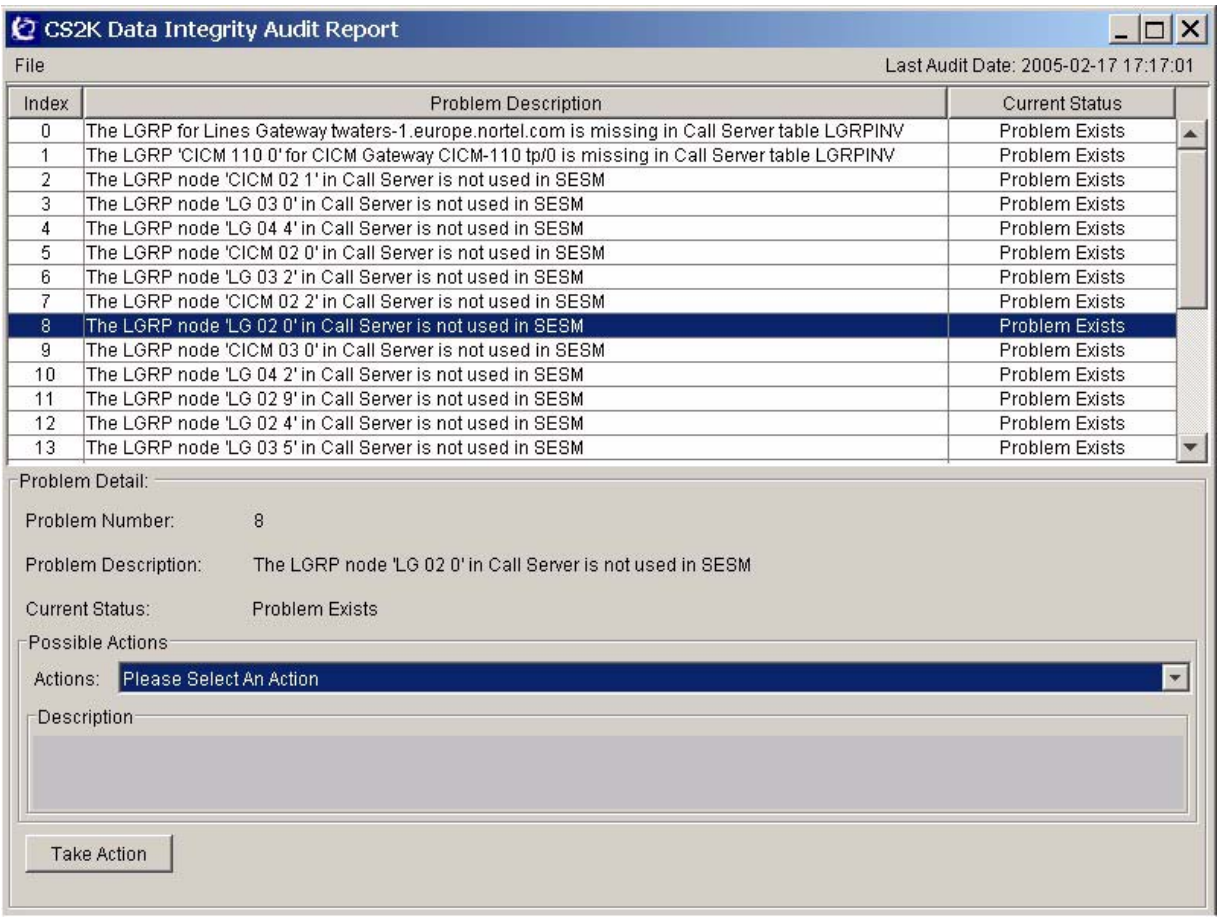
2.4.2.2.7 Context sensitive launching information

None.

2.4.2.2.8 Supplementary information

None.

2.4.2.3 GUI name: CS2K Data Integrity Audit Report



2.4.2.3.1 Functional description

This existing GUI displays problem reports for issues detected during the run of the audit. The functionality of the GUI is completely unchanged, however additional problem types will be detected by the “SIP Media Proxy Data Integrity Audit”. These new problem types will be displayed using the existing mechanism and appropriate Actions will be available via the Actions selector to correct the issues.

2.4.2.3.2 GUI usage and implications

Usage is unchanged.

2.4.2.3.3 GUI size

Table 5 New or modified GUIs

Abbreviated GUI name	Minimum instances	Maximum instances	Information on memory
CS2K Data Integrity Audit Report	0	1	No change

2.4.2.3.4 GUI fields

GUI fields are unchanged.

2.4.2.3.5 Usage example

Usage is unchanged.

2.4.2.3.6 GUI release history update

GUI unchanged but additional problem report types will be displayed.

2.4.2.3.7 Context sensitive launching information

None.

2.4.2.3.8 Supplementary information

None.

2.5 Configuration Walkthrough

Create a user or use an existing user for the Session Server(MCSEM) provisioning interface(OPI).

Use the CS2M configuration tool to configure the Session Server(MCSEM) connectivity information. See the MCSEM configuration that has been documented under activity A00008522.

If there are IP-VPN(NATs) provisioned already into the CS2M configuration manager, then perform an audit for the Session Server(MCSEM), to ensure the current data is synchronised.

Provision any new IP-VPN(NATs) or Distributed NATs into the CS2M Configuration Manager.

Make Configuration changes to existing gateways Or add new Gateways to the CS2K Configuration Manager to use the IP-VPN(NAT) information.

On the Session Server(MCSEM) provision the SIP Lines to use the routability groups that correspond to the Network Zones that were flowed through by the CS2M.

Calls between GWC controlled lines (IAD,H323,CICM) and MCS controlled SIP lines should now correctly insert Media Proxies when required.

Product = CS 2000 Management Tools

A00010617 -- Addition of NUERA_BTX4K and MGCP_IAD_40 Gateway certificates lines (corrective)

Excerpts from the Design Description

1: Applicable Solution(s)

IAW, IAC

1.1 Purpose

In SN09, the gateway certificate/profile "NUERA_BTX4K" is created in order to provision 4032 endpoints on TGCP large trunks gateways in SESM and support DS3 endpoint naming formats (e.g., "ds/ds3-<u1>/ds1-<u2>/[1-24]"). The certificate/profile is needed to support the Nuera BTX-4K gateway which allows 6 DS3s to be provisioned (4032 DS0s – 6x28x24). Up to now, the largest supported TGCP gateway was the Nuera BTX-21 which allowed at most 21 DS1s to be provisioned.

Additionally, the gateway certificate/profile "MGCP_IAD_40" is created in order to provision "Carrier Access Adit 600" MGCP small line gateways in SESM. The "Carrier Access Adit 600" gateway will support up to 40 endpoints (POTS lines).

1.2 Configuration

After the code changes, when associating a media gateway using SESM GUI, in the "Gateway Profile Name" pull down list, the following new profile names in addition to the existing profiles will show up as a selection choice.

- NUERA_BTX4K
- MGCP_IAD_40

The characteristics of the above gateways are listed in the following table.

GW Profile Name	GW Cate-gory	Signal Protocol	Protocol Version	Protocol Port	Service Type	Port/EP Capacity	GWC Profile No.

NUERA_BTX4K	Large	tgcp(6)	1.0	2427	Trunk	4032	60
MGCP_IAD_40	Small	MGCP(5)	1.0	2427	Line	40	49

When filling in the “Protocol Type”, “Protocol Version” and “Protocol Port” fields in the “Associate Gateway” dialog using SESM GUI, please enter in what’s specified in the above table.

When creating an OSSGATE input XML file for associating a “NUERA_BTX4K” or “MGCP_IAD_40” gateway, please reference the above table for values of the tags <mgProfileName>, <mgProtocolType>, <mgProtocolVersion>, and <mgProtocolPort>.

After the introduction of the NUERA_BTX4K certificate/profile, when adding a carrier using SESM GUI, in the “Add Carrier” dialog box, the following carrier name format can be specified in the “Carrier name:” field:

- ds/ds3-<u1>/ds1-<u2>

1.3 Related Documentation

N/A

Product = CS 2000 Management Tools

A00011746 --Addition of LGRP_TYPE field to GW profiles (Corrective)

Excerpts from the Design Description

1: Applicable Solution(s)

UA-IP

1.1 Purpose

In SN08 the ability to define a GWs profile by creating an XML document (referred to as a certificate) was introduced. The SN08 certificate included all of the flexible fields that were available in SN08 for the most part. However, the ability of the core to define profiles was also made available in SN08. This core field was not included in a 1 to 1 relationship with the certificate, but rather was coupled with certificate field Endpoint_Type. Because of the difficulties of updating profiles when this core field is updated, a new field is introduced for SN09 into the CMT certificates that will define the Lgrp Type

value that is sent to the core. Therefore, a direct relationship between core Lgrp types and a specific profile is made available by this enhancement.

1.2 Customer Facing Document Changes

A gateway certificate/profile captures a set of characteristics of a particular type of gateway. This set of characteristics can help us associate a gateway with the right type of gateway controller, manage the load balance of the gateway controller, and eventually achieve CallP purpose using the gateway.

This activity introduces a new optional field that is included in the profiles certificate. The LGRPType field is introduced and is used to drive “core” datafill for table LGRPINV. As suggested from the core table datafilled, LGRPINV, this field is only applicable for line gateways and is therefore optional in the XML document certificate. Even though this is an optional certificate field, this field is mandatory for all profiles that generate LGPRs.

In general, this field affects “core” behaviors applied to LGRPs. For a detailed discussion concerning core behavior driven by this field, refer to core NTP documentation.

1.2.1 SCHEMA UPDATES

Certificate.xsd

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

<xsd:include schemaLocation="../../xsd/certificateif/certificateTypes.xsd" />

<xsd:element name="certificate">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="MaxEndpoints"            type="maxEndpointsType"/>
      <xsd:element name="Category"                type="categoryType"/>
      <xsd:element name="EndpointType"            type="endpointTypeType"/>
      <xsd:element name="LgrpType"                type="lgrpType"
minOccurs="0"/>
      <xsd:element name="GenerateLGRP"            type="stringBoolean"/>
      <xsd:element name="MultiSiteNamesAllowed"   type="stringBoolean"
minOccurs="0"/>
      <xsd:element name="ResvTermMandatory"       type="stringBoolean"/>
      <xsd:element name="ChangeIPAvailable"       type="stringBoolean"/>
      <xsd:element name="DispPhyLocation"         type="stringBoolean"/>
      <xsd:element name="FQDNSupported"           type="fqdnSupportedType"
minOccurs="0" maxOccurs="1"/>
      <xsd:element name="InventoryType"           type="inventoryTypeType"/>
      <xsd:element name="InventoryRole"           type="inventoryRoleType"/>
```

```
      <xsd:element name="SupportedProtocol"       type="supportedProtocolType"/>
      <xsd:element name="GWCProfileNumber"        type="profileNumberType"/>
      <xsd:element name="EPIDGenDesc"             type="EPIDGenDescType"/>
      <xsd:element name="ServiceTypeList"         type="serviceTypeListType"
minOccurs="1" maxOccurs="7"/>
      <xsd:element name="CompatibleGWProfileList" type="profileNameType"
minOccurs="1" maxOccurs="5"/>
      <xsd:element name="BearerFabricList"        type="bearerFabricListType"
minOccurs="0" maxOccurs="5"/>
      <xsd:element name="GwAppData"               type="gwAppDataType"
minOccurs="0" maxOccurs="20"/>
      <xsd:element name="GatewayNameFormatList"   type="nameFormatsType"/>
      <xsd:element name="EndpointNameFormatList"  type="nameFormatsType"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

</xsd:schema>
```

CertificateTypes.xsd

```
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                  version="1.0"
                  xml:lang="en" >

<xsd:include schemaLocation="../../xsd/namesif/nameFormatsType.xsd" />

<xsd:simpleType name="profileNumberType">
  <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="1" />
    <xsd:maxInclusive value="599" />
  </xsd:restriction>
</xsd:simpleType>

.
.
.

<xsd:simpleType name="bearerFabricListType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="AAL1"/>
    <xsd:enumeration value="AAL2"/>
    <xsd:enumeration value="IP"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="lgrpType">
  <xsd:restriction base="xsd:token">
```

```
    <xsd:enumeration value="C"/>
    <xsd:enumeration value="S"/>
    <xsd:enumeration value="M"/>
    <xsd:enumeration value="SSDPL"/>
    <xsd:enumeration value="LL_3RDPTY"/>
    <xsd:enumeration value="CALIX_C7"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="fqdnSupportedType">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="true"/>
    <xsd:enumeration value="false"/>
    <xsd:enumeration value="trueWithDefaultDomain"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:complexType name="gwAppDataType">
  <xsd:attribute name="name"    type="xsd:token"  use="required" />
  <xsd:attribute name="values"  type="xsd:string" use="optional" />
  <xsd:attribute name="pattern" type="xsd:string" use="optional" />
</xsd:complexType>
```

1.3 Related Documentation

N/A

Product = Network Patch Manager

A00009227-- NPM Robustness

Functional Description

1: Applicable Solution(s)

PT-IP, UA-AAL1, UA-IP, IAW, IAC, PT-AAL2

1.1 Description

The NPM Robustness feature addresses areas for improvement in the Network Patch Manager. Following is a list of items that this feature will provide:

- A New log will be provided as part of the NPM Customer logs indicating whether a GWC image was successful or not.
- Six new system defined reports will be added to the NPM as a result of this feature:

- DEVICEINFO - lists the devices in the office, the date the devices registered, the loadname in the device and the date the load was discovered in the device.
- LASTAPPLYACTION - A list of the patch, device, status and description of why the apply attempt failed for this patch device relationship.
- PFRSSETTINGS - Lists the PFRS Dropbox, PFRS userid and status of if the delete patches is turned on.
- SYSTEMPLANSETTINGS - Lists all the system plans in the office along with the tasks, enable status, and schedule for each plan
- OFFICEINFOSETTINGS - Lists office information. Currently, only the GWC Auto imaging enabled setting is available in this report.
- GWCLOADIMAGEREPORT - Lists the imaged load, the patches contained in the load, the time the image was taken and a list of patches available in the office that are not contained in the image.

All of these reports will be included in the inform report that is generated via the PFRSGENREPORT task in the NPM.

- The NPM CLUI will be able to accept patchids in lower case, upper case or a combination of thereof; except for one command, q PATCH.
- The majority of the NPM CLUI commands will be changed to ensure command naming consistency for commands that provide similar types of functions.
- A new alarm will be raised on the Media Gateway 9000 GUI (MG9K EM) after applying or removing a “restart required” patch to any of the Media Gateway 9000 patchable cards.
- The “restart required” patch alarms at the MG9K EM will be lowered after restarts are performed on MG9K patchable cards.
- Logs and alarms for “restart required” patches will be provided during application or removal of the patches.

1.2 Hardware Requirements or Dependencies

None.

1.3 Software Requirements or Dependencies

None.

1.4 Limitations and restrictions

None.

1.5 Interactions

None.

1.6 Glossary

Term	Description
NPM	Network Patch Manager
CLUI	Command Line User Interface
GUI	Graphical User Interface
MG9K EM	Media Gateway 9000 Element Manager

2: Fault Management for A00009227

2.1 Fault management strategy

The standard MG9K EM Fault Management strategy will apply to the NPM Patch Alarm. The alarm will by displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

2.2 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

2.3 Logs and Alarms

There will be a single new patch alarm fault raised and cleared by the MG9000 to indicate when a restart is required for a patch on a specific card. The MG9000 will manage both raise and clear actions based on its own patching implementation.

2.3.1 Explanation

2.3.1.1 patchAlarmFault

Title: patchAlarmFault

Name: PATC

Description: This log is generated when a patchAlarmFault is received from an MG9000 DCC card.

Severity: MAJOR

Event Type: Trouble

2.3.2 Format

The Log Delivery application for this feature generates logs in the Number 2 Switch Control Center (SCC2) format and the NT standard (STD) format.

2.3.2.1 patchAlarmFault

PATC 301APR17 09:31:13 1806 TROUBLE MG9K nnPatchAlarm
Location: 8-co8-Frame000.Shelf2.Slot13
Notification Id: 952
State: not acknowledged
Category: Equipment Alarm
Cause: Equipment Malfunction
Time: Apr 17 09:31:13 2003
Component Id: Card.frame0.shelf2.slot11.OC3
Specific Problem: Patch Alarm - Patch(es) require a restart primary to instrument changes.
Patch ID: Patch N
Description: Patch(es) require a restart primary to instrument changes
Site Flr RPos Bay_id Cary 02 H02 MG9F 012

2.3.3 Field descriptions

2.3.3.1 Patch Alarm Fault

Table 1 Field descriptions PATC 300

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning

Table 1 Field descriptions PATC 300

Field	Value	Description
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=300.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. Threshold for this log.
patch id	String	Patch identification.
event id	String	The Log Title.
NE Number	integer	Number of the NE

Table 1 Field descriptions PATC 300

Field	Value	Description
NE Name	string	Name of the NE
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	warning
Description	string	Patch(es) require a restart primary to instrument changes

2.3.4 Action

PATC 301 - Restart primary to instrument changes.

2.3.5 Associated Operational Measurements or Performance Measurements

- None.

2.4 Related documentation

1. NORTEL-PATCHING-MIB - MG9000's Enterprise MIB, contains patching definitions

2. PLOA and SLOA Logs and Alarms for UE9kMG EM (DID) - MG9000s design documentation for logs and alarms on the MG9000 Element Manager.

3. Logs and Alarms Strategy for WUA Components - MG9000 Alarm strategy guide - version 1.4

3. Reliable Alarms and Alarm Robustness Design Intent Document (DID) - MG9000 Element Manager design document.

4. PLOA and SLOA Alarm Forwarding to OSS(DSUM) - MG9000 Alarm forwarding feature.

3: Configuration for A00009227

3.1 Hardware and Software Requirements

This feature requires an SN09 Network Patch Manager (NPM) and the SN09 SSPFS platform.

3.2 Network Patch Manager Server CLUI

3.2.1 CLUI Interface

The NPM CLUI has been modified to accept patchids and set names in lower case, upper case or a combination of thereof. In addition, several of the NPM CLUI commands have been changed to ensure command naming consistency for commands that provide similar types of functions. Below is a table that maps the old CLUI command to the new command.

Table 3:

Old Command	New Command
getassign	viewassign
ltabs	viewtabs or vtabs
qtask	viewtask or vt
qreps	viewreport all or vr all
qsets	viewset all or vs all
getplan	viewplan or vplan
alarminfo	viewalarm or va
display	viewpatch or vp
addalarm	newalarm or na
newset REPORT	newreport
newset SET	newset
alarm	enablealarm (for the enable portion) disablealarm (for the disable portion) delalarm (for the delete portion) alarmmatches (for the match portion)
sched	modifyplan
updplan	updsched
query	runreport or rr (for executing a report) runset or rs (for executing a set)
getversion	viewversion
getprop	viewprop

In addition a new command: alarmshow has been added. The complete syntax of the new command and well as the changed commands is shown below:

3.2.1.1 The ALARMSHOW Command

The NPM command **alarmshow** is used to toggle the display of alarms as they are raised or cleared. The following syntax is used:

npm 'alarmshow <ON/OFF>'

where:

npm	is the executable.
alarmshow	is the NPM command.
<ON|OFF>	is the switch to indicate whether to display alarms or not. ON indicates that as alarms are raised or cleared the message will be displayed at the CLUI. OFF indicates that the alarms will not be displayed.

3.2.1.2 The VIEWASSIGN Command

The NPM command **viewassign** is used to view the assign fields applicable for the assign command. The following syntax is used:

npm 'viewassign'

where:

npm	is the executable.
viewassign	is the NPM command.

3.2.1.3 The VIEWTABS Command

The NPM command **viewtabs** is used to list all reportable tables and field names. The following syntax is used:

npm 'viewtabs'

where:

npm	is the executable.
viewtabs	is the NPM command.

3.2.1.4 The VIEWTASK Command

The NPM command **viewtask** is used to display the specified task or all defined tasks. The following syntax is used:

npm 'viewtask <taskname | all>'

where:

npm	is the executable.
viewtask	is the NPM command.
<taskname>	is the name of a specific task to be displayed.
<for all>	will display all tasks.

3.2.1.5 The VIEWREPORT Command

The NPM command **viewreport** is used to display the specified report or all defined reports in the database. The following syntax is used:

npm 'viewreport <reportname | all>'

where:

npm	is the executable.
viewreport	is the NPM command.
<reportname>	is the name of a specific report to be displayed.
<for all>	will display all reports.

3.2.1.6 The VIEWSET Command

The NPM command **viewset** is used to view the specified set or all defined sets in the database. The following syntax is used:

npm 'viewset <setname | all>'

where:

npm	is the executable.
viewset	is the NPM command.
<setname>	is the name of a specific set to be displayed.
<for all>	will display all sets.

3.2.1.7 The VIEWPLAN Command

The NPM command **viewplan** is used to view the specified plan or all defined plans in the database. The following syntax is used:

npm 'viewplan <setname | all>'

where:

npm	is the executable.
viewplan	is the NPM command.
<setname>	is the name of a specific plan to be displayed.
<for all>	will display all plans.

3.2.1.8 The VIEWALARM Command

The NPM command **viewalarm** is used to view the specified alarm or all defined alarms in the database. The following syntax is used:

npm ‘viewalarm <setname | all>’

where:

npm	is the executable.
viewalarm	is the NPM command.
<setname>	is the name of a specific alarm to be displayed.
<for all>	will display all alarms.

3.2.1.9 The VIEWPATCH Command

The NPM command **viewpatch** is used to view the administrative information associated with a patch. The following syntax is used:

npm ‘viewpatch <patchid>’

where:

npm	is the executable.
viewpatch	is the NPM command.
<patchid>	is the patchid to be displayed.

3.2.1.10 The NEWALARM Command

The NPM command **newalarm** is used to define a new alarmable condition. The following syntax is used:

npm ‘newalarm <name> <enable> <alarm> <patchinfo> <“Desc”>’

where:

npm	is the executable.
newalarm	is the NPM command.
<name>	is the name of the alarm being defined.
<enable>	indicates whether to enable (Y) or disable (N) the alarm.
<alarm>	is the severity level of the alarm. Valid values are “NONE”, “MINOR”, “MAJOR”, or “CRITICAL”.
<patchinfo>	is SQL criteria that defines the alarm and should be in the form "PATCH|DEVICE where [criteria]".

<“Desc”>	is a brief description of the alarm.

3.2.1.11 The NEWREPORT Command

The NPM command **newreport** is used to create a report. The following syntax is used:

npm ‘newreport <reportname> <“Description”> <“field1... fieldn [where <Criteria>]”>’

where:

npm	is the executable.
newreport	is the NPM command.
<reportname>	is the name of the report to be created.
<“Description”>	is a short description of the report.
<field1...fieldn	is the name of one or more fields to be included in the report.
where	keyword starting SQL statement
<Criteria>	is the SQL statement that identifies the criteria by which to search the NPM database.

3.2.1.12 The NEWSET Command

The NPM command **newset** is used to create a set definition. The following syntax is used:

npm ‘newset <type> <setname> <“Description”> <[“where <Criteria>”]>’

where:

npm	is the executable.
newset	is the NPM command.
<type>	is either PATCHSET (to create a set that will evaluate patches) or DEVICESET (to create a set that will evaluate devices).
<setname>	is the name of the set to be created.
<“Description”>	is a short description of the report.
where	keyword starting SQL statement
<Criteria>	is the SQL statement that identifies the criteria by which to search the NPM database.

3.2.1.13 The ENABLEALARM Command

The NPM command **enablealarm** is used to enable the specified alarm. The following syntax is used:

npm 'enablealarm <alarmname>'

where:

npm	is the executable.
enablealarm	is the NPM command.
<alarmname>	is the name of the alarm.

3.2.1.14 The DISABLEALARM Command

The NPM command **disablealarm** is used to disable the specified alarm. The following syntax is used:

npm 'enablealarm <alarmname>'

where:

npm	is the executable.
disablealarm	is the NPM command.
<alarmname>	is the name of the alarm.

3.2.1.15 The DELALARM Command

The NPM command **delalarm** is used to delete the specified alarm. Only user created alarms can be deleted. The following syntax is used:

npm 'delalarm <alarmname>'

where:

npm	is the executable.
delalarm	is the NPM command.
<alarmname>	is the name of the alarm to be deleted.

3.2.1.16 The ALARMMATCHES Command

The NPM **alarmmatches** command is used to list either the patches or devices that caused the specified alarm to be raised. The following syntax is used:

npm 'alarmmatches <alarmname>'

where:

npm	is the executable.
alarmmatches	is the NPM command.
<alarmname>	is the name of the alarm.

3.2.1.17 The MODIFYPLAN Command

The NPM command **modifyplan** is used to modify the scheduled activities of a plan. The modifyplan command may be used to add a specified task or report to a plan or delete a specified task or report from a plan.

Note: The order in which tasks and reports are added to a plan determines the order in which their execution will be requested.

: The following syntax is used

npm 'modifyplan <plan name> <TASK|REPORT> <Task|Report name> <ADD|DELETE>'

where:

npm	is the executable.
modifyplan	is the NPM command.
<plan name>	is the name of the plan to be modified
<TASK|REPORT>	indicates whether the item being added to or deleted from the given plan is a task or a report.
<Task|Report name>	is the name of the task or report being added to or deleted from the given plan. Note: Prompted reports should not be added to plans. At execution time, prompted reports require a user to supply additional input. Plans run without a user being present and cannot provide the required information. The predefined prompted reports include: DEVICE, PATCH, PATCHES_SINCE, and PATCHINFO. Do not add any of these reports or any user defined prompted reports to any plans.
<ADD|DELTE>	indicates whether the specified task or report is to be added to or deleted from the given plan.

3.2.1.18 The UPDSCHED Command

The NPM command **updsched** is used to update the plan schedule in the database. The following syntax is used:

npm 'updsched <plan name> <freq> <Date Time> <MaxTime> <"Desc">'

where:

npm	is the executable.

updsched	is the NPM command.
<plan name>	is the name of the plan to be updated
<freq>	is how often the plan should execute. Valid values are “Once”, “Hourly”, “Daily”, “Weekly”, or “Monthly”.
<Date Time>	is the date and time plan is to be executed. Should be in “mm-dd-yy hh:mm” format.
<MaxTime>	is Maximum amount of time to execute plan defined as {No_Limit,15_min, 30_min, 1_Hr, 2_Hr, 4_Hr, 8_Hr, 16_Hr}.
<“Desc”>	is a brief description surrounded by quotes.

3.2.1.19 The RUNREPORT Command

The NPM command **runreport** is used to execute the specified report and display the results. The following syntax is used:

npm ‘runreport <reportname>’

where:

npm	is the executable.
runreport	is the NPM command. “rr”or “q” can be used as a shortcut for “runreport”.
<reportname>	is the name of the report to be executed.

3.2.1.20 The RUNSET Command

The NPM command **runrset** is used to execute the specified set and display the results. The following syntax is used:

npm ‘runset <setname>’

where:

npm	is the executable.
runset	is the NPM command. “rs” or “q” can be used as a shortcut for “runset”.
<setname>	is the name of the set to be executed.

3.2.1.21 The VIEWVERSION Command

The NPM command **viewversion** is used to view the version of the NPM software and database components. The following syntax is used:

npm ‘viewversion’

where:

npm	is the executable.
viewversion	is the NPM command.

3.2.1.22 The VIEWPROP Option

The NPM option **viewprop** is used to list the property value for a specified key or all keys. The following syntax is used:

npm ‘getprop <property_type>’

where:

npm	is the executable.
getprop	is the NPM option.
<property_type>	can be a specific key, or “all” to display all keys.

3.3 Network Patch Manager Reports

Six new system defined reports will be added to the NPM as a result of this feature. NPM CLUI examples follow of the reports to show what fields are in each report.

- DEVICEINFO - lists the devices in the office, the date the devices registered, the loadname in the device and the date the load was discovered in the device.

```
npm>q DEVICEINFO
deviceid,registered,hold,devicebornon,loadname,loaddiscoveredon
NC0S8_1_OC3_0_1_10,TRUE,FALSE,2005-03-17 12:05:12.397,SCOA09AH,2005-03-17 12:
05:57.994
NC0S8_1_OC3_0_1_11,TRUE,FALSE,2005-03-17 12:05:12.417,mdw,2005-03-17 12:05:59.804
NC0S8_1_ITP_0_1_12,TRUE,FALSE,2005-03-17 12:05:12.442,ITPA09AF,2005-03-17 12:
06:00.782
MG9KSERVER_09_wnc0s0mh,TRUE,FALSE,2005-03-17 12:04:20.897,NTMG9KS_9_11_0,2005
```

- LASTAPPLYACTION - A list of the patch, device, status and description of why the apply attempt failed for this patch device relationship.

```
npm>q LASTAPPLYACTION
patchid,deviceid,status,lastactionresults
```

- PFRSSETTINGS - Lists the PFRS Dropbox, PFRS userid and status of if the delete patches is turned on.

```
npm>q PFRSSETTINGS
ftpAddress,ftpUserid,deletePatches
wnc0s0kf,FIELD,FALSE
```

- SYSTEMPLANSETTINGS - Lists all the system plans in the office along with the tasks, enable status, and schedule for each plan.

```
npm>q SYSTEMPLANSETTINGS
name,enabled,status,frequency,extime,maxtime,description,tasks,systemDefined
SYSTEMPLAN,N,IDLE,Daily,2004-01-01 00:00:00.000,No_Limit,NPM System scheduled
 routine activities,[TASK:AUTOAPPLY, TASK:AUTORESTART],TRUE
REPORTCLEANUP,N,IDLE,Daily,2004-01-01 00:00:00.000,No_Limit,Delete reports as
sociated with NPM Plans,[TASK:DELETEREPORTS],TRUE
GETPATCH,N,IDLE,Daily,2004-01-01 23:00:00.000,No_Limit,Patch file retrieval,[
TASK:PFRSGETPATCH],TRUE
GENREPORT,N,IDLE,Daily,2004-01-01 10:00:00.000,No_Limit,PFRS Inform list repo
rt generation,[TASK:PFRSGENREPORT],TRUE
FILEAUDIT,Y,IDLE,Daily,2005-03-18 05:00:00.000,No_Limit,File Audit,[TASK:FILE
AUDIT],TRUE
```

- OFFICEINFOSETTINGS - Lists office information. Currently, only the GWC Auto imaging enabled setting is available in this report.

```
npm>q OFFICEINFO
gwcautoimage
Y
```

- GWCLOADIMAGEREPORT - Lists the imaged load, the patches contained in the load, the time the image was taken and a list of patches available in the office that are not contained in the image.

```
npm>q GWCLOADIMAGEREPORT
loadname,imagedtime,imagedpatchlist,missingpatches
GN090AP,2005-03-17 12:15:31.316,[None],[GWC01GAP, GWC02GAP]
```

All of these reports will be included in the inform report that is generated via the PFRSGENREPORT task in the NPM. The following is an example inform report.

```
#  Thu Mar 17 18:39:28 GMT 2005
#  Server:  znc0s0ky.us.nortel.com
#  Address:  47.142.16.120
#
#  Name:    wnc0s0kf.us.nortel.com
#  Address:  47.142.117.20
#
#  CLLI=RLGHNCPRSM8
patchid,apptime,deviceid,category,autoapp,spapp,restarttype,status,processor,fil
eavailable
GWC01GAP,,GWC-1-UNIT-0,GEN,TRUE,FALSE,NONE,VA,GWC,TRUE
GWC01GAP,,GWC-0-UNIT-0,GEN,TRUE,FALSE,NONE,R,GWC,TRUE
GWC02GAP,,GWC-0-UNIT-0,GEN,TRUE,FALSE,NONE,R,GWC,TRUE
GWC02GAP,,GWC-1-UNIT-0,GEN,TRUE,FALSE,NONE,VA,GWC,TRUE
SC001UAH,2005-03-17 12:05:59.258,NC0S8_1_OC3_0_1_10,GEN,TRUE,FALSE,NONE,A,MG9K,T
RUE
SC002UAH,2005-03-17 12:05:59.368,NC0S8_1_OC3_0_1_10,GEN,TRUE,FALSE,NONE,A,MG9K,T
RUE
ABC01U09,2005-03-17 12:06:00.411,NC0S8_1_OC3_0_1_11,,,FALSE,,A,MG9K,FALSE
ABC02U09,2005-03-17 12:06:00.488,NC0S8_1_OC3_0_1_11,,,FALSE,,A,MG9K,FALSE
ITP01UAF,2005-03-17 12:06:01.782,NC0S8_1_ITP_0_1_12,GEN,TRUE,FALSE,NONE,A,MG9K,T
RUE
ITP02UAF,2005-03-17 12:06:01.918,NC0S8_1_ITP_0_1_12,GEN,TRUE,FALSE,NONE,A,MG9K,T
RUE
EPM00O09,2005-03-17 12:07:04.516,SESM_wnc0s0kf-unit0,GEN,TRUE,FALSE,NONE,A,OAM,T
RUE
NPM00O09,2005-03-17 13:18:44.636,NPM_wnc0s0kf-unit0,GEN,TRUE,FALSE,NONE,A,OAM,TR
UE
loadname,deviceid
SCOA09AH,NC0S8_1_OC3_0_1_10
mdw,NC0S8_1_OC3_0_1_11
ITPA09AF,NC0S8_1_ITP_0_1_12
NTMG9KS_9_11_0,MG9KSERVER_09_wnc0s0mh
NTPSE_9_034_0,PSE_wnc0s0kf-unit0
ITPA09AH,NC0S8_1_ITP_0_1_13
ITXA09AF,NC0S8_1_ITX_0_1_14
ITXA09AF,NC0S8_1_ITX_0_1_15
DS1G09AH,NC0S8_1_DS1_0_1_2
ABIG09AF,NC0S8_1_ABI_0_1_18
ABIG09AF,NC0S8_1_ABI_0_1_19
UNKNOWN,GWC-2-UNIT-1
GN090AP,GWC-1-UNIT-0
UNKNOWN,GWC-1-UNIT-1
patchid,deviceid,actstatus,acttime

# GWCLOADIMAGEREPORT
loadname,imagedtime,imagedpatchlist,missingpatches
GN090AP,2005-03-17 12:15:31.316,[None],[GWC01GAP, GWC02GAP]

# PFRSSETTINGS
ftpAddress,ftpUserid,deletePatches
wnc0s0kf,FIELD,FALSE
```

```
# SYSTEMPLANSETTINGS
name,enabled,status,frequency,extime,maxtime,description,tasks,systemDefined
SYSTEMPLAN,N,IDLE,Daily,2004-01-01 00:00:00.000,No_Limit,NPM System scheduled
ro
utine activities,[TASK:AUTOAPPLY, TASK:AUTORESTART],TRUE
REPORTCLEANUP,N,IDLE,Daily,2004-01-01 00:00:00.000,No_Limit,Delete reports
assoc
iated with NPM Plans,[TASK:DELETEREPORTS],TRUE
GETPATCH,N,IDLE,Daily,2004-01-01 23:00:00.000,No_Limit,Patch file
retrieval,[TAS
K:PFRSGETPATCH],TRUE
GENREPORT,N,IDLE,Daily,2004-01-01 10:00:00.000,No_Limit,PFRS Inform list report
generation,[TASK:PFRSGENREPORT],TRUE
FILEAUDIT,Y,IDLE,Daily,2005-03-18 05:00:00.000,No_Limit,File
Audit,[TASK:FILEAUD
IT],TRUE

# OFFICEINFO
gwcautoimage
Could not obtain the autoimaging status boolean from the GWC Element Manager.

# LASTAPPLYACTION
patchid,deviceid,status,lastactionresults

# DEVICEINFO
deviceid,registered,hold,devicebornon,loadname,loaddiscoveredon
NC0S8_1_OC3_0_1_10,TRUE,FALSE,2005-03-17 12:05:12.397,SCOA09AH,2005-03-17
12:05:
57.994
NC0S8_1_OC3_0_1_11,TRUE,FALSE,2005-03-17 12:05:12.417,mdw,2005-03-17
12:05:59.80
4
NC0S8_1_ITP_0_1_12,TRUE,FALSE,2005-03-17 12:05:12.442,ITPA09AF,2005-03-17
12:06:
00.782
MG9KSERVER_09_wnc0s0mh,TRUE,FALSE,2005-03-17
12:04:20.897,NTMG9KS_9_11_0,2005-03
-17 12:07:00.384
PSE_wnc0s0kf-unit0,TRUE,FALSE,2005-03-17 12:04:19.763,NTPSE_9_034_0,2005-03-17
1
2:07:09.089
NC0S8_1_ITP_0_1_13,TRUE,FALSE,2005-03-17 12:05:12.466,ITPA09AH,2005-03-17
12:06:
02.228
NC0S8_1_ITX_0_1_14,TRUE,FALSE,2005-03-17 12:05:12.486,ITXA09AF,2005-03-17
12:06:
03.093
NC0S8_1_ITX_0_1_15,TRUE,FALSE,2005-03-17 12:05:12.524,ITXA09AF,2005-03-17
12:06:
04.217
NC0S8_1_DS1_0_1_2,TRUE,FALSE,2005-03-17 12:05:12.543,DS1G09AH,2005-03-17
12:06:0
5.397
NC0S8_1_ABI_0_1_18,TRUE,FALSE,2005-03-17 12:05:12.563,ABIG09AF,2005-03-17
12:06:
```

Product = CS 2000 TOPS

A00009011 -- Traffic Operator Position System (TOPS) Internet Protocol (IP) Security Enhancements

Functional Description

1: Applicable Solution(s)

PT-AAL1, PT-IP, DMS

1.1 Description

This feature allows the customer to increase the security of the IP eXtended Peripheral Modules (IP-XPMs) in their TOPS-IP network. This feature introduces Succession core datafill which allows the customer to configure the following functions on the IP-XPM:

- Simple Network Management Protocol (SNMP): The customer can enable or disable SNMP, define an SNMP community name, and define an SNMP manager.
- Telnet: The customer can enable or disable Telnet.

These changes are discussed in more detail in the following sections.

1.1.1 Background

The implementation of TOPS-IP is based on the IP-XPM. The IP-XPM is a specialized Digital Trunk Controller (DTC) containing Ethernet-enabled SX05DA processor cards as well as 7X07AA Voice over IP (VoIP) gateway cards. The SX05DA and the 7X07AA each contain processor cards which can support various Internet applications including Ping, SNMP, Telnet, and more.

Nortel recommends that TOPS-IP be implemented on a secure network, not the public internet. A secure network contains subnets, firewalls, and routers which block unauthorized attempts to connect to a TOPS-IP node.

Security risks exist even if an IP-XPM resides on a secure network. For example, a malicious user could attempt to alter IP-XPM settings using SNMP. Another risk might be a user logging on to a 7X07AA card while the card is under heavy load. This action might cause the card to crash and calls to be lost.

This feature improves TOPS-IP security in the areas of SNMP and Telnet as described in the next sections.

1.1.2 SNMP

SNMP allows IP hosts to monitor, modify behavior, and receive unsolicited management information from other IP hosts. The monitoring host is termed the SNMP manager and the monitored host is termed the SNMP element. SNMP is described in several RFCs as follows:

- Version 1 (SNMPv1): RFCs 1155, 1157, 1212
- Version 2 (SNMPv2): RFCs 1441-1452, 1901-1910
- Version 3 (SNMPv3): RFCs 2271-2275

This feature proposes adding three new SNMP settings for TOPS-IP. The new SNMP settings are:

- **SNMP community name:** A character string which serves as a password when reading from or writing to an SNMP host.[1] This feature allows datafill of one community name up to 16 characters in length. The community name is used for reading and writing SNMP data. It is also used when the IP-XPM sends traps (unsolicited SNMP information) to an SNMP manager.

  This feature allows the community name to be set to some other value than "public." This increases security since hackers must guess the community name (through repeated attempts) or break into the secure network in order to use a sniffer to detect the SNMP community name.

  Many IP hosts allow configuration of different community names for SNMP reads, writes, and traps. For example, many users might need read access to a device while only a few need write access, so separate read and write names are defined. For TOPS-IP, SNMP support is limited, and it is not anticipated that many users will need access to SX05DAs and 7X07AAs. As a result only one community name can be defined.
- **SNMP manager:** An IP address specifying a remote host which is allowed to initiate SNMP requests to the IP-XPM. The SNMP manager is also called the trap manager, since it is the host to whom traps are reported. Allowing specification of an SNMP manager by IP address increases security, since the IP-XPM will reject SNMP write attempts from unauthorized remote hosts.
- **SNMP enable/disable:** A Y/N parameter indicating whether the IP-XPM supports any incoming SNMP requests, or sends out any traps.

The SX05DA and the 7X07AA support these settings as follows.

[1] In SNMP parlance, a read is a "get" and a write is a "set."

1.1.2.1 SNMP settings on SX05DA

The SX05DA supports limited SNMP capabilities, as detailed in "2. Appendix A: Supported SNMP objects on IP-XPM (SX05DA)" on page 2027. The new SNMP settings apply to the SX05DA as follows.

- **SNMP community name:** The datafilled community name is validated for incoming read and write requests. The name is not sent in trap messages because the SX05DA does not send traps.
- **SNMP manager:** The SX05DA does not perform originating IP address validation when an SNMP write request is received. So there is no datafill for the SX05DA SNMP manager.
- **SNMP enable/disable:** By setting this parameter to N, the SX05DA will ignore all incoming SNMP requests. This parameter does not affect traps since the SX05DA does not send traps.

The SNMP community name and the SNMP enable/disable parameter are added as new fields in the tuples of existing Table XPMIPMAP. Table XPMIPMAP is used to configure the SX05DA cards on the IP-XPMs. Each tuple represents one IP-XPM. See the Configuration chapter of this document for the new field definitions.

The SNMP settings are datafilled in the Succession core, but the new settings do not take effect until the data is downloaded to the IP-XPM. The craftsperson must perform a LoadPM or Bsy/RTS on each unit to download the SNMP settings.

Dump and restore: Because SNMP is present on deployed IP-XPMs, the new fields are restored as follows when upgrading from an older TOPS Succession core load.

- **SNMP community name:** Restores as "public," the default SNMP community name. "public" is also the name in use on currently deployed IP-XPMs.
- **SNMP enable/disable:** Restores to Y (SNMP enabled) since SNMP is enabled on currently deployed IP-XPMs.

1.1.2.2 SNMP settings on 7X07AA

The new SNMP settings apply to the 7X07AA as follows. These new settings apply only to TOPS 7X07AAs datafilled in existing Table IPINV (field `GW_TYPE` is set to `TOPS`).

- **SNMP community name:** The datafilled community name is validated for incoming read and write requests. The datafilled community name is also sent in trap messages.
- **SNMP manager:** Currently, up to 4 SNMP managers can be configured on a 7X07AA card. One is obtained via DHCP and up to three more can be

configured using PMDEBUG on each card. This feature allows a fifth SNMP manager to be configured in the Succession core. When SNMP write requests arrive, the 7X07AA ensures the originating IP address is present in the allowed SNMP manager list. If not, the 7X07AA rejects the write operation.

- **SNMP enable/disable:** By setting this parameter to N, the 7X07AA will ignore all incoming SNMP requests and will not send any traps.

The new settings are added as individual office parameters in Table OFCENG. The default values are "public," no manager, and SNMP disabled, respectively. Each office parameter applies to all 7X07AAs in the office. See the Configuration chapter of this document for the new office parameter definitions.

The SNMP settings are datafilled in the Succession core, but the new settings do not take effect until the data is downloaded to the 7X07AA. The craftsperson must perform a PMRESET on each 7X07AA to download the SNMP settings.

Dump and restore: Because SNMP is present on deployed 7X07AAs, the new fields are restored as follows when upgrading from an older TOPS Succession core load with TOPS 7X07AAs present in Table IPINV.

- **SNMP community name:** Restores as "public," the default SNMP community name. "public" is also the name in use on currently deployed 7X07AAs.
- **SNMP manager:** Restores as N (no manager) since the 7X07AA currently has other methods of setting SNMP manager IP addresses.
- **SNMP enable/disable:** Restores to Y (SNMP enabled) since SNMP is enabled on currently deployed 7X07AAs.

If no TOPS 7X07AAs are present on the dump side, the parameters are set to their default values on the restore side.

1.1.3 Telnet (7X07AA only)

Telnet is a standard TCP-based service which allows a user to log on to a remote host and access the command line. Telnet is supported on the 7X07AA but not the SX05DA. Telnet is not recommended on a 7X07AA which is handling calls, since the use of Telnet or the use of CPU-intensive 7X07AA commands within a Telnet session can cause the card to crash, thus producing an outage.

Since Telnet is risky to use on an active 7X07AA, this feature allows Telnet to be disabled. This is done using a new office parameter in Table OFCENG. The parameter defaults to N meaning Telnet is disabled. See the Configuration chapter of this document for the new office parameter definition.

The new setting applies only to 7X07AAs datafilled for TOPS usage in existing Table IPINV (field GW_TYPE is set to TOPS).

The Telnet setting is datafilled in the Succession core, but the setting does not take effect until the data is downloaded to the 7X07AA. The craftsperson must perform a PMRESET on each 7X07AA to download the Telnet setting.

Dump and restore: Telnet is present and enabled on deployed 7X07AAs. But since it is such a risk, the new office parameter will restore to N (Telnet disabled) even if the TOPS-IP office has 7X07AAs defined in Table IPINV on the dump side. This is because it is likely that craftspersons do not use Telnet on a 7X07AA except for commissioning and debugging, and at other times Telnet presents the opportunity for an authorized craftsperson to cause an outage inadvertently.

1.2 Hardware Requirements or Dependencies

This feature does not introduce any new hardware requirements or dependencies.

1.3 Software Requirements or Dependencies

This feature requires new loads in the IP-XPM and in the NT7X07AA. These loads interpret and act on the SNMP and Telnet configuration data downloaded from the CM. The applicable loads are as follows:

- IP-XPM (SX05DA): TBD
- 7X07AA: TBD

1.4 Limitations and restrictions

1.4.1 IP-XPM (SX05DA) restrictions

The following existing IP-XPM restrictions are not changed by this feature.

- The SX05DA supports SNMPv1 and SNMPv2c only. The SX05DA does not support SNMPv2 or SNMPv3.
- The SX05DA does not validate the originating IP address of incoming SNMP write requests.
- The SX05DA does not send SNMP traps.
- The SNMP object values are not retained over a restart of the IP-XPM.
- The SX05DA does not support Telnet.

1.4.2 NT7X07AA restrictions

- The new parameters in Table OFCENG only have an effect on 7X07AA cards which are datafilled as TOPS cards in Table IPINV (field GW_TYPE is set to TOPS).

- The 7X07AA supports SNMPv1 and SNMPv2c only. The 7X07AA does not support SNMPv2 or SNMPv3. Please refer to the TOPS-IP User's Guide for further information concerning support of SNMP on the 7X07AA.

1.5 Interactions

Not applicable.

1.6 Glossary

Term	Description
7X07AA	VoIP cards which sit in an IP-XPM and act as a gateway between pulse code modulation (PCM) voice and packetized voice (VoIP)
Bsy	Busy, a maintenance command executed on DMS agents and peripherals
DHCP	Dynamic Host Configuration Protocol, an RFC2131-based method of configuring Internet hosts
DMS	Digital Multiplex System, the central Nortel switching processor
DTC	Digital Trunk Controller, an XPM for digital voice
IP-XPM	Internet Protocol eXtended Peripheral Module, a DTC-based XPM with Ethernet capability which provides the basis for TOPS-IP
LoadPM	Load Peripheral Module, a maintenance command executed on DMS peripherals
PMReset	Peripheral Module Reset, a maintenance command executed on DMS peripherals
RFC	Request For Comments, the standard method of documenting Internet applications
RTS	Return to Service, a maintenance command executed on DMS agents and peripherals
SNMP	Simple Network Management Protocol, described in "1.1.2 SNMP" on page 2022
Succession core	An updated name for the DMS reflecting the addition of geographically diverse IP hosts serving a central processor (the core)
SX05DA	The processor card for the IP-XPM. Each unit of the IP-XPM has an SX05DA.

Term	Description
Telnet	A TCP-based tool for logging on to and executing commands on remote hosts
TOPS	Traffic Operator Position System, a system for providing operator services using operators and automation
VoIP	Voice over Internet Protocol, a method of sending voice over a packetized network
XPM	eXtended Peripheral Module, a device with its own processor sitting off the Succession core but providing essential services for the core

2. Appendix A: Supported SNMP objects on IP-XPM (SX05DA)

This section describes supported SNMP objects on the SX05DA.[2] The SX05DA supports Management Information Base II (MIB-II) as defined in RFC1213. The SX05DA also supports the User Security (USEC) basic group and USEC statistics from RFC1910 (User-based Security Model for SNMPv2).

The following two tables list SNMP objects supported by the SX05DA. MIB-II objects begin with the designation **iso.org.dod.internet.mgmt.mib-2** (numeric **1.3.6.1.2.1**). SNMPv2 objects begin with the designation **iso.org.dod.internet.snmpv2** (numeric **1.3.6.1.6**).

For definitions of these objects, refer to RFC1213 and RFC1910.

Read-write objects are check-marked in the R/W column. If there is no check mark, the object is read-only.

Restrictions apply as listed in section “1.4.1 IP-XPM (SX05DA) restrictions” on page 2025.

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
system.sysDescr	1.1		
system.sysObjectID	1.2		
system.sysUpTime	1.3		
system.sysContact	1.4	✓	

[2] Supported SNMP objects on the 7X07AA are already defined in the TOPS-IP User’s Guide.

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
system.sysName	1.5	✓	
system.sysLocation	1.6	✓	
system.sysServices	1.7		
interfaces.ifNumber	2.1		
interfaces.ifTable.ifEntry.ifIndex	2.2.1.1		
interfaces.ifTable.ifEntry.ifDescr	2.2.1.2		
interfaces.ifTable.ifEntry.ifType	2.2.1.3		
interfaces.ifTable.ifEntry.ifMtu	2.2.1.4		
interfaces.ifTable.ifEntry.ifSpeed	2.2.1.5		
interfaces.ifTable.ifEntry.ifPhysAddress	2.2.1.6		
interfaces.ifTable.ifEntry.ifAdminStatus	2.2.1.7	✓	
interfaces.ifTable.ifEntry.ifOperStatus	2.2.1.8		
interfaces.ifTable.ifEntry.ifLastChange	2.2.1.9		
interfaces.ifTable.ifEntry.ifInOctets	2.2.1.10		
interfaces.ifTable.ifEntry.ifInUcastPkts	2.2.1.11		
interfaces.ifTable.ifEntry.ifInNUcastPkts	2.2.1.12		
interfaces.ifTable.ifEntry.ifInDiscards	2.2.1.13		
interfaces.ifTable.ifEntry.ifInErrors	2.2.1.14		
interfaces.ifTable.ifEntry.ifInUnknownPro-tos	2.2.1.15		
interfaces.ifTable.ifEntry.ifOutOctets	2.2.1.16		
interfaces.ifTable.ifEntry.ifOutUcastPkts	2.2.1.17		
interfaces.ifTable.ifEntry.ifOutNUcastPkts	2.2.1.18		
interfaces.ifTable.ifEntry.ifOutDiscards	2.2.1.19		
interfaces.ifTable.ifEntry.ifOutErrors	2.2.1.20		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
interfaces.ifTable.ifEntry.ifOutQLen	2.2.1.21		
interfaces.ifTable.ifEntry.ifSpecific	2.2.1.22		
at.atTable.atEntry.atIfIndex	3.1.1.1	✓	
at.atTable.atEntry.atPhysAddress	3.1.1.2	✓	
at.atTable.atEntry.atNetAddress	3.1.1.3	✓	
ip.ipForwarding	4.1	✓	
ip.ipDefaultTTL	4.2	✓	
ip.ipInReceives	4.3		
ip.ipInHdrErrors	4.4		
ip.ipInAddrErrors	4.5		
ip.ipForwDatagrams	4.6		
ip.ipInUnknownProtos	4.7		
ip.ipInDiscards	4.8		Always 0
ip.ipInDelivers	4.9		
ip.ipOutRequests	4.10		
ip.ipOutDiscards	4.11		Always 0
ip.ipOutNoRoutes	4.12		
ip.ipReasmTimeout	4.13		
ip.ipReasmReqds	4.14		
ip.ipReasmOKs	4.15		
ip.ipReasmFails	4.16		
ip.ipFragOKs	4.17		
ip.ipFragFails	4.18		
ip.ipFragCreates	4.19		
ip.ipAddrTable.ipAddrEntry.ipAdEntAddr	4.20.1.1		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
ip.ipAddrTable.ipAddrEntry.ipAdEntIfIndex	4.20.1.2		
ip.ipAddrTable.ipAddrEntry.ipAdEntNetMask	4.20.1.3		
ip.ipAddrTable.ipAddrEntry.ipAdEntBcastAddr	4.20.1.4		
ip.ipAddrTable.ipAddrEntry.ipAdEntReasmMaxSize	4.20.1.5		
ip.ipRouteTable.ipRouteEntry.ipRouteDest	4.21.1.1	✓	
ip.ipRouteTable.ipRouteEntry.ipRouteIfIndex	4.21.1.2	✓	
ip.ipRouteTable.ipRouteEntry.ipRouteMetric1	4.21.1.3	✓	
ip.ipRouteTable.ipRouteEntry.ipRouteMetric2	4.21.1.4	✓	Not used
ip.ipRouteTable.ipRouteEntry.ipRouteMetric3	4.21.1.5	✓	Not used
ip.ipRouteTable.ipRouteEntry.ipRouteMetric4	4.21.1.6	✓	Not used
ip.ipRouteTable.ipRouteEntry.ipRouteNextHop	4.21.1.7	✓	
ip.ipRouteTable.ipRouteEntry.ipRouteType	4.21.1.8	✓	
ip.ipRouteTable.ipRouteEntry.ipRouteProto	4.21.1.9		
ip.ipRouteTable.ipRouteEntry.ipRouteAge	4.21.1.10	✓	
ip.ipRouteTable.ipRouteEntry.ipRouteMask	4.21.1.11	✓	
ip.ipRouteTable.ipRouteEntry.ipRouteMetric5	4.21.1.12	✓	Not used
ip.ipRouteTable.ipRouteEntry.ipRouteInfo	4.21.1.13		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaIfIndex	4.22.1.1	✓	
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaPhysAddress	4.22.1.2	✓	
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaNetAddress	4.22.1.3	✓	
ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaType	4.22.1.4	✓	
ip.ipRoutingDiscards	4.23		Always 0
icmp.icmpInMsgs	5.1		
icmp.icmpInErrors	5.2		
icmp.icmpInDestUnreachs	5.3		
icmp.icmpInTimeExcds	5.4		
icmp.icmpInParmProbs	5.5		
icmp.icmpInSrcQuenchs	5.6		
icmp.icmpInRedirects	5.7		
icmp.icmpInEchos	5.8		
icmp.icmpInEchoReps	5.9		
icmp.icmpInTimestamps	5.10		
icmp.icmpInTimestampReps	5.11		
icmp.icmpInAddrMasks	5.12		
icmp.icmpInAddrMaskReps	5.13		
icmp.icmpOutMsgs	5.14		
icmp.icmpOutErrors	5.15		
icmp.icmpOutDestUnreachs	5.16		
icmp.icmpOutTimeExcds	5.17		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
icmp.icmpOutParmProbs	5.18		
icmp.icmpOutSrcQuenchs	5.19		
icmp.icmpOutRedirects	5.20		
icmp.icmpOutEchos	5.21		
icmp.icmpOutEchoReps	5.22		
icmp.icmpOutTimestamps	5.23		
icmp.icmpOutTimestampReps	5.24		
icmp.icmpOutAddrMasks	5.25		
icmp.icmpOutAddrMaskReps	5.26		
tcp.tcpRtoAlgorithm	6.1		
tcp.tcpRtoMin	6.2		
tcp.tcpRtoMax	6.3		
tcp.tcpMaxConn	6.4		
tcp.tcpActiveOpens	6.5		
tcp.tcpPassiveOpens	6.6		
tcp.tcpAttemptFails	6.7		
tcp.tcpEstabResets	6.8		
tcp.tcpCurrEstab	6.9		
tcp.tcpInSegs	6.10		
tcp.tcpOutSegs	6.11		
tcp.tcpRetransSegs	6.12		
tcp.tcpConnTable.tcpConnEntry.tcp-ConnState	6.13.1.1	✓	
tcp.tcpConnTable.tcpConnEntry.tcp-ConnLocalAddress	6.13.1.2		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
tcp.tcpConnTable.tcpConnEntry.tcp-ConnLocalPort	6.13.1.3		
tcp.tcpConnTable.tcpConnEntry.tcpCon-nRemAddress	6.13.1.4		
tcp.tcpConnTable.tcpConnEntry.tcpCon-nRemPort	6.13.1.5		
tcp.tcpInErrs	6.14		
tcp.tcpOutRsts	6.15		
udp.udpInDatagrams	7.1		
udp.udpNoPorts	7.2		
udp.udpInErrors	7.3		
udp.udpOutDatagrams	7.4		
udp.udpTable.udpEntry.udpLocalAddress	7.5.1.1		
udp.udpTable.udpEntry.udpLocalPort	7.5.1.2		
transmis-sion.dot3.dot3StatsTable.dot3StatsEntry.dot 3StatsIndex	10.7.2.1.1		
transmis-sion.dot3.dot3StatsTable.dot3StatsEntry.dot 3StatsAlignmentErrors	10.7.2.1.2		
transmis-sion.dot3.dot3StatsTable.dot3StatsEntry.dot 3StatsFCSErrors	10.7.2.1.3		
transmis-sion.dot3.dot3StatsTable.dot3StatsEntry.dot 3StatsSingleCollisionFrames	10.7.2.1.4		
transmis-sion.dot3.dot3StatsTable.dot3StatsEntry.dot 3StatsMultipleCollisionFrames	10.7.2.1.5		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsSQETestErrors	10.7.2.1.6		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsDeferredTransmissions	10.7.2.1.7		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsLateCollisions	10.7.2.1.8		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsExcessiveCollisions	10.7.2.1.9		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsInternalMacTransmitErrors	10.7.2.1.10		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsCarrierSenseErrors	10.7.2.1.11		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsFrameTooLongs	10.7.2.1.13		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsInternalMacReceiveErrors	10.7.2.1.16		
transmission.dot3.dot3StatsTable.dot3StatsEntry.dot3StatsEtherChipSet	10.7.2.1.17		
transmission.rs232.rs232Number	10.33.1		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortIndex	10.33.2.1.1		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortType	10.33.2.1.2		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortInSigNumber	10.33.2.1.3		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortOutSigNumber	10.33.2.1.4		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortInSpeed	10.33.2.1.5		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortOutSpeed	10.33.2.1.6		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortInFlowType	10.33.2.1.7		
transmission.rs232.rs232PortTable.rs232PortEntry.rs232PortOutFlowType	10.33.2.1.8		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortIndex	10.33.3.1.1		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortBits	10.33.3.1.2		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortStopBits	10.33.3.1.3		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortParity	10.33.3.1.4		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortAutobaud	10.33.3.1.5		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortParityErrs	10.33.3.1.6		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortFramingErrs	10.33.3.1.7		
transmission.rs232.rs232AsyncPortTable.rs232AsyncPortEntry.rs232AsyncPortOverrunErrs	10.33.3.1.8		
transmission.rs232.rs232InSigTable.rs232InSigEntry.rs232InSigPortIndex	10.33.5.1.1		
transmission.rs232.rs232InSigTable.rs232InSigEntry.rs232InSigName	10.33.5.1.2		
transmission.rs232.rs232InSigTable.rs232InSigEntry.rs232InSigState	10.33.5.1.3		
transmission.rs232.rs232InSigTable.rs232InSigEntry.rs232InSigChanges	10.33.5.1.4		
transmission.rs232.rs232OutSigTable.rs232OutSigEntry.rs232OutSigPortIndex	10.33.6.1.1		
transmission.rs232.rs232OutSigTable.rs232OutSigEntry.rs232OutSigName	10.33.6.1.2		
transmission.rs232.rs232OutSigTable.rs232OutSigEntry.rs232OutSigState	10.33.6.1.3		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
transmis-sion.rs232.rs232OutSigTable.rs232OutSigEntry.rs232OutSigChanges	10.33.6.1.4		
snmp.snmpInPkts	11.1		
snmp.snmpOutPkts	11.2		
snmp.snmpInBadVersions	11.3		
snmp.snmpInBadCommunityNames	11.4		
snmp.snmpInBadCommunityUses	11.5		Always 0
snmp.snmpInASNParseErrs	11.6		
snmp.snmpInTooBigs	11.8		Always 0
snmp.snmpInNoSuchNames	11.9		Always 0
snmp.snmpInBadValues	11.10		Always 0
snmp.snmpInReadOnlys	11.11		
snmp.snmpInGenErrs	11.12		Always 0
snmp.snmpInTotalReqVars	11.13		
snmp.snmpInTotalSetVars	11.14		
snmp.snmpInGetRequests	11.15		
snmp.snmpInGetNexts	11.16		
snmp.snmpInSetRequests	11.17		
snmp.snmpInGetResponses	11.18		Always 0
snmp.snmpInTraps	11.19		Always 0
snmp.snmpOutTooBigs	11.20		
snmp.snmpOutNoSuchNames	11.21		
snmp.snmpOutBadValues	11.22		
snmp.snmpOutGenErrs	11.24		

Table 4: SX05DA support of MIB-II

Object name	Numeric name	R/W	Notes
snmp.snmpOutGetRequests	11.25		Always 0
snmp.snmpOutGetNexts	11.26		Always 0
snmp.snmpOutSetRequests	11.27		Always 0
snmp.snmpOutGetResponses	11.28		
snmp.snmpOutTraps	11.29		
snmp.snmpEnableAuthenTraps	11.30	✓	IP-XPM (SX05DA) does not send traps.

Table 5: SX05DA support of SNMPv2

Object name	Numeric name	R/W	Notes
snmpModules.usecMIB.usecMIBObjects.usecAgent.agentID	3.6.1.1.1		
snmpModules.usecMIB.usecMIBObjects.usecAgent.agentBoots	3.6.1.1.2		
snmpModules.usecMIB.usecMIBObjects.usecAgent.agentTime	3.6.1.1.3		
snmpModules.usecMIB.usecMIBObjects.usecAgent.agentSize	3.6.1.1.4		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsUnsupportedQos	3.6.1.2.1		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsNotInWindows	3.6.1.2.2		Always 0
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsUnknownUserNames	3.6.1.2.3		

Table 5: SX05DA support of SNMPv2

Object name	Numeric name	R/W	Notes
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsWrongDigestValues	3.6.1.2.4		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsUnknownContexts	3.6.1.2.5		Always 0
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsBadParameters	3.6.1.2.6		
snmpModules.usecMIB.usecMIBObjects.usecStats.usecStatsUnauthorizedOperations	3.6.1.2.7		Always 0

3: Configuration for A00009011

3.1 Hardware and Software Requirements

This feature does not introduce any new hardware requirements.

This feature requires new loads in the IP-XPM (SX05DA) and in the NT7X07AA. These loads interpret and act on the SNMP and Telnet configuration data downloaded from new datafill in the CM.

The applicable loads are as follows:

- IP-XPM (SX05DA): TBD
- 7X07AA: TBD

3.2 Initial Configuration

The new SNMP settings have default values such that behavior of the IP-XPM (SX05DA) and 7X07AA is unchanged following an upgrade from a pre-SN09 (TOPS22) load to an SN09 or higher load. For security, however, Telnet on a 7X07AA is always disabled following an upgrade from a pre-SN09 (TOPS22) load to an SN09 or higher load.

3.3 Office parameters (OP)

This feature adds four new office parameters. These office parameters affect 7X07AA cards defined in Table IPINV as TOPS IPGWs (`GW_TYPE` = `TOPS`). These parameters do not affect non-TOPS IPGWs.

3.3.1 New/modified office parameters

Table 1 New or modified parameter

Parm table	Parameter name	NEW/CHANGED/DELETED/RELOCATED	Domain (CM or Subnet Management)
OFCENG	IPGW_SNMP_COMMUNITY_NAME	New	CM
OFCENG	IPGW_SNMP_MANAGER	New	CM
OFCENG	IPGW_SNMP_ENABLED	New	CM
OFCENG	IPGW_TELNET_ENABLED	New	CM

3.3.2 Parameter information

3.3.2.1 IPGW_SNMP_COMMUNITY_NAME

Internet Protocol Gateway Simple Network Management Protocol Community Name

3.3.2.1.1 Functional description

This parameter allows the craftsperson to configure one SNMP community name for SNMP read, write, and trap operations on the 7X07AA.

3.3.2.1.2 Provisioning rules

The craftsperson defines the community name (up to 16 characters) then datafills it in Table OFCENG, using single quotes to allow entry of lowercase letters or non-alphanumeric symbols.

3.3.2.1.3 Range information

Table 2 Range Information

Minimum	Maximum	Default
One letter, digit, or non-alphanumeric symbol	Sixteen letters, digits, non-alphanumeric symbols, or any combination thereof	The string “public” (lowercase, and without the quotation marks) is the default. This is a customary default community name, and it is what currently deployed 7X07AAs use.

3.3.2.1.4 Activation

The new community name does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. For all cards to be updated, all cards must be PMRESET. This should be done sequentially using the existing IPGW DRAIN command such that traffic is off-loaded (drained) from each

7X07AA before the card is PMRESET. This minimizes the effect on calls in progress.

3.3.2.1.5 Dependencies
None.

3.3.2.1.6 Consequences
Leaving this parameter set to the default value (“public”) increases the risk that a hacker will be able to use SNMP to alter data on the 7X07.

3.3.2.1.7 Verification
To verify the change, the craftsperson can update the community name on their SNMP manager client, then attempt SNMP operations on the changed 7X07AAs. If the SNMP operations succeed, the new community name is in use by the 7X07AAs.

3.3.2.1.8 Memory requirements
20 bytes

3.3.2.1.9 Parameter release history update
SN09 (TOP22): Creation

3.3.2.2 IPGW_SNMP_MANAGER
Internet Protocol Gateway Simple Network Management Protocol Manager

3.3.2.2.1 Functional description
This parameter allows the craftsperson to configure the IP address of one SNMP manager (also known as a trap manager). The 7X07AA cards will send traps to this IP address.

Prior to SN09 (TOPS22), the 7X07AA allowed entry of up to four SNMP manager IP addresses. The default SNMP manager is obtained using DHCP, while up to three additional SNMP managers can optionally be defined using PMDEBUG on the 7X07AA. This feature allows a fifth SNMP manager IP address to be configured.

3.3.2.2.2 Provisioning rules
The craftsperson datafills the IPv4 address in Table OFCENG. The IPv4 address consists of four numbers, each in the range 0 to 255.

3.3.2.2.3 Range information

Table 3 Range Information

No SNMP manager	SNMP manager	Default
IPGW_SNMP_MANAGER set to N.	IPGW_SNMP_MANAGER set to Y. In this case a second field, IPADDR, appears. The craftsperson datafills the IP address of the SNMP manager. For example, IP address 47.142.225.193 would be datafilled as: Y 47 142 225 193	N (no manager datafilled)

3.3.2.2.4 Activation

The new SNMP manager does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level.

3.3.2.2.5 Dependencies

None.

3.3.2.2.6 Consequences

Leaving this parameter set to the default value (“N”) increases the risk that a hacker will be able to use SNMP to alter data on the 7X07.

3.3.2.2.7 Verification

To verify the change, the craftsperson can attempt SNMP write operations[3] using an SNMP manager client on a host whose IP address was not previously set on the 7X07AA using DHCP or PMDEBUG. If the write operations succeed, the new SNMP manager IP address is in use.

A subsequent security test would be to set the office parameter back to N, PMRESET the card, and try a second set of SNMP write operations using the same host as in the first test. The host is no longer in the valid SNMP manager list on the 7X07AA, so the 7X07AA should reject SNMP write attempts.

3.3.2.2.8 Memory requirements

8 bytes

3.3.2.2.9 Parameter release history update

SN09 (TOP22): Creation

[3] The SNMP manager IP address is only checked for write operations, not read operations.

3.3.2.3 IPGW_SNMP_ENABLED

Internet Protocol Gateway Simple Network Management Protocol Enabled

3.3.2.3.1 Functional description

This Y/N parameter allows the craftsperson to enable or disable SNMP on the 7X07AA.

3.3.2.3.2 Provisioning rules

No special provisioning rules.

3.3.2.3.3 Range information

Table 4 Range Information

Minimum	Maximum	Default
This is a Y/N field	This is a Y/N field	Defaults to N unless TOPS IPGWs are present in Table IPINV on the dump side, in which case this parameter defaults to Y.

3.3.2.3.4 Activation

The SNMP enabled/disabled status does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level.

3.3.2.3.5 Dependencies

None.

3.3.2.3.6 Consequences

Leaving this parameter set to Y increases the risk that a hacker will be able to use SNMP to alter data on the 7X07.

3.3.2.3.7 Verification

To verify the change, the craftsperson can attempt SNMP operations on the changed 7X07AAs. If the operations succeed, SNMP is enabled. If the operations time out, SNMP is disabled.

3.3.2.3.8 Memory requirements

2 bytes

3.3.2.3.9 Parameter release history update

SN09 (TOP22): Creation

3.3.2.4 IPGW_TELNET_ENABLED

Internet Protocol Gateway Telnet Enabled

3.3.2.4.1 Functional description
This Y/N parameter allows the craftsperson to enable or disable Telnet on the 7X07AA.

3.3.2.4.2 Provisioning rules
No special provisioning rules.

3.3.2.4.3 Range information
Table 5 Range Information

Minimum	Maximum	Default
This is a Y/N field	This is a Y/N field	Defaults to N.

3.3.2.4.4 Activation
The Telnet enabled/disabled status does not take effect on a 7X07AA until the card is PMRESET from the MAPCI;MTC;PM level. See "3.3.2.1.4 Activation" on page 2040 for more information.

3.3.2.4.5 Dependencies
None.

3.3.2.4.6 Consequences
Leaving this parameter set to Y increases the risk that a hacker will be able to log on to the 7X07AA and possibly crash the card, ending up to 48 calls.

3.3.2.4.7 Verification
To verify the change, the craftsperson can attempt to Telnet onto the changed 7X07AAs. If the craftsperson receives the login prompt, Telnet is enabled. If the attempt times out, Telnet is disabled.

3.3.2.4.8 Memory requirements
2 bytes

3.3.2.4.9 Parameter release history update
SN09 (TOP22): Creation

3.4 Upgrade Considerations

3.4.1 Dump and Restore (CM)
The following actions occur on dump and restore from a pre-SN09 load to an SN09 or higher load.

- IPGW_SNMP_COMMUNITY_NAME: This parameter is set to "public" (without quotation marks).
- IPGW_SNMP_MANAGER: This parameter is set to N.

- IPGW_SNMP_ENABLED: Table IPINV on the dump side is consulted. If any TOPS IPGWs are present (GW_TYPE = TOPS), this parameter is set to Y. Otherwise this parameter is set to N.
- IPGW_TELNET_ENABLED: This parameter is set to N.

3.4.2 Element Management Upgrade

Not applicable.

3.4.3 Downgrade impact

If data has already been downloaded to the 7X07AAs and the core is downgraded to a pre-SN09 release, the 7X07AAs retain the last settings from the core prior to the downgrade. If a 7X07AA is PMRESET at a later time, data download occurs again. The 7X07AA checks the release level of the downloaded information, and if it is prior to SN09, the 7X07AA will not try to read the SNMP and Telnet fields (since the core did not send them). As a result, the 7X07AA will not change its SNMP and Telnet settings.

3.5 Data schema (DS)

3.5.1 New/modified tables

Table 6 New or modified tables

Table	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
XPMIPMAP	Changed	Unchanged

3.5.2 Table information

3.5.2.1 Name: XPMIPMAP

eXtended Peripheral Module Internet Protocol Mapping

3.5.2.1.1 Functional description

This existing table defines the IP-XPMs and allows configuration of IP capabilities on the redundant SX05DA processor cards.

This feature adds a new field, SNMP, which indicates whether SNMP is enabled on the IP-XPM. If SNMP is enabled, the craftsperson must also datafill an SNMP community name in new subfield COMMNAME.

3.5.2.1.2 Usage sequence and implications

Unchanged.

3.5.2.1.3 Size

Table 7 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
XPMIPMAP	Unchanged	Unchanged	New SNMP datafill adds 20 bytes per tuple

3.5.2.1.4 Fields

Table 8 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
XPMNAME	Unchanged	N/A	N/A	N/A
AUTONEG	Unchanged	N/A	N/A	N/A
SUBNMASK	Unchanged	N/A	N/A	N/A
IPCONFIG	Unchanged	N/A	N/A	N/A
SNMP	New	This field is refined based on the value datafilled.	Y/N	If SNMP is Y, datafill the SNMP community name in the additional field COMMNAME. If SNMP is N, no additional fields can be datafilled.
COMMNAME	New	Subfield of field SNMP This field appears when field SNMP is set to Y.	Vector of one to sixteen characters Non-alpha-numeric symbols and lowercase letters can be entered using single quotes.	This field indicates the SNMP community name for SNMP read and write operations on the IP-XPM. The IP-XPM does not send traps so this community name is not currently used for SNMP traps.

3.5.2.1.5 Datafill example

The following example shows sample datafill for Table XPMIPMAP.

```
TABLE: XPMIPMAP
XPMNAME AUTONEG SUBNMASK IPCONFIG SNMP
-------------------------------------
DTC 11 AUTO 255 255 255 0 CM 95 64 10 164 95 64 10 165 95 64 10 166
95 64 10167 (4) (5) $ N N
DTC 12 AUTO 255 255 255 0 CM 95 92 9 132 95 92 9 133 95 92 9 134
95 92 9 135(3) (2) $ N Y public
```

3.5.2.1.6 Table release history update

TOPS13: Creation

SN09 (TOPS22): Addition of field SNMP

3.5.2.1.7 Supplementary information

On dump and restore from a pre-SN09 Succession core load to an SN09 or later load, new field SNMP is set to Y and new field COMMNAME is set to “public” (without quotation marks). These settings cause IP-XPM behavior to be unchanged from pre-SN09 loads.

3.5.2.1.8 Translation verification and other tools

Not applicable.

3.6 Service Orders (SO)

Not applicable.

3.7 Software optionality control (SOC)

Table 9 SOC

SOC option name:	OSB00101
SOC option title:	Basic Operator Services
SOC option control type:	State
New SOC option?	No
SOC option order code	???
Option defined in DRU:	TOPS
Affected products:	TOPS

3.8 Element Management

Not applicable.

3.9 User interface changes

Not applicable.

3.10 OSSGate Interface Changes

Not applicable.

3.11 Security

3.11.1 Network configuration

TOPS-IP network configuration recommendations are unchanged.

3.11.2 Key management

Not applicable.

3.11.3 Protocol

Not applicable.

3.11.4 Authentication

This feature allows the SNMP community name to be changed from “public” to a customer-specified name. This feature also allows the SNMP manager to be datafilled in the CM. The community name is used to authenticate incoming read and write requests on both the IP-XPM (SX05DA) and the 7X07AA. The SNMP manager is used to authenticate incoming write requests on the 7X07AA.

This feature also allows SNMP to be completely disabled on the IP-XPM (SX05DA) and the 7X07AA. In addition, Telnet can be disabled on the 7X07AA. These measures provide additional security if the customer is not using SNMP and Telnet.

3.12 Configuration Walkthrough

To configure new SNMP settings on the IP-XPM (SX05DA):

- Set the appropriate fields in the Table XPMIPMAP tuple corresponding to the desired IP-XPM.
- Perform a LoadPM or Bsy/RTS to download the settings to the desired units of the IP-XPM.

To configure new SNMP and Telnet settings on the 7X07AA:

- Set the appropriate office parameters in the Table OFCENG.
- Perform a PMRESET on the desired cards to download the settings. The settings do not take affect on a card until it has been PMRESET.

Product = CS 2000 TOPS

A00009012 -- TOPS OSSAIN Service Enhancements

Functional Description

1: Applicable Solution(s)

PT-AAL1, PT-IP, DMS

1.1 Description

This feature addresses a number of items to improve the OSSAIN functionality. It provides the following:

- The ability for an SN function to set the service of the call as it is being transferred or triggered.
- The ability for TOPSOPER and DASERV SN functions to indicate the call being transferred or triggered should be handled as a DA recall to increment the DA recall counter and populate operator messaging as needed.
- The removal of TOPSAUTO option AABS from table OAFUNDEF since AABS was EOL'd in a prior release.
- The support of MCCS for TOPSAUTO options in table OAFUNDEF to replace the default processing left by the AABS option. Since AABS could have still been datafilled, a call could route to AABS but fail since AABS was EOL'd - the call would then be routed to MCCS if available or operator if not.
- The replacement of ping usage in node audits and in the MAPCI command TST. Pings are not supported on certain platforms and are therefore replaced with an OAP message, Node Connectivity Test, as needed.
- The notification of OSSAIN Broadcast Announcements being EOL'd in SN10. The TEOL log will be generated whenever OSSAIN Broadcast Announcements are used.

Each of these areas is described in one of the following sections:

— SN Service for Transfers/Triggers

— DA Recall Support for OSSAIN

— AABS removal; MCCS support for OSSAIN functions

— OSSAIN Ping Replacement

— EOLing of OSSAIN Broadcast Announcements

— SOC and Table TOPSFTR for activation

1.1.1 SN Service for Transfers/Triggers

This portion of the feature enhances OSSAIN by allowing datafill to indicate what the service of the SN function should be for transfers and triggers.

1.1.1.1 Background

When an SN was allowed to offer DA service assistance, it was initially only designed to act like an ADAS/ADAS+ replacement to collect the city/name recording and perform the playback to an operator. The initial design did not anticipate a DA SN being able to fully automate a DA call nor provide service for DA recalls or transfers. Therefore, the switch assumes a DA call going from an operator to an SN must be going for call completion and switches the service to TA (along with cutting an AMA, changing the call origination, and resetting some billing parameters).

1.1.1.2 Enhancements

This feature provides datafill to override the switch assumptions in changing from DA to TA for operator to SN transfers. (If the service is not changed from DA to TA then the call origination will not change.) It also generalizes the ability of setting the proper service for an SN function to all transfers and triggers.

Table OAFUNDEF is enhanced to include two new options, one for the SN service and the other for generating AMA.

- The new SN service indicator datafill will be used for all transitions to an SN but not for initial call presentation. The scenarios include:
  - — Transfers from operator to SN
  - — Transfers from DAS to SN
  - — Transfers from SN to SN
  - — Triggers to SN
  - — Disposition Routing resulting in route to SN

1.1.1.3 Table OAFUNDEF: New Field USESERV

The following illustrates the new look of table OAFUNDEF with this feature; however, each section will bold the new area it is discussing.

A new field, USESERV is added to table OAFUNDEF for calls transitioned to SN functions . When set to Y it indicates the service defined in ORIGSERV should be used for a call in transition (transfer, trigger, disposition routing).

Table 1 New Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
1	DA_SN	SN DASERV Y **N** N N N N Y CQ17 N
2	DA_TOPSOPER	TOPSOPER N OSSAIN_TO_DA_OPR N
3	TA_AUTO	TOPSAUTO MCCS 0_PLUS
4	TA_SN	SN TASERV **N** N N N Y Y CQ0 N
5	DA_SN_RCL	SN DASERV Y **Y** N N N N Y CQ17 N
6	DA_TOPSOPER_RCL	TOPSOPER Y OSSAIN_TO_DA_OPR N
7	TA_AUTO_RCL	TOPSAUTO MCCS 0_PLUS
8	TA_SN_RCL	SN TASERV **Y** N N N Y Y CQ0 N

- For a call in transition (transfer, trigger, disposition routing) to an SN function, the following processing occurs for the new field USESERV:if set to N, then existing functionality is maintained which means the service is maintained or switched DA to TA for operator to SN transfers
- if set to Y and the ORIGSERV is the same as the current service, then no changes are made to the call
- if set to Y and the ORIGSERV is different than the current service, then the service is changed and associated parameters reset as required with all service changes as noted in the OAP spec for service switches

  Note: Whenever the OAFUNDEF option USESERV switches services, the same side effects occur as when an OAP Service Change Request is processed. Consult to OAP Specifications Document for details.

1.1.2 DA Recall Support for OSSAIN

This feature provides a datafillable means for OSSAIN to recognize a DA recall for calls which do not use the switch-based ARU structure for listing announcements. It will increment the DA recall counter and populate operator messaging as needed.

1.1.2.1 Background

A DA SN can offer listings via back-end announcements without using switch-based ARUs. The subscriber can initiate a recall from the announcement for an incorrect listing or for another listing. Transfers or triggers can be used to service the recall via an OSSAIN function. However, there is no mechanism provided for the SN or function to indicate this service

is a recall service to mark recall counters to compare to switch limits as defined in table VROPT: maximum_da_recalls. Thus, if a call was serviced by an SN and then recalls to a TOPS operator, the call can exceed the maximum number of recalls defined in VROPT.

The vropt:maximum_da_recalls parameter was initially developed to limit the number of times a call can recall back to an operator to limit operator work time on one call. This parameter is not intended to track the number of listings. The maximum number of requested listings is datafillable in DATRKOPT field MULTREQ.

1.1.2.2 Enhancement

This feature provides datafill to note a DA recall via OSSAIN function to align SN and operator recall counts. It allows a method to count DA recalls processed by an operator and by an SN.

When the OSSAIN function is datafilled as a DA recall function, the DA recall counter is incremented and the OPP field, reason_for_operator, set to recall for proper processing at the position if the call routes to an operator.

The feature will also check if the maximum number of DA recalls has been reached prior to allowing the transition to the function. If the maximum DA recall limit has been reached and the call attempts to go to a DA recall function, then the call will be routed to treatment using the default_treatment of table OAINPARM, which is also used when the maximum number of transitions has been reached.

1.1.2.3 Table OAFUNDEF: New Field DARECALL

Note: The following illustrates the new look of table OAFUNDEF with this feature; however, each section will bold the new area it is discussing.

New field DARECALL is added in table OAFUNDEF to both TOPSOPER and DASERV SN functions. When set to Y, the count for DA recalls is incremented and, if going to an operator, the OPP field reason_for_operator is populated as recall.

Table 2 New Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
1	DA_SN	SN DASERV **Y** N N N N N Y CQ17 N
2	DA_TOPSOPER	TOPSOPER **N** OSSAIN_TO_DA_OPR N
3	TA_AUTO	TOPSAUTO MCCS 0_PLUS

Table 2 New Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
4	TA_SN	SN TASERV N N N N Y Y CQ0 N
5	DA_SN_RCL	SN DASERV **Y** Y N N N N Y CQ17 N
6	DA_TOPSOPER_RCL	TOPSOPER **Y** OSSAIN_TO_DA_OPR N
7	TA_AUTO_RCL	TOPSAUTO MCCS 0_PLUS
8	TA_SN_RCL	SN TASERV Y N N N Y Y CQ0 N

Note: OAFUNDEF field DARECALL only applies to functions used in transfers and triggers. It is ignored for original services.

1.1.3 MCCS Support for OSSAIN Functions

This feature removes the AABS TOPSAUTO option from table OAFUNDEF datafill and adds the MCCS TOPSAUTO option.

Although AABS has been EOL'd, it was still possible for a call to route to the TOPSAUTO AABS datafill, fail AABS and then try to go to MCCS. Therefore, OSSAIN calls could route to MCCS in this manner. If the call was not eligible for MCCS then it was routed to an operator.

This feature maintains the existing functionality. Therefore, over an ONP, AABS will be replaced with MCCS and the call will route to MCCS instead of failing AABS first.

1.1.4 OSSAIN Ping Replacement

OSSAIN needs to replace ping (ICMP echo) functionality due to the following reasons:

— For security reasons, some customers may not allow ping in their Succession networks.

— Ping is not supported on some SOS platforms on which TOPS may be supported in the future.

SN07 activity A00005160 introduced the OAP Node Connectivity Test operation. The purpose of this operation is to verify application-layer connectivity between the switch and a service node. In SN07 and higher, OAP Node Connectivity Test messaging replaces ping in an OSAC remote in the RTS sequence for an OSN, if the OSN is at OAP 9 or higher and the OSAC host is at SN07 or higher.

This feature addresses the remaining situations in which OSSAIN has historically used pings - in audits and in the TST MAPCI command.

1.1.4.1 OSSAIN Audits

If an OSAC remote has not received a message from an in-service OSN for a datafilled time interval, it audits the OSN. Historically this audit has consisted of first a ping to the OSN and then, if a response is received, a Node Datafill Check Request to OSAC host. If the remote times out waiting for the ping reply, it retries a datafilled number of times.

With this feature, an OSAC remote at SN09 or higher uses the OAP Node Connectivity Test for the audit, rather than using ping, if the OSAC host is at SN07 or higher and the OSN is at OAP 9 or higher. Audit retries and time-outs are unchanged.

1.1.4.2 MAPCI TST Command

The `TST` command is available with an OSNM, OSN, or OSAC node posted at the MAP. A node must be ManB to be tested. The `TST` command has two variations which, prior to this feature, used pings - `TST` with no parameters and `TST` with the optional `PING` parameter.

- If `TST PING` is entered, the switch sends a ping request to the posted node and reports success on receipt of a valid reply. If it can't send the request or doesn't get a valid reply, it reports failure. This feature adds a new failure response, "Use TST without PING," which is displayed if the MAP user enters `TST PING` on a platform that does not support ping.
- If `TST` is entered with no parameters, the functionality prior to this feature depended on the kind of node being tested:
  - OSNM - First did a ping test on the OSNM. Then if that succeeded, sent a Node Test Request to the OSNM.
  - OSAC - First did a ping test on the OSAC node. Then if that succeeded, sent an OSAC Node Test Request to the OSAC node.
  - OSN - First did a ping test on the OSN. Then if that succeeded, sent an OSN Node Datafill Check Request to the OSAC host.

  Notice that for OSNM and OSAC, the ping test was immediately followed by an OAP or OSAC message to the same node. The subsequent message also verifies connectivity. Therefore, this feature eliminates the redundant ping in the test sequence for OSNM and OSAC nodes.

  For OSN, the ping could not simply be removed from the test sequence because it is not followed by another message to the OSN. Therefore, for OSN nodes this feature substitutes a Node Connectivity Test request for the ping. This substitution occurs only if the OSAC remote is at SN09 or higher, the OSAC host is at SN07 or higher, and the OSN is at OAP 9 or higher.

1.1.5 EOLing of OSSAIN Broadcast Announcements

OSSAIN broadcast announcements will be EOL'd in SN10. A TEOL log will be generated in SN09 whenever OSSAIN Broadcast Announcements are used to indicate the functionality will be removed in SN10. The TEOL log will also be patched back to two prior releases.

1.1.6 SOC and Table TOPSFTR

A new entry in table TOPSFTR will control this feature's activation which will be tied to existing SOC option, OSAN0102: OSSAIN Enhancements. This new TOPSFTR entry will be called OSSAIN_RELEASE_22 to align with prior OSSAIN features.

The new entry will activate the call processing of the following portions of this feature (note datafill will be allowed regardless of this parameter):

- Transfer to SN function service
- DA Recall function

Table 3 Table TOPSFTR

FTRNAME	FTRENABL
OSSAIN_RELEASE_22	Y

1.2 Hardware Requirements or Dependencies

No new hardware requirements or dependencies.

1.3 Software Requirements or Dependencies

No special software requirements or dependencies.

Note: The OAP version is not increased by this feature since this feature does not change OAP.

1.4 Limitations and restrictions

- Although the DARECALL option in table OAFUNDEF could have been generalized to include TA recalls, TA recalls would apply to coin calls and since OSSAIN does not support coin at this time, this feature only supports DA recalls.
- Whenever the OAFUNDEF option USESERV switches services, the same side effects occur as when an OAP Service Change Request is processed. Consult to OAP Specifications Document for details.

1.5 Interactions

None

1.6 Glossary

No new terms are introduced with this feature.

2: Configuration for A00009012

2.1 Data schema (DS) (CM)

2.1.1 Modified tables Schema

Table 1 Modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
OAFUNDEF	CHANGED	UNCHANGED
TOPSFTR	CHANGED	UNCHANGED

2.1.2 Table Schema information

2.1.2.1 Name: OAFUNDEF

OSSAIN Function Definitions

2.1.2.1.1 Functional description

The table's functionality is unchanged.

2.1.2.1.2 Size

Unchanged with a maximum tuple range of 1022.

2.1.2.1.3 Fields

The following table lists fields/OIDs for OAFUNDEF.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FUNCAREA	FUNCAREA is unchanged but has two new subfields and a change to an existing subfield			

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
	New	USESERV	Y, N	**Use ORIGSERV** N means to allow the switch to change the DA service to TA when an operator transfers the call to an SN. All other transition scenarios will retain the service of the call. Y means to ensure the service datafilled in field ORIGSERV of OAFUNDEF is used when transferring or triggering to the function. If a service switch occurs, then other fields may be effected based on service switch rules defined in the OAP Specification document. This field is not needed to set the service with ORIGSERV for initial call processing. It is used for transitions only.
	New	DARECALL	Y, N	**DA Recall** N is not a DA recall Y means the call going to the function is a DA recall and the switch will increment the DA recall counter and set operator indicators for recall if going to an operator. This field is not used for initial call processing.
	Changed	AUTOSYS	MCCS, DAS	**Automated Systems** MCCS will route the call to MCCS. If MCCS is not available for the call then it is routed to operator.

2.1.2.1.4 Datafill example

The following example shows sample datafill for table OAFUNDEF.

Table 3 New Table OAFUNDEF

FUNCID	FUNCNAME	FUNCAREA
1	DA_SN	SN DASERV Y N N N N N Y CQ17 N
2	DA_TOPSOPER	TOPSOPER N OSSAIN_TO_DA_OPR N
3	TA_AUTO	TOPSAUTO MCCS 0_PLUS
4	TA_SN	SN TASERV N N N N Y Y CQ0 N
5	DA_SN_RCL	SN DASERV Y Y N N N N Y CQ17 N
6	DA_TOPSOPER_RCL	TOPSOPER Y OSSAIN_TO_DA_OPR N
7	TA_AUTO_RCL	TOPSAUTO MCCS 0_PLUS
8	TA_SN_RCL	SN TASERV Y N N N Y Y CQ0 N

2.1.2.1.5 Table release history update

In SN09, table OAFUNDEF added fields USESERV, DARECALL, removed TOPSAUTO option AABS and added TOPSAUTO option MCCS.

2.1.2.1.6 OAFUNDEF error messages

New error messages for table OAFUNDEF are noted below:

Table 6 Error messages for table OAFUNDEF

Error message	Explanation
`MCCS and DAS are the only TOPS automated system that are currently supported for OSSAIN.`	The user tries to datafill the AUTOSYS refinement with an automated system other than MCCS or DAS.

2.1.2.1.7 ONP Processing

Over a pre-SN09 to SN09+ ONP, the following fields/sub-fields will be populated as shown:

- USESERV will be set to N.
- DARECALL will be set to N.
- AUTOSYS AABS functions will be changed to MCCS.

2.1.2.2 Name: TOPSFTR

TOPS Features

2.1.2.2.1 Functional description

The table's function has not changed.

2.1.2.2.2 Size

Increased by 1

2.1.2.2.3 Datafill example

The following example shows sample datafill for table TOPSFTR.

Table 4 Table TOPSFTR

FTRNAME	FTRENABL
OSSAIN_RELEASE_22	Y

2.1.2.2.4 Table release history update

In SN09, table TOPSFTR added OSSAIN_ENHANCEMENTS_22 to the range.

2.1.2.2.5 Supplementary Information

TOPSFTR entry, OSSAIN_RELEASE_22 is tied to SOC option OSAN0102 for OSSAIN Enhancements and activates the following portions of feature A00009012:

- Transfer to SN function service
- DA Recall function

Although the functionality is controlled by this parameter, the associated datafill can be entered prior to activation.

2.2 Software optionality control (SOC)

Portions of feature A00009012 are activated by SOC option OSAN0102 and TOPSFTR entry OSSAIN_ENHANCEMENTS_22.

Table 5 SOC

SOC option name:	OSSAIN Enhancements
SOC option title:	Yes
SOC option control type:	state
New SOC option?	No
SOC option order code	OSAN0102
Option defined in DRU:	TOPS

2.3 User interface changes

2.3.1 Command: TST

2.3.1.1 Command type: unchanged

2.3.1.2 Command target: unchanged

2.3.1.3 Command availability: unchanged

2.3.1.4 Command description

TST is a command used for OSNM, OSN and OSAC nodes posted at the MAP. When a node is posted at the PM level of the MAP, the TST command is available. The TST command remains unchanged by this feature; however, the functionality of the command is changed and one new response message is provided.

- When TST is entered for a node, a ping is no longer sent. For OSN however, the Node Connectivity Test message is now sent to the OSN node in place of the ping to verify connectivity.
- When TST PING is entered for a node on a platform that does not support ping from SOS, the following new response message is provided: "Use TST without PING.".

2.3.1.5 Command syntax

Unchanged

2.3.1.6 Qualifications and warnings

Unchanged

2.3.1.7 Responses

2.3.1.7.1 "Use TST without PING."

Table 6 MAP outputs with associated meanings and actions

TST PING
"Use TST without PING." **Meaning:** TST PING has been used on a switch which does not support pings from MAP. **System or user actions:** Use command TST without the PING option. Ping from another platform.

Product = CS 2000 TOPS

A00009013 -- TOPS announcements via UAS/AMS

Functional Description

1: Applicable Solution(s)

PT-IP, DMS

1.1 Description

This activity provides the ability for Traffic Office Position System (TOPS) calls to use packet-based announcements. The functionality is available on Communication Server 2000 (CS 2000) with TOPS, in Succession hybrid offices with ENET and IP-based Succession solutions.

The packet announcement platforms that Nortel supports in SN09 for CS 2000 are the Media Server 2000 (MS 2000) Series and the older Universal Audio Server (UAS). The UAS is no longer sold, but this feature will work with it as long as Nortel supports it. The MS 2000 Series model used with IP bearer networks is the MS 2010.

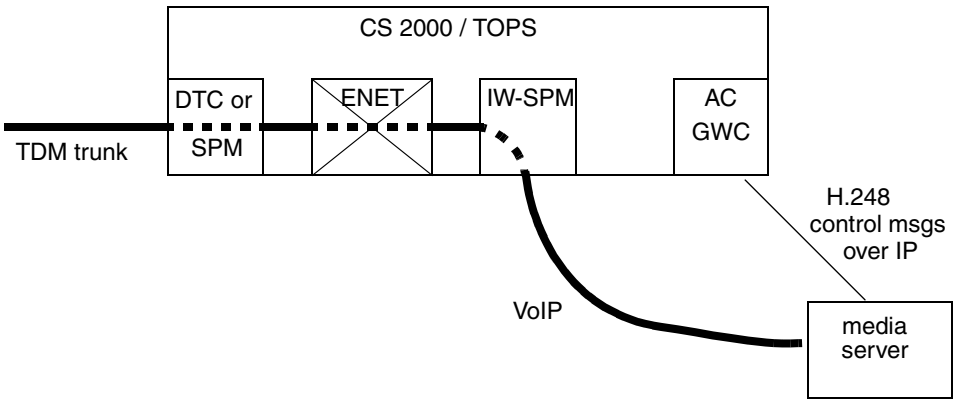
In the Succession architecture, MS 2000 Series and UAS are special-purpose media gateways referred to as media servers. Each media server is controlled by a Gateway Controller (GWC) that is configured with the Audio Controller profile. An Audio Controller GWC can control multiple media servers, with the restriction that the same set of announcements must be provisioned on all the media servers that are controlled by the same GWC. The protocol between the GWC and the media server is H.248.

The operating company provides the voice recordings for packet-based announcements. Your Nortel or AudioCodes representative can refer you to professionals who provide this service. The web-based Audio Provisioning Server (APS) is used to provision the recordings on the media servers. Then CM datafill is entered in table ANNAUDID to associate the announcement phrase names known in the CM with the segment identifiers that were provisioned on the media servers. Other CM announcement tables are datafilled similarly for packet announcements as for legacy announcements.

This activity does not change the restriction that calls can only enter the TOPS environment on legacy TDM trunks, and can only use legacy TDM conference resources. Therefore, an interworking bridge on an Interworking Spectrum Peripheral Module (IW SPM IP) is required for each TOPS call that connects

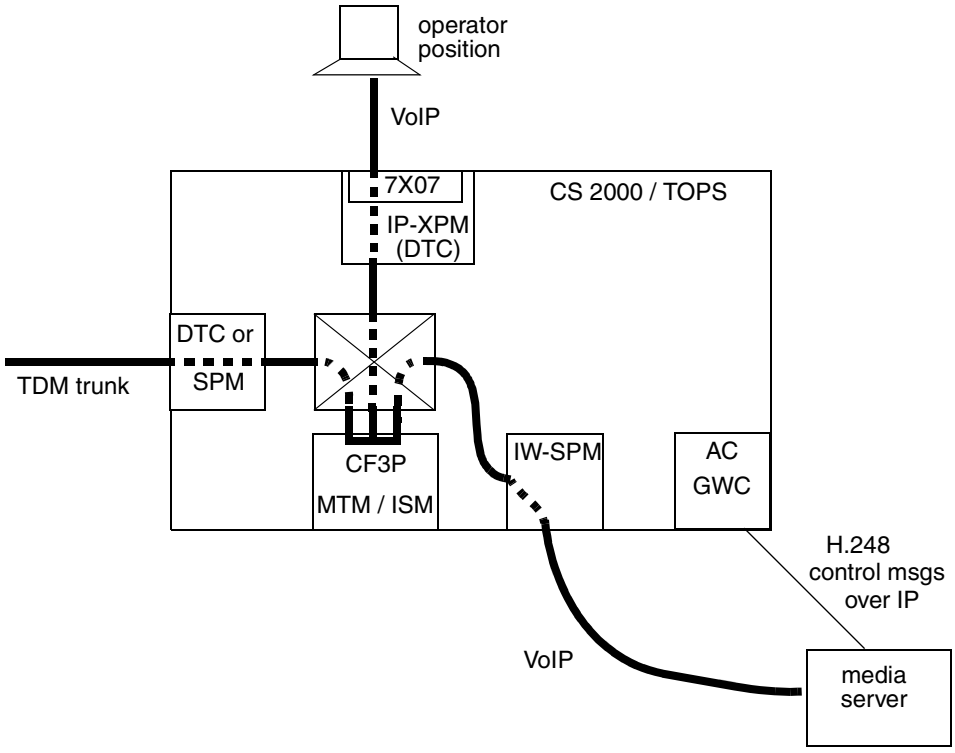
to a packet announcement. The following figures show example topologies. The first example shows a TOPS call that has only the calling party connected to a packet-based announcement.

Figure 1 Legacy trunk connected to packet announcement



The next example shows a TOPS call that has an operator, a calling party, and a packet-based announcement.

Figure 2 Legacy conference connected to packet announcement



In both examples, the TDM trunk is any legacy PTS or ISUP trunk type that could originate calls to TOPS prior to this feature. It could be a looparound trunk, or it could connect to another office.

An announcement can have both legacy DRAM/EDRAM and packet members. If both legacy and packet members are available when a TOPS call needs an announcement, the CS 2000 automatically attempts to select a member whose network fabric matches that of the other agents on the call. Since all other agents on a TOPS call are connected to the ENET in SN09, this implies that legacy announcement members are always selected for TOPS calls if a legacy member is available. However, if only packet members are available, and if an interworking bridge is available, then a TOPS call will use a packet member and will automatically connect to it using the interworking bridge.

This activity supports TOPS use of packet announcements for the following functionalities:

- Branding
- Treatment
- Direct route to announcement via standard translations and routing
- Announcement segments of audio program for the Music and Announcement in Queue feature
- Automatic Coin Toll Service (ACTS)

  ACTS announcements are also used for the TOPS Time and Charges, Non-coin Notify, and ACTS Coin Tone Generation Test features. Those features can also use packet-based announcements.
- Mechanized Calling Card Service (MCCS)

  MCCS announcements are also used for the TOPS Sequence Calling, Account Code Billing, and Authorization Code features. Those features can also use packet-based announcements.

The functionality provided by this feature is automatically activated when packet members are brought into service for announcement groups that are used by TOPS calls.

This feature does not change the functionality of TOPS calls that use legacy DRAM/EDRAM announcements.

1.2 Hardware Requirements or Dependencies

This activity does not introduce new hardware. It uses hardware that is standard for CS 2000 IP hybrid with packet-based announcements.

1.3 Software Requirements or Dependencies

This functionality is first available in SN09. The software is also present in ISN09, but Nortel has tested it only with the North American load.

1.4 Limitations and restrictions

This activity does not add support for TOPS calls to connect directly with any kind of Succession agent other than announcements. Packet calls destined for TOPS in a CS 2000 must still arrive in the TOPS environment on legacy TDM trunks, using looparound facilities if needed to accomplish that.

This activity does not support packet-based announcements for TOPS custom announcement types TOPSVR and MDS. (TOPSVR is used for DRAM-based directory assistance and intercept announcements. MDS is used for the TOPS Message Delivery Service feature, also known as Audiogram Delivery Service. Note that most MDS functionality disappeared with end of life of the VSN.)

This activity does not support use of packet-based media servers for music segments of audio programs used by the Music and Announcement in Queue feature.

When packet-based announcements are used for MCCS and ACTS, the media server does not collect the DTMF or coin signals. Collection is still done by an MCCS or ACTS receiver card in an MTM/ISM.

An interworking bridge is required in SN09 for each TOPS connection to a packet-based announcement.

The functionality provided by this feature will not be supported in international (ISN) loads until it has been verified. At this time of this publication, Nortel planned to verify it only for North America.

The functionality provided by this feature will not be supported in ATM-based hybrid solutions until it has been verified. At this time of this publication, Nortel planned to verify it only with an IP network fabric.

This activity is subject to all of the limitations and restrictions that apply in general to CS 2000 use of packetized announcements. This includes the capacity limitations of media servers and Audio Controller GWCs. Some of the other important restrictions that this activity inherits from CS 2000 in SN09 are:

- Use of packet-based announcements is not supported if the CS 2000 connects two or more packet bearer networks. Note that a Trimodal CS 2000 connects two packet bearer networks, so packet announcements cannot be used on a Trimodal CS 2000. The restriction applies regardless

of whether the two packet bearer networks have the same or different network fabrics.

- All of the media servers controlled by the same GWC must be provisioned with the same set of audio segments. Failure to follow this provisioning rule will result in call failures.

Please see the following section for additional interactions that could be viewed as limitations.

1.5 Interactions

The end user of a TOPS feature that uses announcements should detect virtually no difference in how the feature operates when packet-based announcements are used rather than legacy DRAM announcements. The one exception is that the media server may use different wording for certain variable phrases in custom announcements. The logic for the wording is in the media server, not in the switch. Specifically, when a time duration for ACTS is an even number of minutes, the switch instructs the DRAM to speak only "<x> minutes," but a packet media server may have logic to say "<x> minutes and zero seconds."

The MAXCYC field in CM table ANNS specifies the maximum number of times an announcement should repeat if the listening agent does nothing to terminate the connection. TOPS software has historically ignored the MAXCYC datafill for announcements played while a call is at an operator position or an OSSAIN service node. So, for example, if an operator requests to outpulse to a number and gets a treatment announcement, the announcement has historically continued to repeat itself until the operator keyed to release it. If the announcement member is a packet one, and if the operator does not key to release it before it has played the datafilled number of cycles, the announcement stops playing and the operator should key to release it at that time. The same is true for a packet announcement that is played to a call under control of an OSSAIN service node.

There are no interactions with the criteria by which an announcement is selected for a TOPS call. For example, the branding announcement CLLI for a TOPS call is selected based on criteria that may include the carrier or NBEC, the Service Provider ID (SPID), and datafill in several TOPS tables. All of this occurs before the announcement member is selected, and it happens independently of the network fabric of the member that will be selected.

1.6 Glossary

This activity does not introduce any non-standard terms or acronyms.

2: Fault Management for A00009013

2.1 Fault management strategy

This activity does not introduce any new element for which a fault management strategy is needed. It adheres to the existing fault management strategy for Succession announcements and for TOPS.

2.2 Fault management tools and utilities

Existing fault management tools and utilities for Succession announcements apply to the announcements for this activity.

2.2.1 Faults, Alarms and Logs

This activity makes minor changes in two existing legacy DMS logs.

2.3 Log: TOPS113

Log Title/Log ID: TOPS113

This is an existing legacy DMS log, documented in Log Report Reference Manual. The log can also be generated by the CS 2000 CM. This feature changes the fixed string in the Event Label field. This activity changes that string from

```
TOPS DRAM PLAY TRBL
```

to

```
ANNOUNCEMENT PLAY TRBL
```

2.3.1 Formats

2.3.1.1 NTSTD

Format:

```
<Office Id>     TOPS113 <MMMDD hh:mm:ss> <seq #> INFO ANNOUNCEMENT PLAY TRBL
        CKT <trkid>
        CHECK FOR INCOMPLETE DATAFILL IN TABLE ANNPHLST
```

Example:

```
RTPC09AZ     TOPS113 JAN03 01:16:53 7985 INFO ANNOUNCEMENT PLAY TRBL
        CKT         TOPCOMAMF 0
        CHECK FOR INCOMPLETE DATAFILL IN TABLE ANNPHLST
```

2.3.1.2 SCC2

Standard for CM.

2.3.1.3 Syslog

N/A

2.3.1.4 SNMP

N/A

2.3.1.5 Integrated Element Manager GUI Fields

N/A

2.3.2 Explanation

Unchanged.

2.3.3 Field descriptions

Unchanged.

2.3.4 Action

Unchanged.

2.3.5 Associated Operational Measurements or Performance Measurements

Unchanged.

2.3.6 Additional information

In SN06 the last line of the log body was changed from

```
CHECK FOR INCOMPLETE DATAFILL IN TABLE DRMUSERS
```

to

```
CHECK FOR INCOMPLETE DATAFILL IN TABLE ANNPHLST
```

This was done under a CR and was not documented in NTPs. The reason for the change was that activity A19013546 introduced table ANNPHLST, which replaced table DRMUSERS. All NTP references to DRMUSERS in the description of this log should be changed to refer to ANNPHLST.

2.4 Log: TOPS104

Log Title/Log ID: TOPS104

This is an existing legacy DMS log, documented in Log Report Reference Manual. The log can also be generated by the CS 2000 CM. The only change made by this activity is in the TROUBLE CODE field.

2.4.1 Formats

2.4.1.1 NTSTD

Format:

```
<Office Id>     TOPS104 <MMMDD hh:mm:ss> <seq #> INFO ACTS TROUBLE
        CKT <trkid1>
        CKT <trkid2> CKT <trkid3> CKT <trkid4>
        INCOMING TRK = CKT <trkid>
        OUTGOING TRK = CKT <trkid>
        CLGNO = <dn> CLDNO = <dn>
        TROUBLE CODE = <trouble text>
```

Example:

```
RTPC09AZ     TOPS104 APR01 12:00:00 2112 INFO ACTS TROUBLE
   CKT          ACTSTOPS 111
   CKT         ACTSTOPS 111 CKT         ACTSTOPS 111 CKT         RCVRCOIN 12
   INCOMING TRK = CKT          LNTOPSI  4
   OUTGOING TRK = CKT          LNTOPSO  4
   CLGNO = 613-621-1002         CLDNO = 212-220-1111
   TROUBLE CODE = MISCELLANEOUS_ACTS_TRBL
```

2.4.1.2 SCC2

Standard for CM.

2.4.1.3 Syslog

N/A

2.4.1.4 SNMP

N/A

2.4.1.5 Integrated Element Manager GUI Fields

N/A

Table 7: NTSTD/SCC2 Optional Header Fields

Field Name	Used (Y/N)	Value	Fixed/ Variable	type	size	Description
Event Label	Y	ACTS TROUBLE	Unchanged; see Log Report Reference Manual.			
Equipment ID	N					

Table 8: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
Other fields are unchanged.				

Table 8: Log Body Fields

Field Name	Used (Y/N)	Value(s)	Fixed/ Variable	Description
TROUBLE CODE	Y	CDC_DSP1_FAIL CDC_DSP2_FAIL CDC_DSP3_FAIL CDC_RAM_FAIL CDC_ROM_FAIL CDC_TRAP MISCELLANEOUS_ACTS_TRBL MISC_CDC_FAIL MISC_ANNOUNCEMENT_FAIL RECEIVER_SUSPECTED		Indicates the trouble.

2.4.2 Explanation

The Traffic Operator Position System (TOPS) subsystem generates this report when the operator keys “suspect CDC” trouble at the operator position, or when unexpected messages are received from the coin detector circuit (CDC), the digital recorded announcement machine (DRAM) cards, or the packet media server (UAS or MS 2000 Series).

2.4.3 Field descriptions

The TROUBLE CODE field is the only one changed by this activity.

Table 9: Field descriptions

Field	Value	Description
TROUBLE CODE	NO_REPLY_FROM_DRAM	This value can no longer be generated.
TROUBLE CODE	MISC_DRAM_FAIL	This value can no longer be generated.
TROUBLE CODE	MISC_ANNOUNCEMENT_FAIL	Indicates a miscellaneous problem with an announcement used for an ACTS call. Probably an unexpected message has been received from the announcement machine. When this trouble code is generated, the TOPS104 log is most often accompanied by another log that provides more detailed information.
TROUBLE CODE	*other values*	The meaning of the other values is unchanged. See Log Report Reference Manual.

2.4.4 Action

Most often this log indicates a hardware problem, and the action is to diagnose the indicated circuit cards from the MAP (maintenance and administration position) and replace cards if necessary. The first CKT field in the log body is the agent reporting the problem.

If the agent reporting the problem is an ACTS announcement, check for other logs that may accompany this one and may provide more specific information. If the problem cannot be diagnosed using other logs, then check CM table ANNMEMS to determine whether it is a DRAM announcement (HDWTYPE = DRAM) or a packet announcement (HDWTYPE = UAS). Packet announcement members do not correspond to specific hardware circuits. Table ANNMEMS will identify the logical AUD node that was controlling the announcement, and table SERVSINV will associate that AUD node with a Gateway Controller. Follow standard troubleshooting procedures for the media servers that are controlled by that Gateway Controller.

2.4.5 Associated Operational Measurements or Performance Measurements

Unchanged.

2.5 Alarms

N/A

2.6 Related documentation

Log Report Reference Manual.

3: Configuration for A00009013

3.1 Hardware and Software Requirements

This activity has the following prerequisite requirements:

- Hybrid Communication Server 2000 (CS 2000) with ENET and IP network fabrics
- Interworking Spectrum Peripheral Module(s) (IW SPM IP)

  Note: An interworking bridge is required for each connection of a TOPS call to a packet announcement.
- Gateway Controller(s) (GWC) configured with Audio Controller profile
- Media Server 2010 (MS 2010) or Universal Audio Server (UAS) media server(s)
- Succession element managers for maintenance of the above components. This includes the Announcement Provisioning Server (APS).
- TOPS equipment (such as operator positions)

In an office that is migrating from DRAM-based announcements to packet-based announcements for TOPS, datafill for the applications that use the announcements (for example, Branding or ACTS) will already be present when the migration begins. For new offices, that datafill will not be present, and it may be added after the announcements have been provisioned. This DDOC does not attempt to re-document the data schema for all of the TOPS applications that use announcements. Refer to your Translations Guide (297-nnnn-350) and Data Schema Reference Manual (297-nnnn-351) for more information about basic TOPS datafill.

The following documents include other important prerequisite configuration information.

Table 10: References for Configuration Prerequisites

Document Number	Title
NN10193-511	Communication Server 2000 Configuration Management
NN10100-511	IW SPM IP Configuration Management
NN10205-511	Gateway Controller Configuration Management
NN10095-511	Universal Audio Server Configuration Management
NN10323-111	Media Server 2000 Series Basics
NN10340-511	Media Server 2000 Series Configuration Management
See Helmsman for other related documentation.	

3.2 Initial Configuration

This section assumes, for the most part, that the office is already using DRAM-based announcements for TOPS and is migrating some or all of the TOPS applications to use packet-based announcements. For new TOPS offices, it is necessary to consult both this document and the NTPs that explain the TOPS applications.

3.2.1 Basic configuration steps

The steps for configuring packet-based announcements for TOPS are as follows:

1. Determine what audio segments will be needed for the TOPS applications, and what voice content you want the segments to have.

   For **standard announcements** (ANTYPE = STND in CM table ANNS) this is straightforward. If you are migrating from DRAM-based to packet

announcements, you will want to identify and determine the content of the standard announcements already in use.

The number of standard announcements in the office may be small enough that you can look at table ANNS and immediately know how each of the standard announcements is used. Otherwise, look in the following tables.

— CLLIs for SPID-based branding announcements are datafilled in the TAANN and DAANN fields of CM table SPIDDB.

— CLLIs for carrier-based and NBEC-based branding announcements are datafilled in the TAANN, DAANN, and CDANN fields of CM table BRANDANN.

— Announcement CLLIs for Music and Announcement in Queue are datafilled with the ANN selector in the route lists of tuples in CM table TOPAUDIO.

— TOPS-specific treatment announcement CLLIs are datafilled in subtable TREAT of the TOPSTKGP tuple of CM table TMTCNTL. Depending on the office configuration, the OFFTREAT tuple may be used for TOPS calls, or tuples for other trunk group types may be used.

Once the announcement CLLIs are known, determine the external phrase names that are associated with them. To do this in an existing TOPS office, consult table ANNMEMS for the DRAM track number(s), and then look in table ANNPHLST for the mapping from CLLI + track number to a list of external phrase names. Each of these phrase names must have a segment provisioned on the packet media servers.

Note: Packet-based announcement members cannot have multiple tracks datafilled in the CM. Refer to the Configuration Guide for your media server for information about configuring the media server itself to play announcements in multiple languages.

If you want to hear the content that a DRAM plays for a phrase, look in table DRAMPHRS to determine where the phrase is stored on the DRAM. Then use the DRAMREC utility to listen to the recording that is currently in use.

For **custom announcements** (ANTYPE other than STND in table ANNS), determining what segments need to be recorded for the media servers can be a little harder. This is partly because some of the announcement numbers and phrase names for custom announcement applications are pre-determined by Nortel, while others may be defined by the operating company. Also, custom announcements can use placeholder phrase names, and these are handled differently for packet-based announcements than for DRAM announcements. Refer to “TOPS custom announcement considerations” on page 2075 for specific information about determining the segments that must be provisioned on the media servers for ACTS and MCCS.

2. Record the phrases that were determined in step 1 to be needed, or have them professionally recorded. Refer to the Configuration Management

document for your media server for information about the required format.

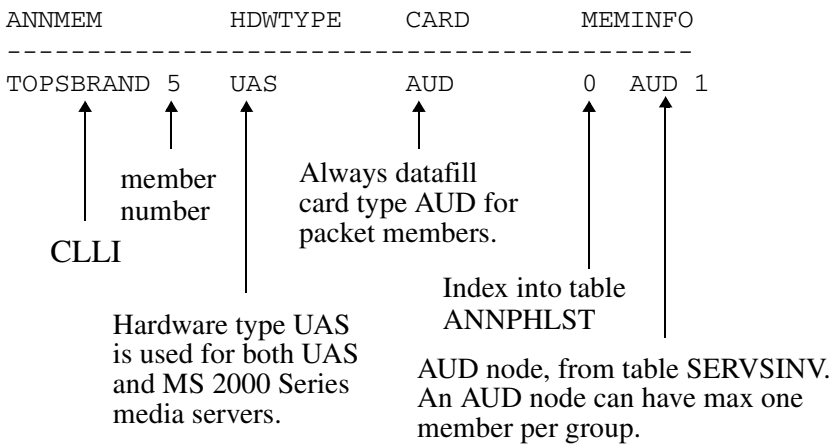
3. Upload the audio files to the Announcement Provisioning Server (APS), and import corresponding physical segments into the APS database. Note the segment ID associated with each. Refer to “Media Server 2000 Series Configuration Management” for more information.
4. Ensure that the segments are made available to all appropriate media servers.

   Note: You must provision the same set of audio segments for all media servers controlled by the same GWC.
5. In CM table ANNAUDID, associate the MS 2000 / UAS audio segment ID with each external announcement phrase name that will be used with this feature.
6. Ensure that CM tables CLLI, ANNS, ANNMEMS, and ANNPHLST are correctly datafilled for the announcements that will use this feature. They should be datafilled in that order.
   - CLLI - Datafill the CLLI codes for the announcements.

     This table will already be datafilled if you are migrating from DRAM to packet announcements. In that case, no changes are needed.
   - ANNS - Specify the characteristics of the announcement groups.

     This table will already be datafilled if you are migrating from DRAM to packet announcements. In that case, no changes are needed.
   - ANNMEMS - Specify the announcement members.

     Add member tuples for all the announcements that will use packet-based media servers. The following figure shows an example.



The index into table ANNPHLST applies only to standard announcements type. It is present but ignored for custom announcement types.

Normally, all packet members of a standard announcement group are datafilled with the same index into table ANNPHLST. If the group also has DRAM members, the index for the packet members may or may not be the same as one of the track numbers of a DRAM member tuple. If it is the same, then the DRAM and AUD members will share a tuple in table ANNPHLST. If it is different, a tuple for the new index must be added to table ANNPHLST.

Note: For custom announcements, it is not possible for DRAM and packet members to use different tuples in table ANNPHLST.

— ANNPHLST - Specify the list of external phrase names that make up the announcement.

For custom announcement types, table ANNPHLST is indexed by the announcement CLLI and the application-specific custom announcement number. For standard DRAM announcements, it is indexed by the CLLI and track number. For standard packet announcements, it is indexed by the CLLI and the phrase list index from table ANNMEMS.

If you are migrating from DRAM-based to packet announcements for TOPS, and if you datafilled table ANNMEMS so that packet and DRAM members of standard announcement groups share the same ANNPHLST tuple, then table ANNPHLST needs no additional datafill.

If you are datafilling TOPS announcement applications from scratch, or if you are migrating but datafilled table ANNMEMS so that packet and DRAM members of a standard announcement group would not share the same ANNPHLST tuple, then datafill must be added to table ANNPHLST. A tuple is needed for each standard announcement member that has its own phrase list index, and for each custom announcement used by supported custom announcement applications (ACTS, MCCS).

Refer to your Translations Guide, Customer Data Schema Reference Manual, and later sections of this document for more information about datafilling table ANNPHLST.

7. Run TABAUDIT on tables ANNS, ANNMEMS, ANNPHLST, and ANNAUDID, and correct any errors found.
8. Ensure that the TOPS applications that are to use packet announcements are fully datafilled, if you are adding new applications rather than migrating existing ones. Refer to your Translation Guide and Customer Data Schema Reference Manual for more information about TOPS application datafill.

9. Bring new packet announcement members into service. This is done at the TTP level of the Maintenance and Administration Position (MAP) in the CM. If the Gateway Controller and/or the media servers are not in service, they must first be returned to service using CS 2000 OAM&P tools.

   Note: It is strongly recommended that test calls be made using the packet announcement members. See "Verifying provisioning" on page 2075 for more information.

10. For at least several days, monitor the applications carefully. Look for the following switch logs, which may indicate provisioning problems: XPKT340, TOPS104, and TOPS113. Also monitor logs and alarms on the media servers themselves. Procedures for doing that are described in the Fault Management document (NNnnnnn-911) for your media server.

3.2.2 Verifying provisioning

When commissioning new TOPS applications that use only packet-based announcements, it is strongly recommended that test calls be made before general TOPS traffic is routed to the announcements.

Test calls should also be made when migrating from DRAM-based to packet-based announcements for TOPS. To minimize the impact of the testing on live calls, the testing must be done at a time of very low traffic. The only way to ensure that a test call will get a packet announcement member is to busy out all DRAM members of the announcement group.

Specific provisioning problems that can cause trouble include (a) failure to provision all of the required phrases on some or all of the media servers, (b) mismatches between the segment identifiers provisioned on the media servers and the ones datafilled in CM table ANNAUDID, (c) failure to add an ANNAUDID tuple for some phrase name that the application uses, (d) failure to add an ANNPHLST tuple for an announcement member that the application uses, and (e) failure to provision the announcement ports on the media server.

Because of the potential disruptiveness of making test calls in a live office that is migrating from DRAM-based to packet-based announcements, it is important to check and double-check the provisioning before bringing packet members into service.

3.2.3 TOPS custom announcement considerations

To plan the audio segments that will be provisioned on the media servers for custom announcement applications such as MCCS and ACTS, it is useful to think backwards from the order in which the provisioning is actually done.

1. First, identify the announcements (announcement numbers) that the application uses. Both MCCS and ACTS predefine most of their announcement numbers, but both allow the operating company to define additional announcement numbers.

2. Second, determine the list of external phrase names that the CM uses (if migrating), or will use (if configuring the new application from scratch), for each of these announcement numbers. Nortel provides detailed recommendations on external phrase name lists to use for the pre-defined MCCS and ACTS announcement numbers. The operating company determines the phrase names for announcement numbers that the operating company defines. Also, the operating company may want to define some of its own phrase names to use with some of the pre-defined MCCS and/or ACTS announcement numbers, rather then using only the phrase names that Nortel suggests. If both legacy and packet members are used for the application, bear in mind that the CM uses the same external phrase name lists for both legacy and packet members.
3. Third, determine the content that will correspond to each phrase name. Nortel provides specific content suggestions for the phrase names that we recommend for the pre-defined announcement numbers. The operating company may choose to record different content, and in any case, the operating company must determine the content for MCCS and ACTS announcements that the operating company defines.
4. Plan the provisioning of audio segments on the media servers. As described in the subsections below, there may not be a one-to-one relationship between physical audio segments on the media servers and phrase names datafilled in the CM. For ACTS, you must take into account the way variable substitution works for placeholder phrases.

When the above steps have been completed, configuration continues as described in “Basic configuration steps” on page 2071. The following subsections provide more detail about MCCS and ACTS.

3.2.3.1 MCCS

Refer to Table 11 on page 2085 for a concise summary of the pre-defined MCCS announcement numbers. For each pre-defined announcement number, the table shows suggested phrase names and content for the phrases.

The operating company can define additional MCCS announcement numbers that are used to brand the “thank-you” acknowledgment for correct card number entry. These operating company defined MCCS announcement numbers are datafilled in CM tables EAMCCSAN and MCCSNBEC.

If you are migrating from DRAM-based to packet-based announcements for MCCS, the easiest way to determine all the phrase names used for MCCS is to consult the MCCS tuples already datafilled in table ANNPHLST. If MCCS is being initially commissioned in the office, however, table ANNPHLST will be datafilled only after the audio segments have been provisioned on the media servers and datafilled in table ANNAUDID and other announcement tables.

MCCS does not use placeholder phrase names. Every phrase name in an MCCS tuple of table ANNPHLST must be mapped in table ANNAUDID to a segment identifier that will be sent to the media server when the corresponding announcement is to be played. MCCS has no requirement for media server provisioning for variable substitution.

The most straightforward way—but not necessarily the best way—to provision the media servers for MCCS is with a single, separate audio file for each MCCS phrase defined in the CM. This would mirror the way MCCS works with DRAMs. Alternatively, it is possible to save space on the media servers by decomposing some of the MCCS announcements into sub-phrases. Each sub-phrase would be a separate voice file on the media servers, and would have its own physical segment ID. A sequence type segment would then be defined in the APS to identify the sequence of physical segments that constitute the announcement. The segment ID of the sequence would be the one datafilled in CM table ANNAUDID against the MCCS external phrase name. The fact that the media server constructs the announcement from a sequence of physical segments would be transparent to the CM. For more information about using audio sequences, refer to "Media Server 2000 Series Configuration Management."

3.2.3.2 ACTS

Table 13 on page 2089 summarizes the pre-defined ACTS announcement numbers. For each pre-defined announcement number, the table explains when the announcement is used and shows a list of suggested phrase names for the announcement. Content for the non-variable phrase names is suggested in Table 14 on page 2092.

The operating company can define additional ACTS announcement numbers that are used to brand the initial correct deposit and initial overdeposit "thank-you" acknowledgments for coin calls. These operating company defined ACTS announcement numbers are datafilled in CM tables SPIDDB, EAACTSAN and ACTSNBEC.

Because ACTS uses placeholder phrases, it is not possible for migrating offices to determine all the phrase names that ACTS uses simply by consulting existing datafill in table ANNPHLST. The remainder of this section is primarily concerned with how placeholder variable substitution works for ACTS, and the implications for provisioning the media servers. Provisioning the media servers is compared and contrasted to provisioning DRAMs for ACTS.

ACTS pre-defines four placeholder, or variable, phrase names in the CM. These are used for

- monetary amounts (ACTS_VAR_CHARGE and ACTS_VAR_CREDIT),
- time durations (ACTS_VAR_PERIOD), and

- coin denominations (ACTS_VAR_COIN).

The placeholder phrase names are not datafilled in table DRAMPHRS (legacy) or ANNAUDID (packet), and they do not directly correspond to recordings provisioned on DRAMs or media servers.

During call processing, the placeholder phrase names are resolved using call-specific information. For coin denominations (used only by the ACTS Coin Tone Generation Test feature), variable substitution works in much the same way for packet and legacy announcement members. For monetary amounts and time durations, variable substitution works very differently for packet members.

Coin denominations

Placeholder phrases for the ACTS Coin Tone Generation Test feature are handled in much the same way for packet members as for DRAM members. Internal logic in the CM maps the placeholder phrase ACTS_VAR_COIN to one of the pre-defined phrase names shown below:

Phrase Name	Recommended Content
ACTS_NICKEL	“nickel”
ACTS_DIME	“dime”
ACTS_QUARTER	“quarter”
ACTS_DOLLAR	“dollar”

The CM then looks in table ANNAUDID (if a packet member was selected) or DRAMPHRS (if a legacy member was selected), and it expects to find a mapping from that pre-defined phrase name to an audio ID that it will send to the announcement server. Therefore, if the ACTS Coin Tone Generation Test feature is used, the media servers must be provisioned with segments that play the content shown in the table above.

Charges and credits

Resolution of placeholder phrases ACTS_VAR_CHARGE and ACTS_VAR_CREDIT is handled differently for packet members than for DRAM members. For DRAM members, the CM resolves a monetary amount to a phrase list such as, for example, ACTS_1, ACTS_DOLLAR, ACTS_AND, ACTS_15, ACTS_CENTS, and it sends the DRAM a list of internal phrase IDs corresponding to the pre-defined phrases in the list. Therefore, when DRAM members are used, the CM requires datafill in table DRAMPHRS for all of the pre-defined phrases to which it can resolve monetary placeholders.

For packet members, the CM does not resolve monetary amounts to their constituent phrases, and it does not require datafill in table ANNAUDID of audio IDs for the constituent phrases. Instead, the CM sends the media server a higher-level message specifying that it should play a monetary amount and providing the currency (U.S. dollars) and the amount.

The media server executes the logic to resolve the monetary amount into physical phrases. To do this, it requires that recordings for the constituent phrases it can use for money be placed in audio files with pre-defined names. The pre-defined file names are the same for MS 2000 and UAS, and they are documented in "Media Server 2000 Series Configuration Management." Only files for the default language need to be provisioned, as ACTS does not support sending language selectors to the media server.

Time durations

The placeholder phrase ACTS_VAR_PERIOD is also handled differently for packet members than for DRAM members. For DRAM members, the CM breaks down the time duration into a sequence of constituent phrases such as ACTS_3, ACTS_MINUTES, and it sends a list of internal phrase identifiers corresponding to these phrase names to the DRAM. Therefore, the CM requires datafill in table DRAMPHRS for all of the pre-defined phrases to which it can resolve ACTS_VAR_PERIOD.

For packet members, the CM does not resolve time durations to their constituent phrases, and it does not require datafill in table ANNAUDID of audio IDs for the constituent phrases. Instead, the CM sends the media server a higher-level message specifying that it should play a duration and specifying the amount of time.

The media server executes the logic to resolve the duration to a list of physical phrases. To do this, it requires that recordings for the constituent phrases it can use for durations be placed in audio files with pre-defined names. The pre-defined file names are the same for MS 2000 and UAS, and they are documented in "Media Server 2000 Series Configuration Management." Only files for the default language need to be provisioned, as ACTS does not support sending language selectors to the media server.

Silence

With DRAMs, pauses in the announcement require audio files that contain silence. The phrase name ACTS_PAUSE is typically used for this, and it requires mapping in table DRAMPHRS to an internal phrase number that identifies a recording of silence on the DRAM.

ACTS_PAUSE is not a placeholder phrase name, and if it is used in a phrase list for ACTS, it requires datafill in table ANNAUDID. The CM sends the media server a segment ID the same way it does for most other phrases. However, it is possible to provision the media server in a way that avoids using

space to store a recording of silence. Refer to “Media Server 2000 Series Configuration Management” for information about provisioning variable-type segments with provisioned values. A variable segment of type silence could be provisioned and associated with a selector that has a provisioned value that determines the duration of the silence. This would be transparent to the logic in the CM.

3.3 Office/Subnet parameters (OP/SP) (CM & SESM)

No impact.

3.4 Upgrade Considerations

3.4.1 Dump and Restore (CM)

No impact.

3.4.2 Element Management Upgrade

No impact.

3.4.3 Downgrade impact

No impact.

3.5 Data schema (DS) (CM)

3.5.1 New/modified tables

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
ANNMEMS	CHANGED	UNCHANGED
ANNPHLST	The table is not changed, but its documentation is.	UNCHANGED

3.5.2 Table Database Schema information

3.5.2.1 Name: ANNMEMS

Announcement Members Table

3.5.2.1.1 Functional description

Unchanged.

3.5.2.1.2 Usage sequence and implications (CM Only)

Unchanged.

3.5.2.1.3 Size
Unchanged.

3.5.2.1.4 Fields
Unchanged, but note that for custom announcement members with hardware type UAS, the PHLSTIDX field is ignored. This field is present for all members datafilled with HDWTYPE UAS, but it is consulted only if the announcement CLLI is datafilled as STND in table ANNS.

3.5.2.1.5 Datafill example
Unchanged.

3.5.2.1.6 Table release history update
As of SN09, packet members cannot be datafilled for a custom announcements of type TOPSVR or MDS.

Also, documentation of the meaning of the PHLSTIDX field for custom announcement types with hardware type UAS is clarified. (This is not a functional change.)

3.5.2.1.7 Supplementary information
Packet announcement members (HDWTYPE = UAS) are not supported for custom announcements of type MDS or TOPSVR. If a UAS member is datafilled for an announcement that is datafilled in table ANNS with ANTYPE = MDS or TOPSVR, one of the following warning messages is displayed:

```
Packet members are not supported for ANNTYPE MDS
Packet members are not supported for ANNTYPE TOPSVR
```

3.5.2.1.8 Translation verification and other tools
Unchanged.

3.5.2.2 Name: ANNPHLST
Announcement Phrase List Table

3.5.2.2.1 Functional description
Unchanged.

3.5.2.2.2 Usage sequence and implications (CM Only)
Unchanged.

3.5.2.2.3 Size
Unchanged.

3.5.2.2.4 Fields/OIDs
Unchanged.

3.5.2.2.5 Datafill examples

Mechanized Calling Card Service

Example datafill for MCCS appears below. The example assumes that the CLLI name datafilled in table ANNS for MCCS is MCCSTOPS. It also assumes that you are using the suggested phrase names shown in Table 11 on page 2085, and that you are not defining additional MCCS announcements in table EAMCCSAN or MCCSNBEC.

```
ANNPHKEY          PHSLIST
-----------------------------------------
MCCSTOPS 1        MCCSENG1 $
MCCSTOPS 2        MCCSENG2 $
MCCSTOPS 3        MCCSENG3 $
MCCSTOPS 4        MCCSENG4 $
MCCSTOPS 5        MCCSENG5 $
MCCSTOPS 6        MCCSENG6 $
MCCSTOPS 7        MCCSENG7 $
MCCSTOPS 8        MCCSENG8 $
MCCSTOPS 9        MCCSENG9 $
MCCSTOPS 15       MCCSENG15 $
MCCSTOPS 16       MCCSENG16 $
MCCSTOPS 17       MCCSENG17 $
MCCSTOPS 18       MCCSENG17 $
MCCSTOPS 19       MCCSENG17 $
MCCSTOPS 20       MCCSENG9 $
MCCSTOPS 21       MCCSENG9 $
MCCSTOPS 22       MCCSENG16 $
MCCSTOPS 23       MCCSENG5 $
```

Automatic Coin Toll Service

Example datafill for ACTS appears below. The example assumes that the CLLI name datafilled in table ANNS for ACTS is ACTSTOPS. It also assumes that you are using the suggested phrase names shown in Table 13 on page 2089,

and that you are not defining additional ACTS announcements in table SPIDDB, EAACTSAN, or ACTSNBEC. .

```
ANNPHKEY        PHSLIST
---------------------------------------
ACTSTOPS 1      (ACTS_VAR_CHARGE)(ACTS_PLEASE)(ACTS_PAUSE)
                (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_FOR_FIRST)
                (ACTS_VAR_PERIOD) $
ACTSTOPS 2      (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
ACTSTOPS 3      (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_MORE) $
ACTSTOPS 4      (ACTS_THANK_YOU) $
ACTSTOPS 5      (ACTS_THANK_HAVE)(ACTS_VAR_CREDIT)(ACTS_CR_OVERTIME) $
ACTSTOPS 6      (ACTS_ALERT)(ACTS_VAR_PERIOD)(ACTS_END_SIGNAL) $
ACTSTOPS 7      (ACTS_ALERT)(ACTS_VAR_CHARGE)(ACTS_PLEASE)
                (ACTS_PAUSE)(ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)
                (ACTS_FOR PAST)(ACTS_VAR_PERIOD) $
ACTSTOPS 8      (ACTS_ALERT)(ACTS_VAR_CHARGE)(ACTS_PLEASE)(ACTS_PAUSE)
                (ACTS_YOU_HAVE)(ACTS_VAR_CREDIT)(ACTS_CREDIT)
                (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)
                (ACTS_MORE)(ACTS_FOR_PAST)(ACTS_VAR_PERIOD) $
ACTSTOPS 9      (ACTS_ALERT)(ACTS_CHARGES_ARE)(ACTS_VAR_CHARGE)
                (ACTS_PLUS_TAX)(ACTS_VAR_PERIOD) $
ACTSTOPS 10     (ACTS_ALERT)(ACTS_VAR_PERIOD)(ACTS_HAS_ENDED) $
ACTSTOPS 11     (ACTS_PLS_DEPOSIT)(ACTS_1)(ACTS_VAR_COIN) $
ACTSTOPS 12     (ACTS_PAUSE)(ACTS_ALERT) $
ACTSTOPS 13     (ACTS_THANK_YOU)(ACTS_VAR_COIN)(ACTS_TST_ENDED) $
ACTSTOPS 14     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
ACTSTOPS 15     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
ACTSTOPS 16     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_MORE) $
ACTSTOPS 17     (ACTS_THANK_YOU) $
ACTSTOPS 18     (ACTS_THANK_HAVE)(ACTS_VAR_CREDIT)(ACTS_CR_OVERTIME) $
ACTSTOPS 19     (ACTS_ALERT)(ACTS_CHARGES_ARE)(ACTS_VAR_CHARGE)
                (ACTS_PLUS_TAX)(ACTS_VAR_PERIOD) $
ACTSTOPS 20     (ACTS_ALERT)(ACTS_VAR_CHARGE)(ACTS_PLEASE)(ACTS_PAUSE)
                (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_FOR_NEXT)
                (ACTS_VAR_PERIOD) $
ACTSTOPS 21     (ACTS_ALERT)(ACTS_VAR_CHARGE)(ACTS_PLEASE)(ACTS_PAUSE)
                (ACTS_YOU_HAVE)(ACTS_VAR_CREDIT)(ACTS_CREDIT)
                (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE)(ACTS_MORE)
                (ACTS_FOR_NEXT)(ACTS_VAR_PERIOD) $
ACTSTOPS 22     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
ACTSTOPS 23     (ACTS_PLS_DEPOSIT)(ACTS_VAR_CHARGE) $
```

3.5.2.2.6 Table release history update

The explanations and example datafill for custom announcement types MCCS and ACTS were updated in SN09, to correct errors and to document that these applications can use either DRAM or packet announcement resources.

The information about custom announcement type AOSSVR was removed in SN09. This application was specific to TOPS MP positions, which are no longer supported.

3.5.2.2.7 Supplementary information

Mechanized Calling Card Service

MCCS is a TOPS custom announcement type. Although the DMS250 also supports an MCCS application, that application uses standard announcements. This section applies to TOPS MCCS.

MCCS announcements can be provided by DRAMs or by packet-based media servers in a hybrid solution with IP and ENET fabrics. The Media Server 2010 (MS 2010) and the Universal Audio Server (UAS) are examples of media servers.

For DRAMs, MCCS announcements can take the form of prerecorded phrases on two NT1X76CA double density erasable programmable read-only memory (EPROM) cards. Alternatively, an operating company can record its own DRAM announcements for MCCS. Use the DRAMREC CI to define phrases on a DRAM. All MCCS announcements are single-track.

For packetized MCCS announcements, the operating company provides the recordings and provisions them on the media servers using the Announcement Provisioning Server (APS). After that, tables ANNAUDID, CLLI, ANNS, ANNMEMS, and ANNPHLST must also be datafilled in the CM.

MCCS provides no secondary language support in the CM. An operating company can provide bilingual MCCS announcements by recording the announcements in both languages. For DRAMs, since MCCS announcements are single-track, both languages must be recorded on the same track. For packet-based MCCS announcements, a sequence can be created using the APS.

In addition to basic calling card validation, the MCCS custom announcement type can be used for sequence call prompts and for the TOPS Authorization Code and Account Code Billing features.

MCCS pre-defines custom announcement numbers 1 through 9 and 15 through 23. It reserves 10 through 14 for future development. Through datafill in tables EAMCCSAN and/or MCCSNBEC, the operating company can specify that announcement numbers 24 and higher are to be used to brand the initial "thank-you" acknowledgment for correct card entry.

MCCS does not use any variable, or placeholder, phrase names. Nortel suggests, but does not require, that the operating company use phrase names shown in Table 11 for MCCS announcements. The table shows the pre-defined MCCS announcement numbers, the scenario in which each is used, the suggested phrase name for each (assuming the language is English), and suggested content for each. The table shows the announcement numbers in an order that is logical in terms of call flow, rather than listing them in order by announcement number. The table uses the following abbreviations:

CCV	Calling Card Validation
SEQ	Sequence calling
ACB	Account Code Billing
AUTH	Authorization Code

Table 11: Pre-defined MCCS Announcements with Suggested Content

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List	Suggested Content
17	Initial prompt for CCV and ACB if originating station treatment (OST) from table MCCSOST is TONE. Also used as the initial and retry prompt for AUTH.	MCCSENG17	Alert tone ("bong") for calling card dialing. This is a complex tone consisting of 60 ms DTMF #-tone (941/1477 Hz @ -10 dBm), followed immediately by 940 ms of exponentially decayed dial tone (440/350 Hz with time constant of 200 ms initially at -10 dBm)
18	Initial prompt for CCV and ACB if originating station treatment (OST) from table MCCSOST is TONEANN.	MCCSENG17	
1	Re-prompt for CCV and ACB when initial prompt was announcement 18 (OST = TONEANN) and timeout occurred.	MCCSENG1	Please dial your card number or zero for an operator now.

Table 11: Pre-defined MCCS Announcements with Suggested Content

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List	Suggested Content
2	Re-prompt for CCV and ACB if caller entered an invalid card number (CCV) or invalid account code (ACB).	MCCSENG2	Please dial your card number again now. The card number you have dialed is not valid.
19	Re-prompt when timeout occurs after caller has heard announcement 2.	MCCSENG17	
3	Re-prompt when timeout occurs after caller has heard announcement 19.	MCCSENG3	Please dial your card number.
9	Re-prompt when timeout occurs after caller has heard announcement 3.	MCCSENG9	Please hang up and dial zero plus the number you are calling.
4	Sign-off message for CCV when caller has entered too many invalid card numbers.	MCCSENG4	Please hang up and dial zero plus the number you are calling. (pause) The card number you have dialed is not valid.
16	Announcement played when card number (CCV) or account code (ACB) has been successfully validated.	MCCSENG16	Thank you.
The following MCCS announcements are used only for sequence calls.			
5	Prompt when # is entered, initiating a sequence call.	MCCSENG5	You may dial another call now.
23	Re-prompt when timeout occurs after announcement 5.	MCCSENG5	
20	Sign-off message when timeout occurs after announcement 23.	MCCSENG9	
6	Re-prompt when caller enters an incorrect number in response to announcement 5.	MCCSENG6	Please dial the number you are calling again now. The number you have dialed is not correct.
7	Re-prompt when timeout occurs after announcement 6.	MCCSENG7	Please dial the number you are calling.
21	Sign-off announcement when timeout occurs after announcement 7.	MCCSENG9	
8	Sign-off announcement when caller has entered too many incorrect numbers for a sequence call.	MCCSENG8	Please hang up and dial zero plus the number you are calling. The number you have dialed is not correct.

Table 11: Pre-defined MCCS Announcements with Suggested Content

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List	Suggested Content
15	The number dialed is restricted for sequence calling.	MCCSENG15	Please hang up and dial direct. This number cannot be dialed as a sequence call.
22	Announcement played when caller has entered a correct number for a sequence call.	MCCSENG16	
Note: MCCS announcement numbers 10 through 14 are reserved for future development. ***Note:*** MCCS announcement numbers higher than 23 may be used to brand the initial thank-you acknowledgment by carrier or NBEC. The datafill for that is in tables EAMCCSAN and MCCSNBEC.			

Note that for some phrases, Table 11 lists the same phrase name against several different announcement numbers or scenarios. The table shows the suggested content only once for each phrase name. The operating company can provision different phrases for some of the announcements that share the same phrase name in the table above. To do that,

- First record the new announcement on the DRAM(s) or provision it on the media servers.
- Then add datafill to table DRAMPHRS (using the DRAMREC CI) or ANNAUDID (manually) mapping a new phrase name defined by the operating company to the internal ID provisioned on the announcement server.
- Finally, datafill the new phrase in table ANNPHLST against the CLLI used for MCCS and the new MCCS announcement number.

Note also that Table 11 shows a relatively inefficient scheme for using announcement store. It is based on the pre-recorded announcements that Nortel provides for DRAMs. If you do not plan to use these pre-recorded announcements, you may want to break out some of the sub-phrases that appear multiple times into their own phrases. For example, the sub-phrase “Please hang up and dial zero plus” appears in several different phrases. A separate recording could be created for that, and it could be included in the phrase lists for all of the announcements that begin that way.

If packet announcements are used for MCCS, the scheme for phrase names shown is Table 11 can be efficient if the media server is provisioned with audio sequences for the announcements that contain common phrases. The sequence identifier is then the one datafilled in table ANNPHLST.

If both DRAM and packet members are used for MCCS (or for any other custom announcement type), be aware that the two kinds of members share the same tuple in table ANNPHLST.

Automatic Coin Toll Service

ACTS is a TOPS custom announcement type that can be used for coin call automation and also for the TOPS Time and Charges, Non-coin Notification, and TOPS Coin Tone Generation Test features.

ACTS announcements can be provided by DRAMs or by packet-based media servers in a hybrid solution with IP and ENET fabrics. The Media Server 2010 (MS 2010) and the Universal Audio Server (UAS) are examples of media servers.

For DRAMs, ACTS announcements can take the form of prerecorded phrases on circuit pack NT1X76AE. Alternatively, an operating company can record its own DRAM announcements for ACTS. Use the DRAMREC CI to define the phrases on a DRAM. All ACTS announcements are single-track.

For packetized ACTS announcements, the operating company provides the recordings and provisions them on the media servers using the Announcement Provisioning Server (APS). After that, tables ANNAUDID, CLLI, ANNS, ANNMEMS, and ANNPHLST must also be datafilled in the CM.

ACTS provides no secondary language support.

ACTS pre-defines custom announcement numbers 1 through 23. Through datafill in tables SPIDDB, EAACTSAN and/or ACTSNBEC, the operating company can specify that announcement numbers 24 and higher are to be used to customize the initial correct deposit and overdeposit “thank-you” acknowledgments for coin calls by Service Provider ID, interLATA carrier, or Non-Bell Exchange Company.

ACTS defines certain placeholder phrase names that are datafilled in table ANNPHLST but should not be datafilled in either DRAMPHRS or ANNAUDID. The following table shows the ACTS pre-defined placeholder phrase names.

Table 12: ACTS use of placeholder phrases

Placeholder Phrase Name	Meaning
ACTS_VAR_CHARGE	Amount of money due.
ACTS_VAR_CREDIT	Amount of credit from overdeposit.
ACTS_VAR_PERIOD	Time duration for charges or for notification.
ACTS_VAR_COIN	Denomination of coin to be deposited for coin test feature.

In addition to the placeholder phrases, Nortel recommends, but does not require, that the operating company use certain other phrase names for ACTS. These are shown in tables 13 and 14. Those phrase names are added to table DRAMPHRS (using the DRAMREC CI) or ANNAUDID (manually, after provisioning the media servers) before they are datafilled in table ANNPHLST.

The following table shows the pre-defined ACTS announcement numbers, the scenario in which each is used, and the suggested phrase list for each. The table shows the announcement numbers in an order that is logical in terms of call flow, rather than listing them in order by announcement number.

Note: Suggested content for the non-variable phrase names is shown in Table 14.

Table 13: Pre-defined ACTS announcements with suggested phrase lists

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List (PHLIST field of table ANNPHLST)
1	Initial deposit request	(ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_FOR_FIRST) (ACTS_VAR_PERIOD) $
2	Re-prompt on timeout after announcement 1, no coins entered	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $
3	Inter-coin prompt - Re-prompt after inter-coin timeout for initial period	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_MORE) $
4	Acknowledgement of correct deposit for initial period	(ACTS_THANK_YOU) $
5	Acknowledgement of overdeposit for initial period	(ACTS_THANK_HAVE) (ACTS_VAR_CREDIT) (ACTS_CR_OVERTIME) $
6	Notification at end of initial period, for post-paid overtime	(ACTS_ALERT) (ACTS_VAR_PERIOD) (ACTS_END_SIGNAL) $

Table 13: Pre-defined ACTS announcements with suggested phrase lists

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List (PHLIST field of table ANNPHLST)
7	Charge due deposit request, post-pay, with no previous overdeposit	(ACTS_ALERT) (ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_FOR PAST) (ACTS_VAR_PERIOD) $
14	Re-prompt on timeout after announcement 7	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $
8	Charge due deposit request, post-pay, with previous overdeposit	(ACTS_ALERT) (ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_YOU_HAVE) (ACTS_VAR_CREDIT) (ACTS_CREDIT) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_MORE) (ACTS_FOR_PAST) (ACTS_VAR_PERIOD) $
15	Re-prompt on timeout after prompt 8	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $
20	Charge due deposit request, pre-pay, with no previous overdeposit	(ACTS_ALERT) (ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_FOR_NEXT) (ACTS_VAR_PERIOD) $
22	Re-prompt on timeout after prompt 20	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $

Table 13: Pre-defined ACTS announcements with suggested phrase lists

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List (PHLIST field of table ANNPHLST)
21	First overtime charge prompt, pre-pay, with previous overdeposit	(ACTS_ALERT) (ACTS_VAR_CHARGE) (ACTS_PLEASE) (ACTS_PAUSE) (ACTS_YOU_HAVE) (ACTS_VAR_CREDIT) (ACTS_CREDIT) (ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_MORE) (ACTS_FOR_NEXT) (ACTS_VAR_PERIOD) $
23	Re-prompt on timeout after prompt 21	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) $
16	Overtime inter-coin prompt (pre-pay or post-pay)	(ACTS_PLS_DEPOSIT) (ACTS_VAR_CHARGE) (ACTS_MORE) $
17	Acknowledgement of correct deposit for overtime period (pre-pay or post-pay)	(ACTS_THANK_YOU) $
18	Acknowledgement of overdeposit for overtime period (pre-pay or post-pay)	(ACTS_THANK_HAVE) (ACTS_VAR_CREDIT) (ACTS_CR_OVERTIME) $
9	Time and charges quotation	(ACTS_ALERT) (ACTS_CHARGES_ARE) (ACTS_VAR_CHARGE) (ACTS_PLUS_TAX) (ACTS_VAR_PERIOD) $
19	Repeat time and charges quotation (timeout after announcement 9)	(ACTS_ALERT) (ACTS_CHARGES_ARE) (ACTS_VAR_CHARGE) (ACTS_PLUS_TAX) (ACTS_VAR_PERIOD) $
10	Non-coin, customer-requested notification of time.	(ACTS_ALERT) (ACTS_VAR_PERIOD) (ACTS_HAS_ENDED) $
11	Coin test prompt	(ACTS_PLS_DEPOSIT) (ACTS_1) (ACTS_VAR_COIN)

Table 13: Pre-defined ACTS announcements with suggested phrase lists

Pre-defined Announce-ment Number	When this Announcement is Used	Suggested Phrase List (PHLIST field of table ANNPHLST)
12	Coin test failure. Also coin test cycle done.	(ACTS_PAUSE) (ACTS_ALERT) $
13	Coin test success	(ACTS_THANK_YOU) (ACTS_VAR_COIN) (ACTS_TST_ENDED) $

You do not have to use the exact phrase lists that are suggested in the table above, but it is important that placeholder phrases be datafilled only for the announcements for which they make sense and are shown in the table. For example, it would be an error to datafill placeholder phrase ACTS_VAR_CREDIT in announcement 1, the initial deposit request.

One reason you might want to define your own phrase names would be to play a different “thank-you” acknowledgment for announcement 4 than for announcement 17. To provision different announcements:

- First record the new announcement on the DRAM(s) or provision it on the media servers.
- Then add datafill to table DRAMPHRS (using the DRAMREC CI) or ANNAUDID (manually) mapping a new phrase name defined by the operating company to the internal ID provisioned on the announcement server.
- Finally, datafill the new phrase in table ANNPHLST against the CLLI used for ACTS and the ACTS announcement number.

The following table shows the suggested content for the phrase names from Table 13. It does not include the placeholder phrase names, for which variable substitution occurs before the audio identifiers are determined. It also does not include the pre-defined phrase names that are substituted for placeholder phrases.

Table 14: Suggested content for ACTS phrases, other than those used for placeholder substitution

Phrase Name	Suggested Phrase Content
ACTS_ALERT	(alerting tone, recording as an announcement)
ACTS_PLEASE	“please”
ACTS_PAUSE	(2 s pause)

Table 14: Suggested content for ACTS phrases, other than those used for placeholder substitution

Phrase Name	Suggested Phrase Content
ACTS_PLS_DEPOSIT	“Please deposit”
ACTS_FOR_FIRST	“for the first”
ACTS_MORE	“more”
ACTS_THANK_YOU	“Thank you”
ACTS_THANK_HAVE	“Thank you. You have”
ACTS_CR_OVERTIME	“credit toward overtime”
ACTS_END_SIGNAL	“has ended. Please signal when through.”
ACTS_FOR_PAST	“for the past”
ACTS_YOU_HAVE	“You have”
ACTS_CREDIT	“credit”
ACTS_CHARGES_ARE	“The charges are”
ACTS_PLUS_TAX	“plus tax for”
ACTS_HAS_ENDED	“has ended.”
ACTS_1	“one”
ACTS_TST_ENDED	“test has ended.”

Note: The ACTS phrases shown in the tables in this section are not the complete list of phrases that must be present in table DRAMPHRS or ANNAUDID to support ACTS. Tables DRAMPHRS (legacy) and ANNAUDID (packet) must also include certain phrases to support variable substitution. Variable substitution is done differently for packet announcements than for DRAM announcements. Section “Automatic Coin Toll Service” in “DMS-100 Family NA100 Translations Guide” lists all the phrases that must be provisioned on DRAMS if legacy announcements are used for ACTS, and these include the ones used for variable substitution. If packet announcements are used, refer to “ACTS” on page 2077 of this document.

Auxiliary Operator Service System

The AOSSVR custom announcement type is no longer supported. It was used with TOPS MP positions, which are no longer supported.

3.5.2.2.8 Translation verification and other tools

Unchanged.

3.6 Service Orders (SO) (CM & SESM)

No impact.

3.7 Software optionality control (SOC)

This feature is not controlled by SOC. Note however that some of its prerequisite configuration is SOC controlled. Refer to “Hardware and Software Requirements” on page 2070 for information about the feature’s prerequisites.

3.8 Element Management

No impact.

3.9 User interface changes

No impact.

3.10 OSSGate Interface Changes

No impact.

3.11 Security

No impact.

3.12 Configuration Walkthrough

See “Initial Configuration” on page 2071.

Chapter 4: International-only features

Publication History

January 2006

Version 01.04, re-release of the Standard version of this document for ISN09 FVS. No changes were made to the International section of this document.

September 2005

Version 01.03, re-release of the Standard version of this document for ISN09 due to churn. The following features have been added since the first Standard release.

Under Call Server 2000:

- A00009165, USP - Offline Routesets without Alarms
- A00009282, Emergency Stand Alone (ESA) International Support for MG9KEM
- A00010168, H.323 support for COnnected Line Presentation/COnnected Line Restriction (COLP/COLR)

Under World Trade:

- A00006663, DDRM Alarms and Audits
- A00006664, DDRM Line Testing
- A00006665, DDRM ESA Support
- A00009145, Record Feature Usage
- A00009216, JI-ISUP to Base ETSI ISUP V2 Mapping Enhancement

June 2005

Version 01.02, release of the Standard version of this document for ISN09. Feature A00011363, International H.323 2CLI (Calling Line Identity) Support has been added since the Preliminary release.

The following features have been deferred to the SN09.1 release and have been removed from this document since the Preliminary release:

- A00009020, Australia Country Fit
- A00009037, Core - Enhanced ESA for International MG9000
- A00009039, International MG9000 Line Test Support
- A00009282, Emergency Stand Alone (ESA) Multiple Level Precedence and Preemption (MLPP) for MG9KEM
- A00009297, Quality of Service Support of AAL2 and Timestamp

April 2005

Version 01.01, release of the Preliminary version of this document for ISN09.

Overview

This chapter supports Nortel's International Carrier VoIP Solutions ISN09 release. It describes ISN09 features that affect inputs to or outputs from the solutions. These changes, therefore, affect the use of the Operations Support System (OSS) for ISN09. The document includes copies of feature descriptions used in software design.

Information in this document is believed to be accurate at the time of publication, but it is subject to change. Use of this document should be restricted to resource planning and estimating for ISN09. DO NOT use this document to make changes to existing software.

How the International section is organized

This section of the document is divided into the following areas:

- *International activities mapping tables*. These tables relate the activity identifier associated with each International-only feature to:
  - the product/application/network element, or market area affected
  - affected software object types (data schema, for example)
- *International features list*. This list shows ALL features applicable for the International market. Therefore, it includes both International-only features as well as features that apply to both the International and North American markets.
- *New or changed* for ISN09. This section provides a table for each software object type, as follows:
  - Office parameters

- Logs and alarms
- Operational and Performance Measurements (OMs and PMs)
- Data Schema tables or MIBs
- User Interface (commands)
- Service Orders (Servord+)
- AMA/billing
- Software Optionality Control (SOC)

Each table gives a summary of the changes caused per feature. Within each table, features are arrranged by product/application, network element, or market and then in numeric order by the ACTID of the feature which creates new information or causes the change.

- *Feature descriptions*. This section provides feature descriptions, based on design documents, limited to International-only features. Features that apply to both the International and North American markets may be found in Chapter 3 which contains North American market feature descriptions. The feature descriptions in Chapter 3 are organized by product/application/ network element. The feature descriptions in Chapter 4 (this chapter) are grouped first by CS 2000 features and then by World Trade features. Within each group, the features are arranged in numeric order by ACTID.

ISN09 Activity mapping tables

Introduction

This document contains advance information about differences in operations, administration, maintenance, and provisioning (OAM&P) for International Release ISN09. The purpose of this document is to provide early information about new, modified or deleted items related to OSS-impacting areas.

The table below shows the mapping from the activity identifier (ACTID) associated with each new feature to the following:

- the associated product, application, network element, or market
- the international solution that the feature affects, of the following:
  - International PT-AAL2
  - International PT-IP
  - International IAC
  - International IAW
  - International UA-IP
  - International DMS
  - International CHS
- the software object type or area that the feature affects, of the following:
  - Logs/faults
  - Data schema tables/MIBs
  - Office parameters
  - Service orders (ServOrd)
  - User interface/human-machine interface
  - Operational and performance measurements (OMs/PMs)
  - Automatic Message Accounting (AMA)/billing
  - Software Optionality Control (SOC)

Activity Mapping Table: Solutions Affected

		ISN09 Solutions						
PRODUCT or APPLICATION	ACTID	Int'l PT-AAL2	Int'l PT-IP	Int'l IAC	Int'l IAW	Int'l UA-IP	Int'l DMS	Int'l CHS
Call Server 2000	A00009165				X			
Call Server 2000	A00009282					X		
Call Server 2000	A00010168							X
World Trade	A00006663						X	
World Trade	A00006664						X	
World Trade	A00006665						X	
World Trade	A00007289						X	
World Trade	A00008429						X	
World Trade	A00008477						X	
World Trade	A00008484						X	
World Trade	A00008556							X
World Trade	A00009145						X	
World Trade	A00009216						X	
World Trade	A00009321				X			
World Trade	A00009322				X			
World Trade	A00009489				X			
World Trade	A00011363							X

Activity Mapping Table: Software object types or areas impacted

ISN09 Solutions		SW object types / areas impacted							
PRODUCT or APPLICATION	ACTID	Logs/Faults	Data Schema	Office Parms	ServOrd	Commands/User Interf/HMI	OMs/PMs	AMA/Billing	Optionality
Call Server 2000	A00009165								
Call Server 2000	A00009282								
Call Server 2000	A00010168								
World Trade	A00006663								
World Trade	A00006664								
World Trade	A00006665								
World Trade	A00007289								X
World Trade	A00008429		X						X
World Trade	A00008477		X						X
World Trade	A00008484		X						
World Trade	A00008556		X		X	X			X
World Trade DMS	A00009145								
World Trade DMS	A00009216								
World Trade	A00009321					X			
World Trade	A00009322					X			
World Trade	A00009489		X						
World Trade	A00011363		X						

International Features List

Introduction

The following table shows ALL features applicable for the International market. Therefore, it includes both International-only features as well as features that apply to both the International and North American markets.

Features for International Solutions

ACTID	Feature Title	Solution	Location
A89007819	QoS Reporting: QoS Collector Application	Int'l PT-IP, Int'l IAW, Int'l IAC	Chap. 3
A00006663	DDRM Alarms and Audits	DMS	Chap. 4
A00006664	DDRM Line Testing	DMS	Chap. 4
A00006665	DDRM ESA Support	DMS	Chap. 4
A00007289	RT Selector Enhancement	DMS	Chap. 4
A00007544	NCAS Link & SIP NMS Support	Int'l PT-IP	Chap. 3
A00008429	RBWF Enhancement	DMS	Chap. 4
A00008477	Increase size of table MSGRTE	DMS	Chap. 4
A00008484	IN Terminating Trigger Feature Interactions	DMS	Chap. 4
A00008556	SIP Lines Core OAMP Support	Int'l CHS	Chap. 4
A00008916	Increase Port Density	Intl IAW, Intl IAC, Intl PT-IP, Intl UA-IP	Chap. 4
A00008969	MG9000 ATM50 SSI Monitoring	Intl UA-IP	Chap. 4
A00009011	TOPS IP Security Enhancement	Intl PT-AAL2, Intl PT-IP, DMS	Chap. 3
A00009012	TOPS OSSAIN Service Enhancement	Intl PT-AAL2, Intl PT-IP, DMS	Chap. 3
A00009013	TOPS Announcements	Intl PT-IP	Chap. 3
A00009078	ICM Dual CT	Intl UA-IP, DMS	Chap. 3
A00009085	ACD & ICM Capacity Expansion	Intl UA-IP, DMS	Chap. 3
A00009120	Multi Time Zone Enhancement	Int'l UA-IP	Chap. 4
A00009129	Conotrolled Hot SWACT	Int'l PT-IP	Chap. 3
A00009145	Record Feature Usage	DMS	Chap. 4

ACTID	Feature Title	Solution	Location
A00009165	USP - Offline Routesets without Alarms	Intl IAW	Chap. 4
A00009189	SESM Support for 64 Character	Intl IAW, Intl IAC	Chap. 3
A00009208	180K Lines Support	Int'l UA-IP, Int'l IAW, Int'l IAC	Chap. 3
A00009216	JI-ISUP to Base ETSI ISUP V2 Mapping Enhancement	DMS	Chap.4
A00009227	NPM Robustness	Int'l IAW, Int'l IAC, Intl PT-AAL2, Intl PT-IP, Int'l UA-IP	Chap. 3
A00009282	Emergency Stand Alone (ESA) International Support for MG9KEM	Int'l UA-IP	Chap. 4
A00009321	NMC Code Blocking	Int'l IAW	Chap. 4
A00009322	CHT Linde Service Complilance	Int'l IAW	Chap. 4
A00009332	P-time and Codec Negotiation Selection Policy	Int'l UA-IP	Chap. 3
A00009489	CHT: Call Waiting Enhancement	Int'l IAW	Chap. 4
A00010168	H.323 support for COnnected Line Presentation/COnnected Line Restriction (COLP/COLR)	Int'l CHS	Chap. 4
A00011363	International H.323 2CLI (Calling Line Identity) Support	Int'l CHS	Chap. 4

New and Changed for ISN09

Introduction

This section of the document contains tables which give an overview of the feature-based changes occurring in this International release for the following areas:

- Office parameters
- Logs/faults
- Operational measurements (OMs) and performance measurements (PMs)

- Data Schema tables or MIBs
- User interface (commands)
- Service Order (Servord+)
- AMA/billing
- Software Optionality Control (SOC)

Within each table, the changes are arranged by associated product, and then in numeric order by the activity identifier (ACTID) of the feature which creates new information or causes the change.

Office Parameter changes overview

The following office parameters are new or changed for ISN09. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed Office Parameters

Office Parm Name	New or Changed	Description
Product = CS 2000		
PN_SUPPORTED	Changed	A00011363 (Int'l CHS) modifies this parameter to support ETSI ISUP V2, SPIROU, ETSI PRI and International H.323. Field ACTIVE must be set to Y to enable 2 CLI behaviour for PRI/H323 to H323.
Product = World Trade		
LCM-ESA_ENTRY_BADCSIDE RLCM_ESAENTRY_BADLINK RLCM_ESA_NOTIFY_TONE RLCM_ESASDUPD_HOUR	Changed	A0006665 (Int'l DMS) modifies these parameters to provide ESA support. • LCM-ESA_ENTRY_BADCSIDE determines the delay before entering ESA-mode after a failure is detected. • RLCM_ESAENTRY_BADLINK determines the desired delay timer between the failure of the C-side message link and the entry of ESA mode. • RLCM_ESA_NOTIFY_TONE controls whether the subscriber hears a distinctive dial-tone burst during ESA mode. When this parameter is set to Y then ESA specific tone is expected to be applied by DDRM. • RLCM_ESASDUPD_HOUR is used to set the start time to download ESA static data to all remotes on host site.

Logs/faults changes overview

The following logs or faults are new or changed for ISN09. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed Logs/Faults for ISN06

Log/Fault Type	Log/Fault Name	New/Modified/Deleted, ACTID and Solution
Product = CS 2000		
PM Logs (new)	**ESA311** **ESA312**	A00009282 (Int'l UA-IP) creates the following logs: • ESA311 is generated by the EM when a problem is detected when trying to download the datafile from the core. This new condition is when the Core datafile is more than 48 hours old, indicating that the file on the Core is not being generated nightly. • ESA312 indicates an internodal ESA provisioning failure.
Product = World Trade		
PM Logs (new)	**PM179** **PM116**	A00006663 (Int'l DMS) creates PM179 to log DDRM exception reports. It also creates PM116 to log unexpected values in the fields of exception reports and problems with handling messages.
DDRM alarms (new)	**(see description)**	A00006663 (Int'l DMS) describes the following alarms reported by the DDRM node to DMS: • Module Alarm • Card Configuration Alarm • POC Alarm • Ring Alarm • - 48v Alarm
PM Logs (new)	**PM171**	A00006665 (Int'l DMS) creates PM171 to report on up to 23 ESA-related fields listedin Table 1 of the FN.

Operational Measurements/Performance Measurement changes overview

No new or changed OMs or PMs are seen in these features for ISN09.

Summary of new or changed OMs/PMs

OM Group or PM name	New or Changed	Description

Data Schema tables/MIBs changes overview

The following Data Schema tables or MIBs are new or changed for ISN09. More complete descriptions appear in the Feature Descriptions section of this document.

DS Table/MIB	Changed or New
Product = CS 2000	
LTDATA (changed)	A00010168 (Int'l CHS) provides support for COLP/COLR on International H.323 Gateways. The service is provided on a per trunk-group basis, datafilled in table LTDATA.
Product = World Trade	
LCMINV (changed)	A00006665 (Int'l DMS) modifies table LCMINV to allow ESA support if datafill is set to Y.
IBNXLA (changed)	A00008429 (Int'l DMS) modifes this table by adding two new IBN_LOG_FEATURES: "RAGD" and "RAGINT" for RAG deactivation and RAG interrogation. These features are functional when SOC "SVBI RBWF Enh" is ON.
AMAOPTS (changed)	A00008429 (Int'l DMS) modifes this table by adding new option NODAL_RAG_BILL. Both "SVBI RBWF Enh" SOC and NODAL_RAG_BILL option must be ON in order to enable billing of Nodal RBWF calls.
CUSTSTN, CUSTNTWK (changed)	A00008429 (Int'l DMS) modifes these tables so that the Ring again cancellation timer allows the end user to set a limit on how long a nodal or network ring again request can remain active. This value is datafillable through tables CUSTSTN for nodal RAG and CUSTNTWK for network RAG. The range for RAG Cancellation Timer in CUSTSTN is extended up to 185 so that it includes the value 45.

DS Table/MIB	Changed or New
ISERVOPT (changed)	A00008429 (Int'l DMS) modifes this table by adding new option RBWFENH with two subfields: MAX_RBWF_REQ and IGNORE_INTRAGRP. • MAX_RBWF_REQ determines the maximum number of RBWF requests that can be activated by a RAGOR simultaneously. It takes values between 1 and 6. Its default value is 5, if not datafilled. • IGNORE_INTRAGRP allows RBWF Service to function independently of the INTRAGRP flag. NOTE: SOCs SVBI0036 and SVBI0037 should also be ON to make these options fully functional.
MSGRTE2 (new)	A00008477 (Int'l DMS) provides the expansion of the MSGRTE table size up to 100,000 tuples by adding a new table MSGRTE2. MSGRTE and MSGRTE2 tables are not effective at the same time. SOC option XLAS0057 determines which table will be used.
SERVINFO (changed)	A00008484 (Int'l DMS) modifies the FI option by adding new entry CONV_DESK to the possible values which allows IN to co-exist with line-based DMS services, subject to certain limitations and restrictions.
SERVRINV LGRPINV IPAPPL IBNFEAT (changed)	A00008556 (Int'l CHS) modifies the following tables: • SERVRINV adds new value DPL_TERM under subfield TERM_TYPE and new value DPLEX under subfield EXEC_LINEUP, both in field SRVREXEC. • LGRPINV adds new entry SSDPL in field GRPTYPE to support DPL agents. • IPAPPL adds new entry SIPMTC to the option list under subfiled Application iin field OPTS. • IBNFEAT is enhanced as follows to support a new feature DPL which will convert the IBN line into a DPL line: — Fields DF and Feature add a new entry, DPL, to be assigned to an IBN line. — The DATA field adds new subfield SIP with a Y/N entry to identify a SIP line. — The DATA field adds new subfield MAX_NUM_ CALLS to specify the maximum simultaneous call appearances. — The DATA field adds new subfield ALLOW_BSY_ TERM to determine whether or not a busy SIP line can take an additional call termination.

DS Table/MIB	Changed or New
ISERVOPT (changed)	A00009322 (Int'l IAW) enhances the existing Call Lock feature as following. Table SERVOPT is modified, new fields of tuple ILRCLS and CEPTPW are introduced. • supports dial tone during the deactivation procedure. The user can originate a new call directly after the successful deactivation without going on hook. This function is optional and controlled by the new field ALLOW_ORIG_AFTER_DEACT(Y/N) of ILRCLS tuple. • allows class of restriction to be overwritten by new entry without doing a feature deactivation. This function is optional and controlled by the new field OVERRIDE_ILR_CLASS(Y/N) of ILRCLS tuple. • allows the user to change the password according to the required dialing sequence LH DT*SC*PWO*PWN#CT. The password is 4 digits. This function is optional and controlled by the new field NEW_PWD_ONCE(Y/N) of tuple CEPTPW. • generates a report and disallows any feature modification (activation, deactivation, change) until the following day upon 3 times of wrong password entry in succession, or until the administration by operator. The following day is the time after the next 00:00 midnight. The 3 times is the value of field MAX_PIN_RETRY which is datafilled in CEPTPW tuple of table ISERVOPT. The password is 4 digits. This function is optional and controlled by the new field AUTO_UNLOCK(Y/N) of tuple CEPTPW.
ISERVOPT (changed)	A00009489 (Int'l IAW) enhances the CEPT Call Waiting for CS2Kc IP platform. Only IBN lines and TW ISUP, TW PRI are supported. Table SERVOPT is modified, new fields of tuple ICWT is introduced. • supports generating the second Call Waiting Tone B for both parties during Call Waiting scenario. This function is optional and controlled by the new field ICWT_2PTY_TONE_B (Y/N) in ICWT tuple. • supports answering the call and toggling between held parties by hook-flash only, no need to enter any digit right after hook-flash. This function is optional and controlled by the new field ICWT_DFLT_RCODE (Y/N) in ICWT tuple.

DS Table/MIB	Changed or New
ISERVOPT (changed)	A00009489 (Int'l IAW) enhances the CEPT Call Waiting for CS2Kc IP platform. Only IBN lines and TW ISUP, TW PRI are supported. Table ISERVOPT is not modified, but the feature describes datafill needed. • supports generating the second Call Waiting Tone B for both parties during Call Waiting scenario. • supports answering the call and toggling between held parties by hook-flash only, no need to enter any digit right after hook-flash.
LTDATA (changed)	A00011363 (Int'l CHS) modifies LTDATA as follows: • Existing 2CLI option is now enabled for H.323 QSIG trunks (previously only functional for PRI trunks). • The CLIP option is applicable to ETSI PRI and International H.323 terminator. • Other existing options used for 2CLI in LTDATA are the CLIR option provisioned for the originator, and the NOSCRN option.

User Interface (commands) changes overview

The following User Interface GUIs or Commands are new or changed for ISN09. More complete descriptions appear in the Feature Descriptions section of this document,

Field	Command/User Interface Description
Product = Call Server 2000	
(see description)	A00009165 (Int'l IAW) sets routeset state to offline rather than system busy when provisioned from the USP. It also allows the craftsperson to manually offline the routeset in CORE to clear inadvertant alarms.

Field	Command/User Interface Description
ESA Config Panel **ESA Tanslation List View** **ESA Customer Group List View**	A00009282 (Int'l UA-IP) modifies the following GUIs: • **ESA Config** Panel removes the reference to the North American market for the "Enhanced" ESA Mode selector. Prior to SN09 Enhanced ESA was only available for the North American Market. • ESA Tanslation List View now indicates the source of the CORE translator that the translation entry came from. Also if the translation entry is of the type DGCOD then the existing Digits field will be split in the middle to separate the To and From digits. • **ESA Customer Group List View now** indicates whether the Extension IDs are actually indexes into the EXTN table or the DGCOD table. This will be performed by modifying the existing "Extension ID" column name to "DGCOD ID" when the indexes are for DGCOD.
Product = World Trade	
Support for LTP test comands on DDRM(new)	A00006664 (Int'l DMS) provides support in DMS-MMP product for line testing available in DDRM. The feature creates an interface between DMS and DDRM through E1 (PCM30) links to execute supported LTP and ALT level test commands for the posted DDRM subscriber lines.
QSIP command (new)	A00008556 (Int'l CHS) creates the QSIP command at the CI level to query the CS2KSS to get the SIP information. QSIP query takes place through the NCAS link. Hence, the command response depends upon the availability of the NCAS link.
MASSCALL command **CODECTRL commands in MAPCI** **(changed)**	A00009321 (Int'l IAW) adds the CBK option PCT, which allows calls to be blocked from proceeding based upon the destination code (digits). Calls can be blocked by a specified percentage, ranging from 1 to 100. Blocked calls can have one of three possible treatments applied: NCA, EA1, or EA2. PCT is also available in MAPCI commands as a CBK option. Direct access to the CodeCtrl menu level is from the Command Interpreter (CI) level by entering the commands "MAPCI;NWM;CODECTRL". CodeCtrl commands are to List, Apply and Remove code controls.The PCT option is available in these code control commands. TRAVER output is modified to indicate if the PCT option is activated while doing TRAVER.

Field	Command/User Interface Description
Enhanced Do Not Disturb feature **(changed)**	A00009322 (Int'l IAW) enhances the existing Do Not Disturb feature as follows: • supports Special Dial Tone if the feature is activated. • disables the ring splash. • supports dial tone upon feature deactivation dialing sequence, the user is able to originate new call without hanging up.
Enhanced Call Lock feature **(changed)**	A00009322 (Int'l IAW) enhances the existing Call Lock feature as follows: • supports dial tone during the deactivation procedure.The user can originate a new call directly after the successful deactivation without going on hook. • allows class of restriction to be overwritten by new entry without doing a feature deactivation. • allows the user to change the password according to the required dialing sequence LH DT*SC*PWO*PWN#CT. The password is 4 digits. • generates a report and disallows any feature modification (activation, deactivation, change) until the following day upon 3 times of wrong password entry in succession, or until the administration by operator. The following day is the time after the next 00:00 midnight. The 3 times is the value of field MAX_PIN_RETRY which is datafilled in CEPTPW tuple of table ISERVOPT. The password is 4 digits.

Service Order changes overview

The following Service Order information is new or changed for ISN09. More complete descriptions appear in the Feature Descriptions section of this document..

Summary of new or changed Service Orders

Area	New or Changed	ServOrd Description
Product = World Trade		
DPL line option	**New**	A00008556 (Int'l CHS) modifies SERVORD+ to accept three new options related to DPL lines provisioning: DPL, SIP_PASSWORD and SIP_DATA. When provisioning a SIP line all three of the options described above must be present in the SERVORD+ NEW command. They can not be added later via ADO. The new system prompts for the DPL option are SIP, MAX_NUM_CALLS, and ALLOW_BSY_TERM.

AMA/billing changes overview

The following AMA/Billing information is new or changed for ISN09. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed AMA/billing

AMA/billing item	New or Changed	Description
Product = World Trade		
AMAOPTS option	New	A00009145 (Int'l DMS) creates AMAOPTS option MC611_FOR_RFU (where RFU stands for **R**ecord **F**eature **U**sage) to control the recording of feature actions. Subscribers' feature actions are recorded only if the MC611_FOR_RFU option is set to ON. A brand new billing record is generated after the feature action is initiated.

Software Optionality Control (SOC) changes overview

The following SOC information is new or changed for ISN09. More complete descriptions appear in the Feature Descriptions section of this document.

Summary of new or changed SOCs

SOC code	New or Changed	Description
Product = World Trade		
METRO018	New	A00007289 (Int'l DMS) creates this state SOC, "Retrans Selector." When this SOC is ON and the translation is in XXRTE RT-based retranslation, the DMS-100 MMP product will preserve LNET and MZONE during the retranslation, in the same way as DMS-100I.
CS2C0005	New	A00008556 (Int'l CHS) creates this usage SOC, "Number of SIP Clients." The SOC limit defines the maximum number of DPL lines that can be provisioned in the switch. The SOC code is functional whenever a line is provisioned with the DPL option whether through table control / servord.

Summary of new or changed SOCs

SOC code	New or Changed	Description
SVBI0036 SVBI0037	New	A00008429 (Int'l DMS) creates the following state SOCs: • SVBI0036, "SVBI RBWF Enh" (Service Base International Ring Back When Free Enhancement) controls the following: — Allowing nodal RBWF between different customer groups via ignoring INTRAGRP flag. — Billing of nodal RBWF usage. — Deactivation and interrogation functionalities with new dialling sequences. • SVBI0037, "Multiple RBWF" (Service Base International Multiple Ring Back When Free) controls the following: — Allowing N RBWF request to be activated by the RAGOR. — Rejecting N+1th request.
XLAS0057	New	A00008477 (DMS) creates this state SOC to determine whether table MSGRTE or MSGRTE2 is used. When this SOC is ON, the MSGRTE table is disabled and call processing will begin to use the new table MSGRTE2.
NETK0087	New	A00009216 (DMS) creates this state SOC, "NETK Jpn I ISUP Parm Enh," to enable passing the value of NOA in calling party number as unchanged to the Base ETSI ISUP V2 for the JI-ISUP to Base ETSI ISUP V2 interworking.

ISN09 Feature Descriptions

Product = Call Server 2000

A00009165 -- USP - Offline Routesets without Alarms

1: Applicable solution(s)

Int'l IAW

1.1 Description

Before this feature, if customer datafills new SS7 routesets in USP which acts as Signal Gateway, but does not wish to, or cannot for some reason, bring them into service immediately, CORE shows alarms for those routesets. The critical alarms caused by it masks other legitimate alarms, resulting in a signaling outage being overlooked.

This type of behavior is very typical for operator craftspersons. In large corporations, the addition of SS7 routesets can be a multi-company activity, where schedules have to be coordinated and resources have to be used as they become available.

The purpose of this feature is to eliminate this kind of alarms found on XA-CORE switch, and provide an OFFLINE state for routeset in CORE.

1.1.1 Set the routeset to offline when it is provisioned from USP

Before this feature, when the routeset is provisioned from USP, its state is set to system busy, then an alarm is generated.

In this feature, the state is set to offline when the routeset is just provisioned from USP.

1.1.2 Enable the operation to offline a routeset in CORE

When CORE receives a DUNA from SG for a routeset, the routeset state is set to SYSB, and an alarm is generated for it. But sometimes, operator wants to offline the routeset and would not expect any alarms on it.

In this feature, when the routeset is seen SYSB (system busy) in CORE , if operator thinks it should be in offline state, the routeset can be offline manually in CORE so that the additional alarm is cleared. This operation can not be done while the routeset is in-service in CORE.

When routeset is in offline state, it can be turn into man-busy state by the command BSY from craftsperson. When DUNA/DAVA/SCON message are

received while the corresponding routeset is in offline or man-busy state, these message are discarded.

When RTS command is run for a routeset by craftsperson, routeset state is set to SYSB, and send out a DAUD to USP to get the correct state.

1.1.3 Routeset related with ASM can be deleted at USP only when it is at OFFL state in CORE.

If the routeset is not at OFFL state at CORE, the request to delete it will be rejected by CORE, and the corresponding information will be given.

1.2 Hardware Requirements or Dependencies

N/A.

1.3 Software Requirements or Dependencies

N/A.

1.4 Limitations and restrictions

Need operator to take more action to offline the routeset in CORE, and the additional alarm will exists before the action.

1.5 Interactions

1.6 Glossary

Term	Description
DAVA	Destination Available
DUNA	Destination Unavailable

Product = CS 2000

A00009282 -- Emergency Stand Alone (ESA) International Support for MG9KEM

Functional Description

1: Applicable Solution(s)

Int'l UA-IP

1.1 Description

SN08 Introduced Internodal ESA for North American (NA) Markets. This feature provided a Community of Interest (COI) for MG9000 nodes to communicate if unable to communicate with the GWC.

For SN09, this feature is to be expanded to include International markets. COI provisioning will be provided as is used for North America. This feature also removes the restriction that Enhanced ESA be only associated with North America.

International ESA allows the download of information necessary to support International Emergency Stand Alone (ESA) call processing across all native (non ABI) and ABI lines served by a single MG9000 for intra and internodal ESA.

1.2 Hardware Requirements or Dependencies

None

1.3 Software Requirements or Dependencies

This ESA activity on the MG9K is dependent upon two additional activities for successful completion and will be integrated together under an ICAF.

1.4 Limitations and restrictions

- The ESA data from the core will be autonomously downloaded to the MG9000 only once every 24 hours.
- ESA data can be manually downloaded from the core and sent to individual VMGs.
- The MG9000 EM will not allow the modification of any ESA data retrieved from the core.

1.5 Interactions

None

1.6 Glossary

Term	Description
ATM	Asynchronous Transfer Mode
EM	Element Manager (MG9K)
ESA	Emergency Stand Alone
ITP	Integrated Telephony Processor
MEGACO	Media Gateway Control

Term	Description
MG9K	Media Gateway 9000
POTS	Plain Old Telephone Service
SIP	Session Initiation Protocol
TID	Terminal Identifier
VMG	Virtual Media Gateway

2: Fault Management for A00009282

2.1 Fault management strategy

The standard MG9k EM Fault Management strategy will apply to the faults for this feature. Alarms will be displayed by the MG9K EM Alarm Browser, logged in NT standard format to the SSPFS CUST logs and forwarded to northbound OSS.

2.2 Fault management tools and utilities

Alarm Browser - Reports alarms from registered events. When an alarm is generated, it is displayed in the Alarm Browser along with the date and time, the NE Id, the resource (where the alarm was generated), the severity and probable cause. Highlighting the alarm displays the description of the alarm in the text box at the bottom of the Alarm Browser.

Log Adaptor - Generates logs from registered events. The log names and numbers are predetermined and are matched with the incoming event. A log with the corresponding name and number which contains the date, time, physical location, severity and any other pertinent information is generated and placed into a separate file.

2.3 Logs and Alarms

No new alarms will be added. A new alarm reason will be generated for ESA download problems from the Core when the timestamp of the Core file is more than 48 hours old.

The alarm will be displayed at the Alarm Browser at the subnet as well as the well as the alarm browser for each corresponding network element. A log is also generated. Both are NE level alarms.

2.3.1 Explanation

2.3.1.1 ESA311

Title: Core Download Failed

Name: ESA

Description: This log is generated by the EM in when a problem is detected when trying to download the datafile from the core.

This new condition is when the Core datafile is more than 48 hours old, indicating that the file on the Core is not being generated nightly.

Severity: Minor

Event type: ESA Core Data Download

2.3.2 Field descriptions

2.3.2.1 ESA311 (nnEsaCoiFault)

Table 1 Field descriptions ESA304

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=600.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.

Table 1 Field descriptions ESA304

Field	Value	Description
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
Fault Type	string	The type of the fault: ESA Community of Interest
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Major
Description	string	Failed to ping members of communityof interest

2.3.2.2 ESA312 (Internodal ESA Provisioning Fault)

Table 2 Field descriptions ESA304

Field	Value	Description
office identification	String	Identifies the switch that generates the log. This field is optional. The maximum length of this field is 12 characters.
alarm	***,**,*, or blank	Indicates the alarm type of the log report. ***=critical, **=major, *=minor, blank = no alarms/warning
threshold	+ or blank	Indicates if a threshold is set for the log report. Plus (+) sign indicates that a threshold was set; if a blank, a threshold was not set.

Table 2 Field descriptions ESA304

Field	Value	Description
report identification	AAAA nnn	Identifies the log subsystem that generates the report. This field uses 2-4 alphabetical characters and the number 100-999 of the log report in this subsystem. For this log AAAA= MGC and nnn=600.
day	String	Identifies the day of the week.
mmmmdd	January-December (01-31)	Identifies the month and date the report generates.
hh:mm:ss	00-23 00-59 00-59	Identifies the hour, the minute, and the second the report generates.
zone	PST, EST, MST, CST, AST	Identifies the time zone.
yyyy	0000-9999	Year
ssdd	0000-9999	Defines a different sequence number for each log report generated.
event type	TBL, INFO, etc	Trouble, Service Summary, State Change, Information, Threshold and Expert. TBL for this log.
event id	String	The Log Title.
NE Number	integer	Number of the NE
NE Name	string	Name of the NE
Fault Type	string	The type of the fault: Processing Error
nnUemgEventTime	DateandTime	The Date and Time the event occurred in the following format: day mmmmdd hh:mm:ss zone yyyy
nnUemgAlarmSeverity	String	Major
Description	string	Internodal ESA provisioning failure

2.3.3 Action

ESA304 (nnEsaCoiFault):

Check failure cause in alarm or log text and perform corrective action This will typically require network route troubleshooting. The MG9000 will clear the alarm autonomously once the root cause is fixed.

ESA312 (Internodal ESA provisioning failure):

Check failure log in the alarm or log text (most common is communication failure between the MG9000 EM and the MG9000). Once the root cause is fixed the alarm can be cleared by running and audit on the affected NE, or hitting “Apply” button on the Internodal ESA configuration GUI.

2.3.4 Associated Operational Measurements or Performance Measurements

None.

2.4 Related documentation

1. NORTEL-UEMG-BASE-MIB - MG9000’s Enterprise MIB, contains the Alarm Log Table.

2. PLOA and SLOA Logs and Alarms for UE9kMG EM (DID) - MG9000s design documentation for logs and alarms on the MG9000 Element Manager.

3. Logs and Alarms Strategy for WUA Components - MG9000 Alarm strategy guide - version 1.4

3. Reliable Alarms and Alarm Robustness Design Intent Document (DID) - MG9000 Element Manager design document.

4. PLOA and SLOA Alarm Forwarding to OSS(DSUM) - MG9000 Alarm forwarding feature.

3: Configuration for A00009282

3.1 Hardware and Software Requirements

This functionality is for a MG9000 EM running a SN09 or higher software version.

3.2 Initial Configuration

No changer to the initial configuration.

3.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

3.4 Upgrade Impact

3.4.1 Dump and Restore

N/A

3.4.2 Element Management Upgrade

International and MLPP ESA functionality is only applicable if the MG9000 is at a software release of SN09 or higher.

3.5 Data schema (DS) (CM, MIBS, RDB)

N/A

3.6 Service Orders (SO) (CM & SESM)

N/A

3.7 Software optionality control (SOC)

N/A

3.8 Element Management

3.8.1 New/modified GUIs

Table 1 New or modified GUIs

GUI name	NEW, CHANGED, or DELETED
ESA Config Panel	Changed
ESA Translation List View	Changed
ESA Customer Group List View	Changed

3.8.2 GUI information

3.8.2.1 ESA Config Panel

3.8.2.1.1 Functional description

This GUI is being enhanced to remove the reference to the North American market for the “Enhanced” ESA Mode selector. Prior to SN09 Enhanced ESA was only available for the North American Market.

3.8.2.1.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled.

3.8.2.1.3 GUI size

N/A

3.8.2.1.4 GUI fields

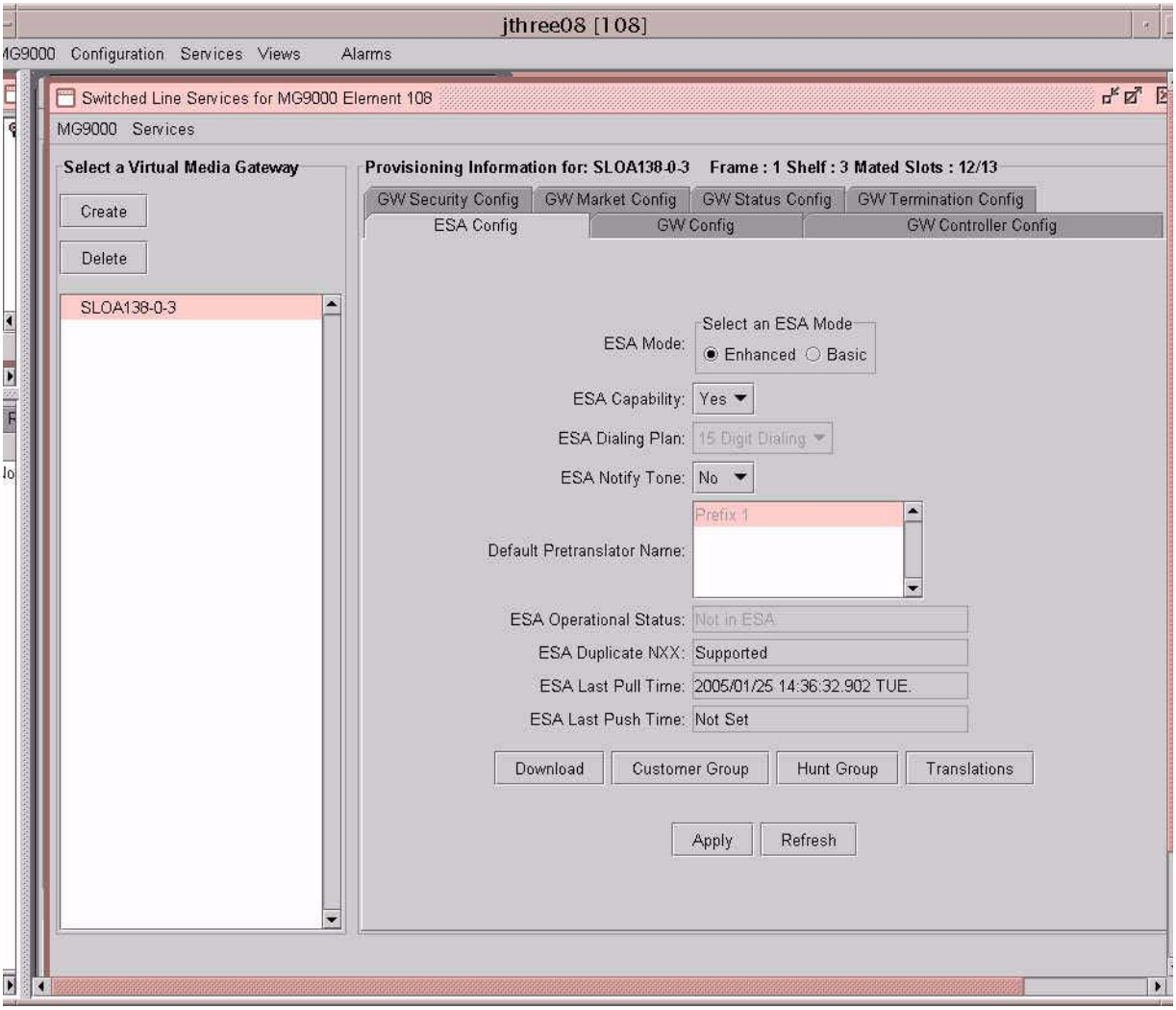
The following table lists the modified fields for the ESA Config Panel

Table 2 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
ESA Mode	Changed	N/A	“Enhanced” or “Basic”	The “Enhanced” will use the ESA data provided by the Core. This will be used by both ABI and ITP VMGs. Enhanced ESA can now be used for both the North American and International markets. The “Basic” will work in the same manner that ESA is configured in SN06 using the MG9000 EM for ITP VMGs but will not be supported for ABI VMGs.	None

3.8.2.1.5 Usage example

The following is an example of the new ESA Config Panel:



3.8.2.1.6 GUI release history update

The following fields were modified:

- ESA Mode entry labels

3.8.2.1.7 Supplementary information

None

3.8.2.1.8 CLUI Interface

N/A

3.8.2.2 ESA Translation List View

3.8.2.2.1 Functional description

This GUI is being enhanced to now indicate the source of the CORE translator that the translation entry came from. Also if the translation entry is of the type DGCOD then the existing Digits field will be split in the middle to separate the To and From digits.

3.8.2.2.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled. The fields added are for display only.

3.8.2.2.3 GUI size

N/A

3.8.2.2.4 GUI fields

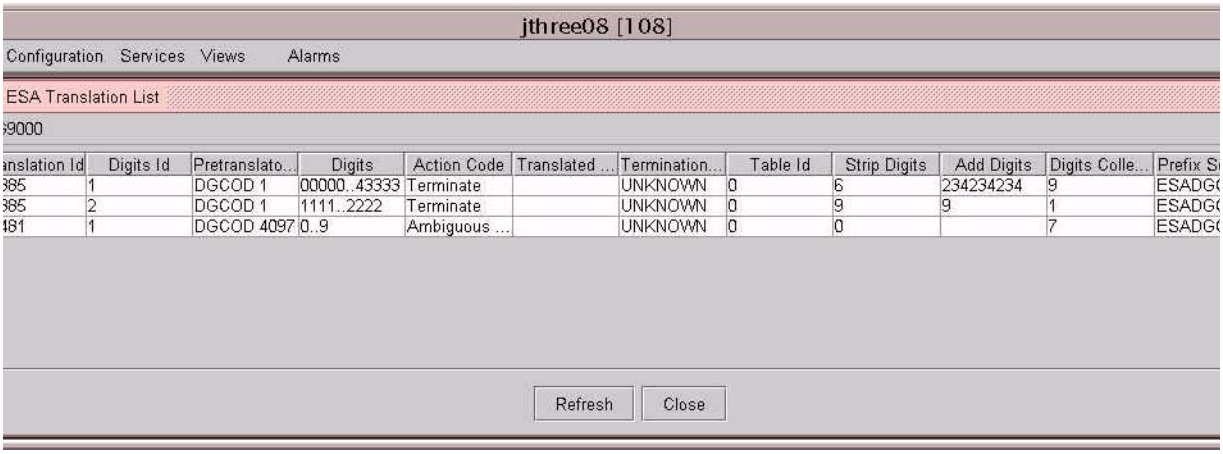
The following table lists the modified fields for the ESA Translation List View

Table 3 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Source	New	N/A	ESAPLXA IBNXLA and ESADGC OD	Indicates which CORE translator the entry came from.	None
Digits	Changed	N/A	TO..From	For ESADGCOD translation entries this field will display the To and From digits in the 111..222 format.	nnESAPrefixDigits

3.8.2.2.5 Usage example

The following is an example of the new ESA Translation List View:



3.8.2.2.6 GUI release history update

The following fields were added:

- Source

The following fields were modified:

- Digits

3.8.2.2.7 Supplementary information

None

3.8.2.2.8 CLUI Interface

N/A

3.8.2.3 ESA Customer Group List View

3.8.2.3.1 Functional description

This GUI is being enhanced indicate whether the Extension IDs are actually indexes into the EXTN table or the DGCOD table. This will be performed by modifying the existing “Extension ID” column name to “DGCOD ID” when the indexes are for DGCOD.

3.8.2.3.2 GUI usage and implications

This is an existing GUI and there are no changes to the order that the GUIs must be datafilled. The fields added are for display only.

3.8.2.3.3 GUI size

N/A

3.8.2.3.4 GUI fields

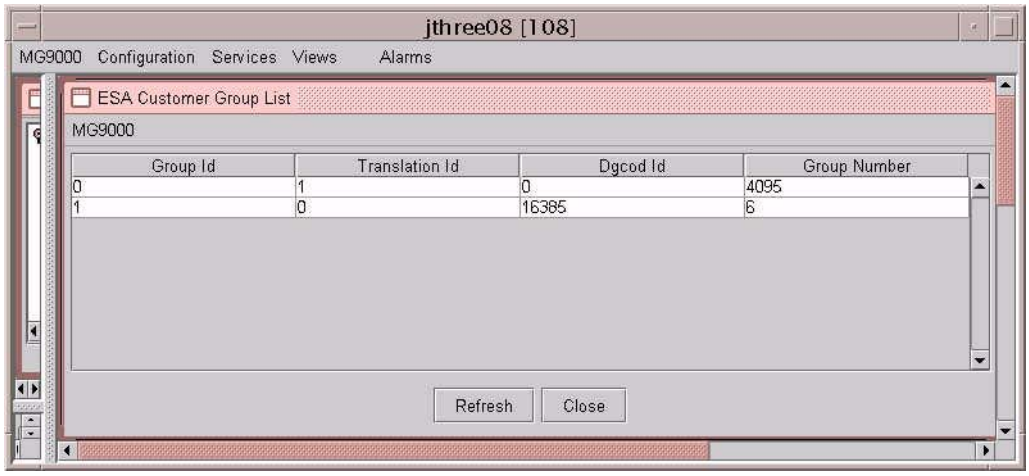
The following table lists the modified fields for the ESA Translation List View

Table 4 GUI field descriptions

Field	New or Changed	Subfield	Entry	Explanation and action	Associated MIB entry
Extension ID/DGCOD ID	New	N/A	read only	The Extension or DGCOD index.	

3.8.2.3.5 Usage example

The following is an example of the new ESA Translation List View:



3.8.2.3.6 GUI release history update

The Extension ID column name will now read DGCOD ID whenever the indexes are for a DGCOD table, international.

3.8.2.3.7 Supplementary information

None

3.8.2.3.8 CLUI Interface

N/A

3.9 Command interface changes

N/A

3.10 Security

N/A

3.11 Configuration Walkthrough

N/A

Product = CS 2000

A00010168 -- H.323 support for COnnected Line Presentation/COnnected Line Restriction (COLP/COLR)

Functional Description

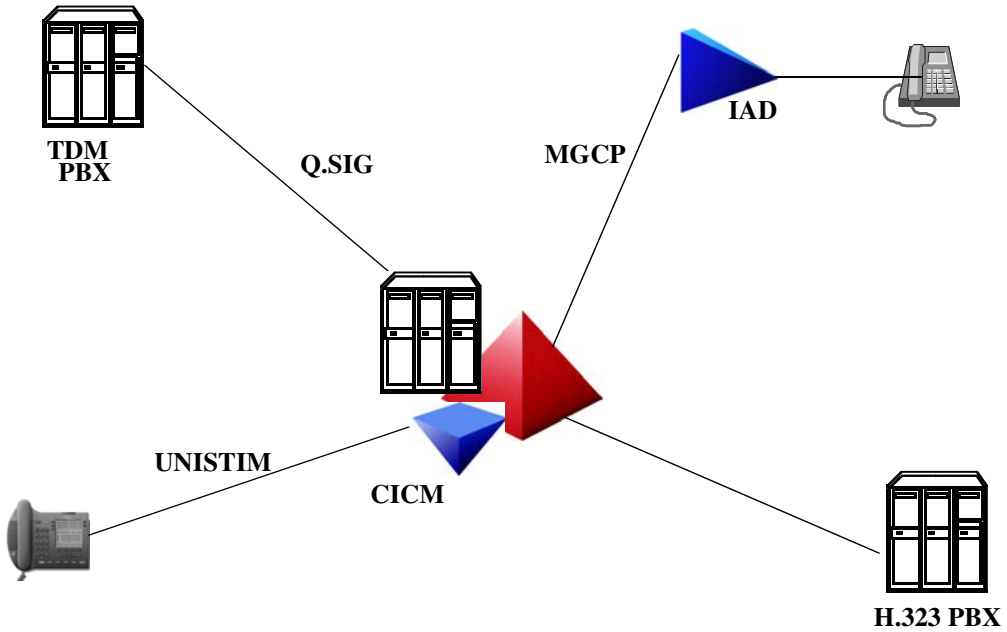
1: Applicable Solution(s)

Int'l CHS

1.1 Description

This feature is to support COLP/COLR on International H.323 Gateways. In the context of H.323, QSIG (Q-reference point SIGnalling) is a private (i.e. corporate) network signaling protocol for communication between ISDN Private BranchExchanges (PBX). In respect to H.323 GWs Q.SIG will be used between H.323 and the core. COLP/COLR are existing QSIG functionalities. No new COLP/COLR capabilities are introduced by this feature. Refer to the following figure.

Figure 1: Agent Interworkings over which COLP/COLR Mapping will be supported



1.1.1 COnnected Line Identification Presentation

COnnected Line Identification Presentation (COLP) supplementary service (SS) provides the calling party with the possibility to receive the connected users number.

COLP has the following functionalities:

- Provides the calling user with the connected number (CNN).
- The CNN IE is provided in the CONNECT message.
- The service is provided on a per trunk-group basis, datafilled in table LTDATA.

When the COLP SS is activated, the Connected Party Subaddress Information Element (CNS IE), if provided by the connected user is included in the CONNECT message if COLR is not activated.

For a Private call, provisioning is not required for the presentation of the CNN or the CNS IEs. Whenever a CNN IE and CNS IE are received they are transparently passed on.

Supposing no information is provided by the connected user, the network provides the Default Number associated with the connected user. The DFLTCNN option in table LTDATA stores the Default Connected Number for the terminating side. If this is not datafilled then no digits are sent across to the originating side.

If the Presentation number is datafilled, then COLP enables the originator to receive the connected presentation number. If NOSCRN option is datafilled, then the COLP enables the originator to receive the unscreened connected number.

For a call originated by a QSIG trunk which does not have COLP datafilled in table LTDATA, the COLP SS is not supported. To invoke the COLP SS, the originating QSIG trunk must be defined with the COLP option in table LTDATA. Refer to the following table.

Table 1 Sample Datafill for COLP in Table LTDATA

LTDKEY LTDRSLT
ISDN 4 SERV SERV N N ALWAYS ALWAYS **COLP**

Default Connected Number:

In case, the COLP SS is activated for the originator QSIG trunk and no information (CNN IE) is provided by the connected user or the information

provided is invalid, the network provides the DeFauLT CoNnected Number (DFLTCNN) associated with the connected user's QSIG access in the destination local network. The default connected number is obtained from the DFLTCNN option in table LTDATA associated with the terminating QSIG trunk. The maximum number of connected number digits is 15.

Refer to the following table.

Table 2 Sample Datafill for Default Connected Number in Table LTDATA

LTDKEY LTDRSLT
ISDN 4 SERV SERV N N ALWAYS ALWAYS **DFLTCNN 6966970**

2.2.3 COnnected Line Identification Restriction

COnnected Line Identification Restriction (COLR) supplementary service (SS) enables the connected party to prevent presentation of its number to the calling party.

COLR has the following functionalities:

- The COLR SS is offered at the terminating end.
- It prevents the presentation of the connected number (CNN).
- The service is provided on a per trunk-group basis. For COLR temporary, the default value (allowed/restricted) can be overwritten on a per call basis.
- It prevents the presentation of the Connected Party Subaddress (CNS).
- The COLR SS is offered by a permanent mode (PERM), or by a temporary mode (TEMP):

PERM mode: The COLR SS is invoked automatically by the network on all calls. If the calling party has subscribed to COLP SS, and the COLR SS datafilled as PERM RESTRICT is invoked and the valid CNN IE is sent from the terminating side, then the calling party receives the Connected Number IE with the indication of 'presentation restricted' and the digits not included.

TEMP mode: The COLR SS is invoked on a per call basis. This means that one of the following scenarios occurs, according to the default value set in the network:

a. If the Presentation Indicator (PI) value is supplied into the Connected Number Information Element (CNN IE), then the PI remains as received from the connected user.

b. If the PI value is not supplied into the Connected Number IE, the presentation indicator is set according to the COLR TEMP sub option that could be Allow or Restrict.

Refer to the following table.

Table 6 Sample Datafill for COLR: Table LTDATA

LTDKEY LTDRSLT
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR TEMP ALLOW**
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR PERM RESTRICT**
ISDN 3 SERV SERV N N ALWAYS ALWAYS **COLR TEMP RESTRICT**

2.2.4 Values supported for SI, PI, TON, NPI in CNN IE

The connected number information is contained in the optional connected number information element (CNN IE) of the Q.931 connect message. The CNN IE is coded as shown in fig. 6. Please observe that octet 3 can have 0 or 1 value depending upon the usage. The maximum length of this information element is 24 octets. Refer to the following figure.

Figure 5 Connected Number Information Element (CNN IE)

<table>
<tr><th>Bit 8</th><th>Bit 7</th><th>Bit 6</th><th>Bit 5</th><th>Bit 4</th><th>Bit 3</th><th>Bit 2</th><th>Bit 1</th><th>Octet</th></tr>
<tr><td>0</td><td>1</td><td>0</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Length of Information Element</td><td>2</td></tr>
<tr><td>0/1</td><td colspan="3">Type of Number</td><td colspan="4">Numbering Plan Identification (NPI)</td><td>3</td></tr>
<tr><td>1</td><td colspan="2">Presentation Indicator (PI)</td><td>0</td><td>0</td><td>0</td><td colspan="2">Screening Indicator (SI)</td><td>3a</td></tr>
<tr><td>0</td><td colspan="7">Number Digits (IA5 Characters)</td><td>4.n</td></tr>
</table>

The different option values of Screening Indicator (SI), Presentation Indicator (PI), Type Of Number (TON), Numbering Plan Indicator (NPI) as supported on the DMS100, are explained below.

Refer to the following figure.

Figure 6 Option Values

Screening Indicator (SI)

2	1	
0	0	user-provided, Not Screened
0	1	user-provided, Verified, and Passed
1	0	user-provided, Verified and Failed
1	1	Network Provided

Presentation Indicator (PI)

7	6	
0	0	Allow
0	1	Restrict
1	0	Not available

Type Of Number (TON)

7	6	5	
0	0	0	Unknown
0	0	1	International Number
0	1	0	National Number
1	0	0	Subscriber number

Numbering Plan Identification (NPI)

4	3	2	1	
0	0	0	0	Unknown
0	0	0	1	ISDN Telephony Numbering Plan (E164)
1	0	0	1	Private Numbering Plan

An incoming CNN IE at the terminating side is considered as valid only if the NPI field has "Unknown" or "ISDN Telephony Numbering Plan (E164)" values. Otherwise the information is discarded. The CNN fields from CONNECT message are updated at the CM level to reflect the CNN information that is delivered to the originating interface.

2.2.6 Connected Party Subaddress (CNS)

The purpose of the Connected party subaddress information element is to identify a subaddress associated with the terminator of a call. Please refer to "Figure 12 Format of the Q931 Connected Party Subaddress IE" on page 54.

Figure 12 Format of the Q931 Connected Party Subaddress IE

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Octet
0	1	0	0	1	1	0	1	1
Length of Information Element								2
1	Type of Subaddress			Odd/ even ind	spare			3
Subaddress information								4

For the Connected Party Subaddress the following is done,

- The CNS is mapped to the APP-PSS1 parameter. (For QFT only)
- The CNS is mapped to the ATP parameter in case of ISUP.
- If COLP SS is activated, add the Connected Party Subaddress Information Element to the CONNECT message.
- If COLR SS is activated, the Connected Party Subaddress Information Element is not added to the CONNECT message.
- If the calling user has not subscribed to COLP, then the CNN IE and the CNS info are not sent in the CONNECT message.
- On interworking of QSIG to QSIG, the CNS IE shall be mapped independently of the COLP SS.

The Presentation of the CNS IE depends on the following:

Public call:

- When COLP SS is not subscribed, the CNN IE and CNS IE are not sent to the calling user.

- When COLP SS is subscribed and PI = allowed, the CNN IE and CNS E (if available) are sent to the calling user.

- When COLP SS is subscribed and PI = restricted, an 'empty/restricted' CNN IE is sent to the calling user. The CNS IE is not sent in this case.

Private Call:

- The CNN IE and CNS IE are mapped transparently.

- Exception for Originating and END PINX:

- When COLP SS is subscribed and PI = restricted, and empty/restricted' CNN IE is sent to the calling user. The CNS IE is not sent in th

2.2.8 Interworkings

Networked services support for interworking QSIG for H.323-based originating/terminating at a 3rd party based PBX (e.g., Siemens HiPath) should include the following:

- COnnected Line Identification Presentation (COLP) supplementary service (SS).
- COnnected Line Identification Restriction (COLR) supplementary service (SS).

Networked services support for interworking QSIG for H.323-based originating/terminating at a Nortel PBX (e.g., BCM50, BCM 200/400) should include the following:

- COnnected Line Identification Presentation (COLP) supplementary service (SS).
- COnnected Line Identification Restriction (COLR) supplementary service (SS)

1.2 Limitations and restrictions

There is no attempt within this feature to map MCDN versions of COLP/COLR to H.323 or to Q.SIG. This feature merely maps Q.SIG versions of COLP/COLR to H.323 versions of COLP/COLR (and vice versa). The following provide specific examples of messaging in MCDN environments

This feature is implemented exclusively for the support of International H.323 COLP/COLR. Refer to A59027747 QSIG Support for COLP/COLR for additional restrictions on COLP/COLR.

1.3 Glossary

TERM	DESCRIPTION
CNN	Connected Number
CNN IE	Connected Number Information Element
CNS	Connected Number Subaddress
CNS IE	Connected Number Subaddress Information Element

TERM	DESCRIPTION
COLP	COnnected Line identification Presentation
COLR	COnnected Line identification Restriction
QSIG	Q Interface Signaling
SS	Supplementary Service

1.4

References

1. AF7494, PLS DOC, COLP/COLR
2. AR2191, PLS DOC, ND ISDN SVCs:WT: Basic Call Services
3. AJ5284, PLS DOC, Presentation CLI Support
4. AU3248, PLS DOC, COLP/COLR Phase I
5. COLPRDOC in FMDOC, PRI COLP/COLR Phase II
6. A59012493 in FMDOC, PRI COLP/COLR Phase III
7. ETS 300-173 Specs
8. ECMA 148 Specs
9. ITU Q.699 Interworking Between ISDN access and non-ISDN access over ISUP SS #7
10. AE0975, CLIP/CLIR, Supplementary Services
11. A59027747 QSIG support for COLP/COLR.

Product = World Trade

A00006663 -- DDRM Alarms and Audits

1: Applicable solution(s)

Int'l DMS

1.1 Introduction

DDRM (DMS Dicle Remote Module) project provides remote LCM node facility to DRX-4 rural exchanges in Turk Telecom network.

This activity handles two components: Alarms and OM & LOGS

- **Component 1. Alarm**

DDRM is capable of detecting and reporting faults for almost all hardware cards. This feature enables to follow up those alarms via OM, LOGs & MAPCI and allows the craftperson to specify the faulty cards remotely. Alarm severity are positioned properly on MAPCI and activate proper processes in DDRM Maintenance SW. Node Status is set to SBSY or ISTB and/or related line states are set to lockout state till the recovery messages are received by DDRM in brief.

Solicited Queries of configuration are made by basic DMS MTC process.

*** RTS:** In test phase all DDRM Alarms are cleared except LC Alarm to refresh permanent alarm conditions in case of any missing recovery messages: **this cleanup is done if only both units are out of service**

Then status of cards datafilled at LCMINV is requested by DMS during test phase. DDRM bundles those status in one ack. response message (implemented ISN08 Activity A00006661). DDRM rescan the alarm conditions and reports all card faulty once it gains the activity.

*** TEST PM:** This clears all DDRM Alarms except LC Alarms on DMS if both unit states are out of service. DDRM reports the mismatch on the configured / datafilled cards at LCMINV in reply. DDRM is expected to produce the current alarm messages if alarm condition remains after INSV state by means of unsolicited messages.

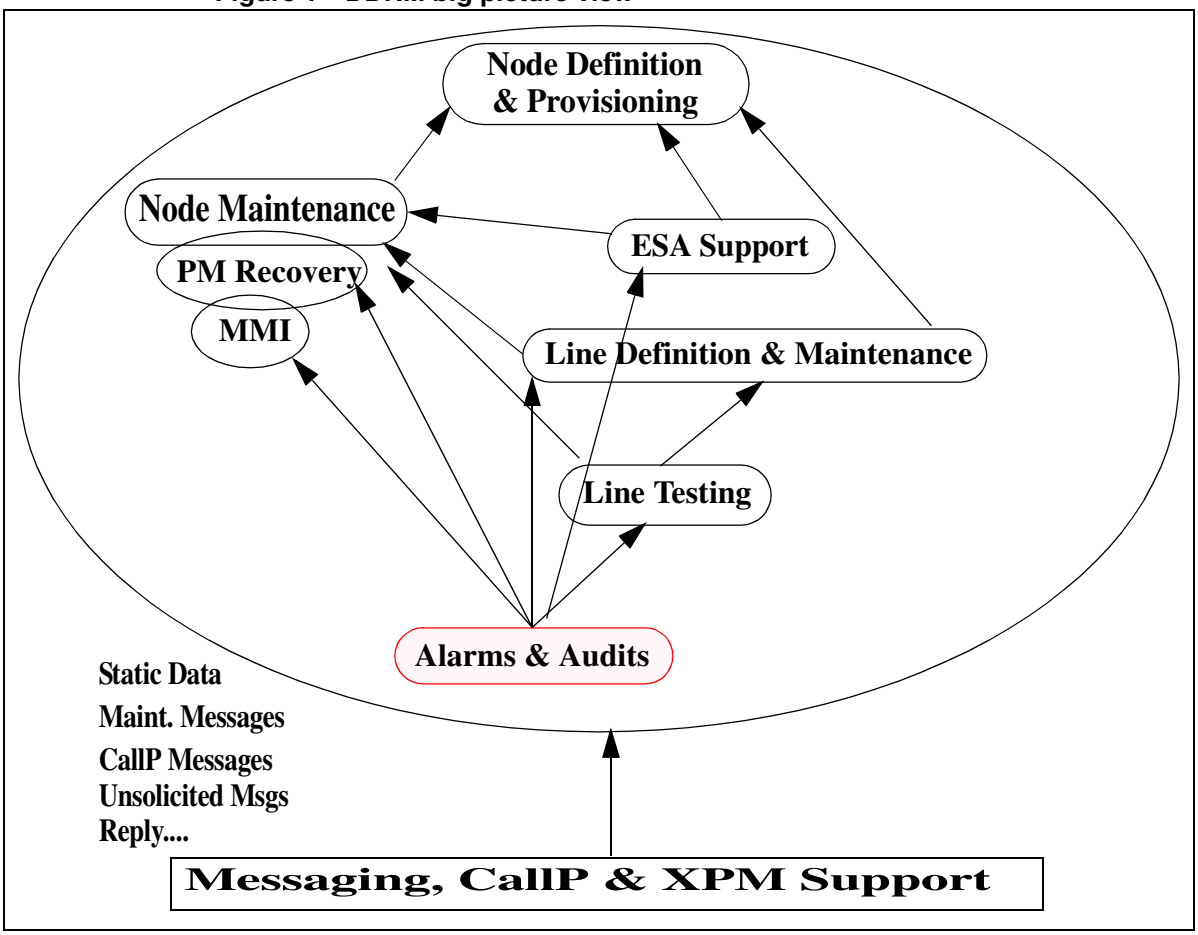
*** AUDIT**: Existing RLCM Node and Line Audits continue to work for DDRM. For babbling faults, DMS Babbling Audit and recovery may commence diagnostic tests for recovery of the alarms if Babbling is reported: DDRM is not capable of reporting babblings on the line at ISN09 but DMS is ready to accept. As such babbling is not testable.

DMS doesn't limit to send existing audits, queries and maintenance messages for DDRM: DDRM is expected to ignore those messages as they are not useless for DDRM.

- **Component 2. OMs**

This component aims changes to reuse the existing OM of RLCMs for new RLCM variant - DDRM. Figure 1 on page 2138 shows the big picture view and how this part of the project fits in the overall project:

Figure 1 DDRM big picture view



1.2 Alarms - Generic Behavior

The following alarms are reported by DDRM node to DMS:

- Module Alarm
- Card Configuration Alarm
- POC Alarm
- Ring Alarm
- -48v Alarm

DDRM reports the mismatches during RTS if the configuration data sent by DMS according to the datafill at LCMINV doesn't match the real configuration on DDRM shelves. Mismatches are registered as an alarm and be monitored by executing Query Fault for posted at MAPCI:MTC:PM Level.

When the reasons occurred on DDRM for those alarms the modified DMS-X / LCM messages are sent to DMS. After the reception of this indication, DMS

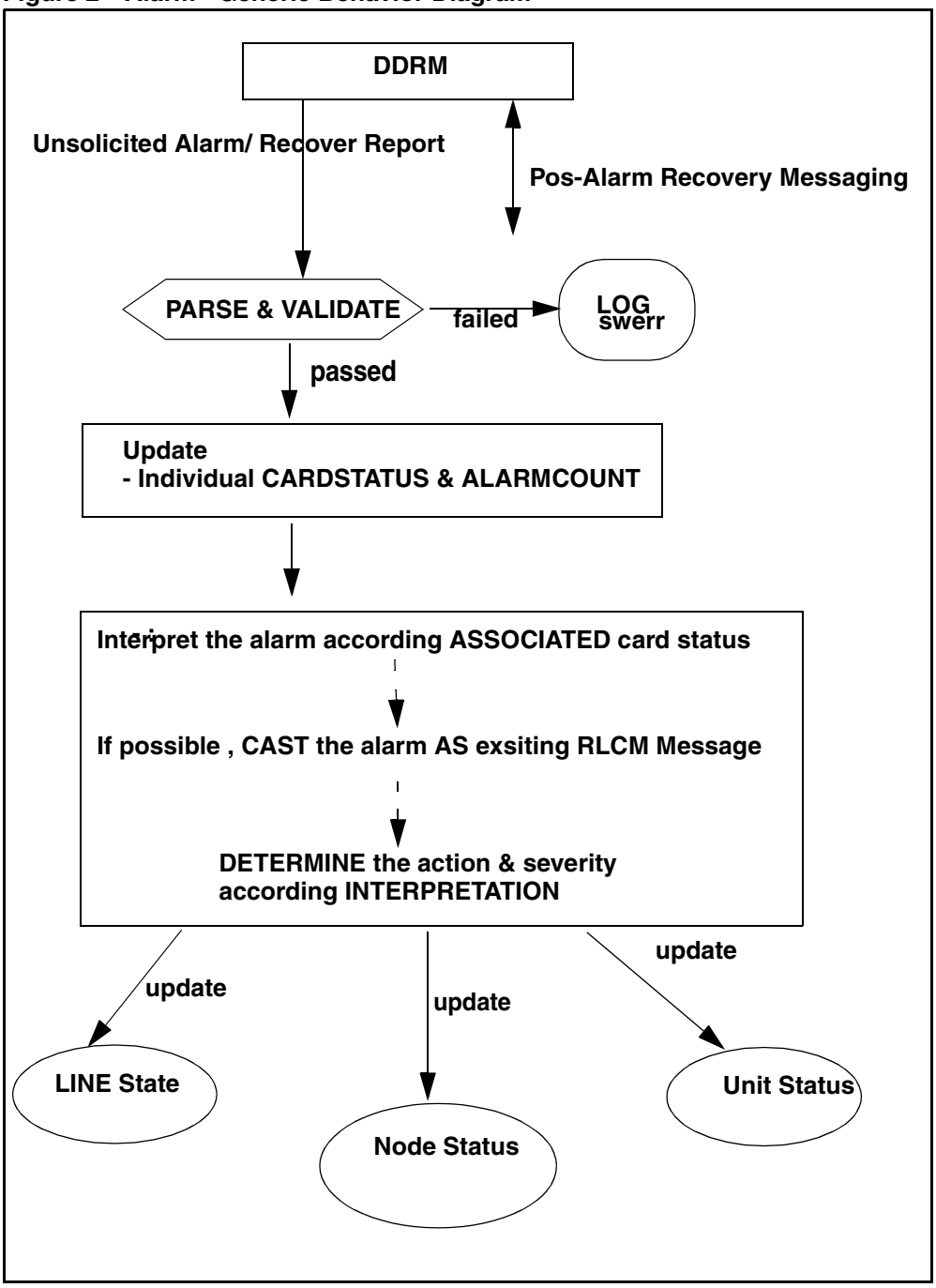
takes the related actions like changing the state of DDRM and / or changing the state of lines and managing the call processing related facilities etc.

When the reasons which cause the alarms are recovered DDRM sends the modified DMS-X / LCM messages to DMS. After that DMS takes the related actions and the service facilities of DDRM node and it's subscribers continue as expected.

DMS-X/LCM messages conveys the faulty card address as the subject of recovery or alarmed condition.

DMS accept those messages if node state is INSV or ISTB status: **any reports are ignored by DMS for status except of INSV or ISTB status.**

Figure 2 Alarm - Generic Behavior Diagram



1.2.1 Additional Queries By DMS

RTS and TEST PM queries GNS, MXC, UTR, LTT-TMS, DTCs if those are datafilled at LCMINV properly (ISN08 MTC Activity).

ISN09 DDRM enables to reports all of alarms once it gains the activity.

RTS fails if bundle ack message includes the alarms which causes a SBSY condition on Node Status. status for these cards: This messaging is done by Test Sub-routine of RTS process, which is also called during TEST PM command.

All alarms are cleared during Test Phase of TST./RTS/or SBSY->RTS transition if node status is not ISTB/INSV.

Other queries are relevant with Node Audit and Line Diagnostics: those audits may enable DDRM to rescan the alarms and report unsolicited (not expected as reply against audit/recover messages) if the need is raised.

1.2.2 Alarm Conditions and Severity Map

The following table gives the problem reasons which cause alarms, their severity class, the state of DDRM after reception of the alarm and the existence of a recovery message for them, as described at DMS_DDRM Spec. Document at FMDOC.

Any individual module alarm does not reveal a problem associated with single or both units of DDRM. For example an MXC controls the LCs on its shelf and each shelf contains odd and even subdrawers (equivalent 4xLC = 1 Subdrawer of a standard LCM), where RLCM even drawers are controlled by unit0 whilst odds are under control of unit1. So an individual MXC cannot indicate a single unit problem.

When a alarm occurs for DDRM node it is shown on DMS MAP level. For the display of alarms on DMS MAP level see section.

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/LCM report message (From DDRM)	DDRM state	Modified DMS-X/LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
Last GNS Card (single and double plane)	+			+	SYSB	+	

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/LCM report message (From DDRM)	DDRM state	Modified DMS-X/LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
One GNS Card (double plane)		+		+	ISTB	+	Both units of DDRM is INSV.
One DTC card (for 2 DTC configuration)		+		+ [1]	ISTB	-	The DDRM unit which is connected to the DTC card with problem is in SYSB state and DDRM is in take-over mode. The other unit is in INSV and DDRM state is ISTB. Any clean-up is not expected on SYSB unit because DDRM is ISTB state. The existing calls which are connected through this DTC should be released by DDRM / DMS. If there is no problem with E1 links then they are taken from the service.
Last DTC card	+			+ [2]	CBSY/ SYSB	NA	The alarm report message is expected if there is at least one E1 available.

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/LCM report message (From DDRM)	DDRM state	Modified DMS-X/LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
One MXC card		+		+	ISTB	+	The subscribers on the same shelf with this MXC card are not given any service facilities and their state are set to LO. DDRM state is ISTB. LTT / TMS, UTR, POC & RG cards on the same shelf are assumed as out of service even if there are no alarm messages specific for these cards. If LTT / TMS cards are on the same shelf then MTA tests are affected for all subscribers
Last MXC card	+			+	SYSB	+	
One UTR card			+	+	ISTB	+	
Last UTR card		+		+	ISTB	+	
LTT - TMS card		+		+	ISTB	+	The messages are received separately for each card.

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/LCM report message (From DDRM)	DDRM state	Modified DMS-X/LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	Critical	Major	Minor				
One POC card			+[3]	+	ISTB	+	The POC card alarm can not be provided from DDRM for standby POC card. **So when a problem occurs on the standby POC card** the alarm severity class is based on MXC and GNS cards. But for any reason a POC alarm about the standby card is received but any other alarm message e.g. like MXC on this shelf is not received standby POC alarm is seen on DMS MAP but subscribers are expected to continue their service facilities as before this alarm. If there is not any Critical alarm reason then DDRM state is ISTB.
Last POC card	+			NA	SYSB	NA	When a problem on last POC card occurs E1 links are went down and the problem can not be reported.*DDRM node is restarted*. If this alarm is received because of any reason but not any other alarm condition (e.g about DTC,MXC & GNS) occurs then POC alarm is received by DMS but subscribers are expected to continue their service facilities as before this alarm.
One -48V input			+	+	ISTB	+	

Table 1: Alarm - Severity

Card problems & subscriber alarms on DDRM	Alarm severity Class			Modified DMS-X/LCM report message (From DDRM)	DDRM state	Modified DMS-X/LCM Recovery message (From DDRM)	Remarks
Card problems on DDRM	**Critical**	**Major**	**Minor**				
2nd -48v	+			NA	SYSB	NA	When the 2nd -48v problem occurs E1 links are went down and the 2nd 48v problem can not be reported. If this alarm is received because of any reason but not any other alarm condition (e.g about DTC,MXC & GNS) occurs then -48v alarm is received by DMS but subscribers are expected to continue their service facilities as before this alarm.
Ringing generator on one POC card			+	+	ISTB	+	
Ringing generator on standbyPOC card		+		+	ISTB	+	
Last ringing generator on POC card	+			+	ISTB	+	
Subscriber alarms on DDRM [4]							
Line is defined but there is no H/W				+	Not affected	+	
Line is defined but there is wrong card				+	Not affected	+	
Hazard / Babbling				+	Not affected	+	

Note 1: If the DTC alarm message is received and there is no E1 link problem between this DTC card and DMS the alarm report message is expected from both units. The existing calls which are connected by this DTC card are released **by DDRM / DMS.** The related E1 links are taken from the service for not to assign a speech channel through them.

Note 2: The alarm report message is expected for the last available DTC card if there is at least one available E1 link.

Note 3: It is a Critical alarm for a single plane configuration.

Note 4: Subscriber alarm is expected for the cases; a- during the initializing phase b-RTS DRWR command c-TST DRWR command d-card out. The alarm severity class of the defined conditions for DDRM subscribers are based on the existing threshold value criteria on DMS as office based.

1.2.3 Module Alarm: GNS

If the CPUs can not be communicated on DDRM node, DMS is informed via the modified DMS-X / LCM message which is sent from DDRM. The CPUs can be on MXC, DTC and GNS cards of a DDRM node. The effect of the alarm changes based on the card type of CPU.
These type of problems are recovered on DDRM node itself.

DDRM is expected to drop the calls which are controlled with GNS in alarmed condition.

If the problem is with one of GNS card then DDRM node is out of order unless there is no standby of GNS card. If there is a standby GNS (double plane configuration) then the service facilities are given to the related modules over the standby GNS. The priority of the alarm is identified based on the message is for the last available GNS or not.

For “double plane” configuration;

- If modified DMS-X / LCM message is received for one of GNS card it means **a Major PM** alarm for DMS. A major alarm indication is seen on DMS and the state of DDRM node is changed to **ISTB** while both units are in INSV. The service facilities of DDRM subscribers are not effected. When the problem with GNS card is recovered then DDRM sends a new defined DMS-X / LCM message to DMS. If there is not another alarm or problem, “Major PM” alarm indication is cleared on DMS MAP and the state of DDRM node is changed to INSV again.
- If the 2nd of modified DMS-X / LCM message is received for the remaining GNS card it means a **Critical PM** alarm for DMS. A critical alarm indication is seen on DMS and the state of DDRM node is changed as **SYSB** on DMS. DDRM node stays in SYSB state until a message about the recovery of at least one GNS card is received. The existing procedures on DMS for a critical PM alarm on a remote node is valid (call processing stops, state changes of DDRM node and its’ subscribers etc). If at least one of GNS card problem is recovered DDRM sends a new defined DMS-X / LCM message to DMS. After that if there is not another alarm or problem, the state of DDRM is returned to ISTB from SYSB. If the problem with the

2nd GNS card is also recovered then the state of DDRM is changed to INSV from ISTB. Call processing and other service facilities continue as expected.

For "single plane" configuration if the modified DMS-X / LCM message is received for the problem on GNS card it means a **Critical PM** alarm for DMS. A critical alarm indication is seen on DMS and the state of DDRM node is changed as **SYSB** on DMS. DDRM node stays in SYSB state until a message about the recovery of the GNS card is received. The existing procedures on DMS for a critical PM alarm on a remote node is valid (call processing stops, state changes of DDRM node and its' subscribers etc)

When the problem is recovered then DDRM sends a new defined DMS-X / LCM message to DMS. If there is not another alarm or problem, **Critical PM** alarm indication is cleared on DMS MAP and the state of DDRM node is changed to INSV again.

The details of this alarm is queried via "QueryPM FLT" command on PM level.

1.2.4 Module Alarm: MXC

If there is a problem with MXC card then the subscribers which are on the same shelf with this MXC are not given any service. It means a **Major PM** alarm for DMS. DMS changes the state of DDRM node to **ISTB**.

*A*ll lines (LMB), UTR, LTT, TMS, POC and RG cards on the shelf are out of service along the period of alarmed condition. The service facilities for the subscribers which are controlled by MXC cards on other shelves continue without any interruption.

MXC Alarms raise LC alarms on the shelf of the alarmed MXC and all datafilled lines on the shelf goes to LO until recovery of MXC alarms.

For all card alarms are displayed as MXC Alarmed once Query LC command is executed. All applications that utilize attr, ltt-tms functions are expected to check MXC alarms first: if MXC is alarmed, the application assume that other cards relevant with the shelf of MXC alarmed are out of service.

If MXC alarm is recovered, all LC alarms of the cards that equipped on the shelf of MXC are cleared at DMS, all equipped/datafilled lines goes to IDLE. Other card status are returned to the status that is set prior to MXC Alarm. And DDRM is expected to reports the alarms after rescan is done once MXC recovers on DDRM. (LTT/TMS, UTR, POC and RG).

The modified DMS-X / LCM message is separately received for each MXC card problem and DDRM state is ISTB. If all MXC cards on a DDRM node have problem then all subscribers are effected and it means a **Critical PM**

alarm for DMS. The state of DDRM node is changed as SYSB on DMS. The existing behaviors of DMS will be kept for line states.

When the problem with the MXC card is recovered DDRM sends the modified DMS-X / LCM message to DMS. This message is separately sent for each MXC card. After that if there is not another alarm or problem the line states of subscribers are changed automatically and the service facilities of subscribers which are controlled by this MXC are started. The state of DDRM node stays in ISTB until the problems for all MXC cards are recovered in case that no another ISTB reasons exist.

The details of this alarm is queried via “QueryPM FLT” command on PM level. All cards are displayed as MXC Alarm or the current alarms are masked with MXC Alarm when DDRM reports MXC Alarm exception message. Upon receiving Recover Message, masks on the current alarms disappeared and previous alarm are displayed if no recover message is received regarding to the previous alarm.

1.2.5 DTC Problems

1.2.5.1 DTC Hardware and Setup Configuration on DDRM

The sharing of E1 link indexes according to 2 DTC card and 4 E1 link configuration on DDRM:

- **The E1 links with 0th and 2nd indexes** are connected to DTC 0 and they are assumed as Unit 0. The 1st channel of E1 primary link (with 0th index) is the messaging channel.
- **The E1 links with 1st and 3th indexes** are connected to DTC 1 and they are assumed as Unit 1. The 1st channel of E1 primary link (with 1th index) is the messaging channel.

The number of message channels for DDRM are based on DTC card configuration as defined below;

- **2 DTC card with 2 / 1 E1 links -** Each DTC has one message channel and each DTC card means a unit of DDRM node
- **1 DTC with 2 E1 links -** This DTC card has two message channels and each E1 means a unit of DDRM node
- **1 DTC with 1 E1 link -** This DTC card has one message channel and only one unit of DDRM is in-service. This means that DDRM node is in takeover mode.

At least one DTC is expected on DDRM side. If one of two messaging channels are full then takeover occurs and the subscribers on this unit are given their service facilities over the other units’ message channel. If the speech channels of a unit is full other unit’s speech channels are used. But its’ message

channel is in-service and DMS sends the messages over the available 2 message channels.

See the following table for the number of E1 link and message channels based on the relation between DMS datafill and DDRM configuration.

Table 2:DDRM units based on the DTC & E1 datafill on DMS and DDRM configuration

DMS datafill	DDRM config	DDRM Unit 0	DDRM Unit 1	Remarks
DTC 0 : 2 E1 DTC 1 : 2 E1	DTC 0 : 2 E1 DTC 1 : 2 E1	INSV (One message channel & 2 E1 link)	INSV (One message channel & 2 E1 link)	
DTC 0 : 1 E1 DTC 1 : 2 E1	DTC 0 : 1 E1 DTC 1 : 2 E1	INSV (One message channel & 1 E1 link)	INSV (one message channel & 2 E1 link)	
DTC 0 : 1E1 DTC 1 : 1 E1	DTC 0 : 1E1 DTC 1 : 1 E1	INSV (one message channel & 1 E1 link)	INSV (one message channel & 1 E1 link)	
DTC 0 : 2 E1 DTC 1 : 1 E1	DTC 0 : 2 E1 DTC 1 : 1 E1	INSV (one message channel & 2 E1 link)	INSV (one message channel & 1 E1 link)	
DTC 0 : 2 E1 DTC 1 : -	DTC 0 : 2 E1 DTC 1 : -	INSV (one message channel & 1 E1 link)	INSV (one message channel & 1 E1 link	
DTC 0 : - DTC 1 : 2 E1	DTC 0 : - DTC 1 : 2 E1	INSV (one message channel & 1 E1 link)	INSV (one message channel & 1 E1 link	
DTC 0 : 1 E1 DTC 1 : -	DTC 0 : 1 E1 DTC 1 : -	INSV (one message channel & 1 E1 link)	MANB / CBSY	
DTC 0 : - DTC 1 : 1 E1	DTC 0 : - DTC 1 : 1 E1	MANB / CBSY	INSV (one message channel & 1 E1 link	
DTC 0 : 2 E1 DTC 1 : 2 E1	DTC 0 : 1 E1 DTC 1 : 1 E1	ISTB (One message channel & 1 E1 link	ISTB (One message channel & 1 E1 link)	DDRM does not send an E1 alarm for DTC 0 & DTC 1.

DMS datafill	DDRM config	DDRM Unit 0	DDRM Unit 1	Remarks
DTC 0 : 2 E1 DTC 1 : 2 E1	DTC 0 : 1 E1 DTC 1 : 2 E1	ISTB (One message channel & 1 E1 link)	INSV (One message channel & 2 E1 link)	DDRM does not send an E1 alarm for DTC 0.
DTC 0 : 2 E1 DTC 1 : 2 E1	DTC 0 : 2E1 DTC 1 : 1E1	INSV (one message channel & 2 E1 link)	ISTB (One message channel & 1 E1)	DDRM does not send an E1 alarm for DTC 1.
DTC 0 : 2 E1 DTC 1 : -	DTC 0 : 2 E1 DTC 1 : 2 E1 / 1 E1/ -	INSV (one message channel & 1 E1 link)	INSV (one message channel & 1 E1 link	Both E1 links should be connected to DTC 0. DTC 1 is not configured on DDRM.
DTC 0 : 2 E1 DTC 1 : -	DTC 0 : 1 E1 DTC 1 : 2 E1 / 1 E1/ -	ISTB (one E1 is available & 1 E1 link)	MANB / CBSY	E1 link should be connected to DTC 0. DDRM does not send an E1 alarm for DTC 0. DTC 1 is not configured on DDRM.
DTC 0 : 1 E1 DTC 1 : -	DTC 0 : 2 E1 DTC 1 : 2 E1 / 1 E1 / -	ISTB (one message channel & 1 E1 link)	MANB / CBSY	DTC 1 is not configured on DDRM.
DTC 0 : - DTC 1 : 2 E1	DTC 0 : 2 E1 / 1 E1 / - DTC 1 : 2 E1	INSV (One message channel & 1 E1 link)	INSV (one message channel & 1 E1 link	Both E1 links should be connected to DTC 1. DTC 0 is not configured on DDRM.
DTC 0 : - DTC 1 : 2 E1	DTC 0 : 2 E1 / 1 E1 / - DTC 1 : 1 E1	MANB / CBSY	ISTB (one message channel & 1 E1 link)	E1 link should be connected to DTC 1. DDRM does not send an E1 alarm for DTC 1. DTC 0 is not configured on DDRM.

DMS datafill	DDRM config	DDRM Unit 0	DDRM Unit 1	Remarks
DTC 0 : - DTC 1 : 1 E1	DTC 0 : 2 E1 / 1 E1 DTC 1 : 2 E1	MANB / CYSB	ISTB (one message channel & 1 E1 link	E1 link should be connected to DTC 1. DTC 0 is not configured on DDRM.
DTC 0 : - DTC 1 : -	**Not allowed configuration on DMS**			

ISN09 Table Control SW is enhanced and new optional keys are defined to configure DTC cards. New tuple will be in following format:

DTC0/1_values can be 0, 1, 2 as corresponding to SINGLE, DOUBLE, NONE in order.

DDRM needs two messaging channels at least. LCMINV allows user to datafill C-side ports of DDRM connected to PLGC and forced to datafill the first two ports. Those two ports are indicated as Messaging E1 and carry the messaging channel for units, separately. E1-0 for unit0, E1-1 for unit1.

At least one DTC must be datafilled otherwise add/change fails in datafill on LCMINV.

When DTC0=0/2 (Single/None) and DTC1=2/0 (None/Single,) Table Control SW produces a warning ('UNIT-.... CANNOT BE INSV/ISTB') & ('UNIT-.. TAKEOVER') accordingly.

New enhancements allows user to define DTC Number and Channel Configuration as shown below:

Table 3: LCMINV DTC vs. Channel Configuration

DTC0	DTC1	DTC0 1th E1	DTC0 2nd E1	DTC1 1th E1	DTC1 2nd E1
DOUBLE	-	M	M	-	-
-	DOUBLE	-	-	M	M
DOUBLE	DOUBLE	M	S	M	S
DOUBLE	SINGLE	M	S	M	-
SINGLE	DOUBLE	M	-	M	S
SINGLE	SINGLE	M	-	M	-

Table 3: LCMINV DTC vs. Channel Configuration

DTC0	DTC1	DTC0 1th E1	DTC0 2nd E1	DTC1 1th E1	DTC1 2nd E1
SINGLE	-	M	-	-	-
-	SINGLE	-	-	M	-

SINGLE: It presents capacity covering 1 message channel and 29+30= 59 Speech Channels on the DTC (with HDLC).

DOUBLE: It presents the capacity covering 2 Message Channels and 29+29 Speech Channels on the 2xE1 DTC (with HDLC).

M: Messaging Channel

S: Speech Channel

DDRM has configured the channels according to the above table during RTS. If no DTC card exists on the slot physically against the configuration, no alarm is needed to fail the RTS for unit: it is expected that DMS cannot communicate with DDRM and RTS cannot start for this specific unit.

RTS fails for the unit for which DTC Mismatch is reported. RTS logs the fail reason for related DTC.

1.2.5.2 DTC Alarm Handling

DTC Unsolicited Exception Reports cause to log the alarm and display via QueryPM FLT on DMS. Each DTC Alarm causes to down the relevant unit according to the datafill in LCMINV. Recovery message causes to cleanup the alarm: closed E1s are opened within the system recovery started by DMS.

An special (rare) exceptional condition may occur when any DTC loss the connection with other module cards: in this case DDRM is expected to close the M+S Channels of unit which the DTC is alarmed and associated with for that reason. DDRM needs to know this condition and doesn't produce virtual module alarms. DMS needs to close this link so this can be achieved to stop the carrier maintenance on this E1 so DMS disconnects the existing calls in TakeOver mode. If other DTC detects this special condition on the DTC and sent the DTC alarm, DMS will drop the unit and takeover is realized.

For the configurations with 2 DTC cards if there is a problem with one of DTC card the service facilities for DDRM node and its' subscribers are given through the remaining DTC card. It means a **Major PM** alarm for DMS. The related unit of DDRM is set to CBSY / SYSB and the state of DDRM node is changed to **ISTB**. When the problem is recovered the recovery alarm message

is sent from DDRM through the available DTC card. If there is not another alarm or problem the state of DDRM node is changed to INSV again.

In case the alarm message is received for the 2nd or for the last available DTC card this means a **Critical PM** alarm for DMS. The state of DDRM node is changed to CBSY / SYSB. If it is allowed on DMS and at least one UTR card is available, ESA-mode is entered on DDRM node.The recovery alarm message is not expected for the first DTC availability. In this case the general DMS-X/ LCM messaging is expected during E1 link alignment as in the existing structure and ESA-Exit procedure is performed. But for the 2nd DTC availability the recovery message is sent through the DTC card which is given into the service previously. If there is not other alarm or problem the critical alarm indication on DMS MAP is cleared. The state of DDRM node is changed to INS.

When DTC card alarm is received and if there is no E1 link problem between this DTC card and DMS the existing calls which are already established through this DTC card are released by DMS / DDRM. Also the related E1 links are taken from the service for not to assign a speech channel.

The details of this alarm is queried via “QueryPM FLT” command on PM level.

1.2.6 Card configuration Alarms

In generic this type of alarm is reported for the problems on peripheral cards of a DDRM node. LC, LTT-TMS and UTR cards are used as peripheral cards. These type of problems are recovered on DDRM node itself.

This message identifies the shelf and slot number and it means a **Major PM** alarm for DMS. A major alarm indication is seen on DMS and the state of DDRM node is changed to **ISTB**. The service facilities of DDRM subscribers are not effected except MTA test facilities.

When the problem with the LTT -TMS cards is recovered then DDRM sends the modified DMS-X / LCM message to DMS. If there is not another alarm or problem, the alarm indication on DMS MAP is cleared and the state of DDRM node is changed to INSV. After that MTA test facilities can be run again for DDRM subscribers.

The details of this alarm is queried via “QueryPM FLT” command on PM level. MTA tests which require LTT-TMS in are effected.

If the UTR cards on DDRM are not on the same slots which are configured on DMS DDRM sends the modified DMS-X / LCM message. This message identifies the shelf and slot number of UTR Card and it means a **Minor PM** alarm for DMS. A minor alarm indication is seen on DMS and the state of DDRM node is changed to **ISTB**. The service facilities of DDRM subscribers

are not effected. This modified DMS-X / LCM message is separately received for each UTR card.

When the message is received for the last remaining UTR card then the services which are given in ESA-mode are effected. It means a **Major PM** alarm for DMS. A major alarm indication is seen on DMS MAP and the state of DDRM node is changed to ISTB.

When the problem with UTR card is recovered then DDRM sends the modified DMS-X / LCM message to DMS. If there is not another alarm or problem, the indication on DMS MAP is cleared and the state of DDRM node is changed to INSV.

MXC recovery also cleanup the LTT, TMS, UTR and LC alarms if those cards are placed on the shelf of MXC.

The details of this alarm is queried via “QueryPM FLT” command on PM level.

LC Card faults:

The card configuration of DDRM node is sent from DMS during the initializing phase. Based on this information DDRM knows the occurrence of the below cases and informs DMS via a modified DMS-X / LCM message for both conditions;

- The line is defined but there is no H/W on LC slot (**etc: card-out**)
- The line is defined but there is a wrong card on LC slot (e.g. UTR or LTT / TMS)

The LC Message has not include any information of above conditions. DMS treat this alarm message as Missing Card Alarm Exception in DMS and MCARD RLCM Line Fault Alarm is raised. Existing RLCM Missing Card Alarm thresholds are kept.

When this message is received from DDRM the states of related lines will be set as LO on DMS

This alarm is also sent;

- during the initializing
- at the end of RTS drwr
- at the end of TST DRWR
- when the card is out of the LC slot

This message identifies the shelf and slot number of LC for 8 ports. When this message is received from DDRM node it causes LO for the lines on the LC of the message.

As an unexpected case if the line states can not be set to LMB because of any reason after the reception of this message from DDRM then the incoming call attempt to this subscriber is ended with **“Ring Failure”** message by remote node as response to **“Ring Request”**. Also DMS Line Audits follows the status of Line.

The details of this alarm is queried via “QueryPM FLT” command on PM level.

Upon reception of LC Recovery message LO Lines returns to IDLE and ready for new calls.

1.2.7 POC alarm

This alarm indicates that the DC voltage level failure on POC card.

The modified DMS-X / LCM message is sent from DDRM and this message identifies shelf number of the POC card. When this message is received it means that there is no standby of +/-5v, +/-12v and -48v between two shelves. It is a Minor PM alarm for DMS. A Minor PM alarm indication is seen on DMS and the state of DDRM node is changed to ISTB.

Generally shelf 1 - shelf 2 and shelf 3 - shelf 4 have standby facility for each other.

This alarm is not service effective and service facilities are not impacted for DDRM node and its’s subscribers unless the standby POC card has a problem.

If both POC cards are alarmed, then the subscribers which are on the same shelves with POC cards are not given any service facilities. In this case DDRM does not send standby POC alarm but sends a Module alarm for MXC cards on the same shelves. If both POC alarms are received for one unit, it means that one of those cards has virtual alarm since POC Alarm circuit can be broken for any reason.

If GNS cards are on the same shelves with these POC cards which have the problem then Module Alarm for GNS cards are received as well. Alarm severity class for MXC and GNS cards are valid.

If POC alarm for standby POC card is received because of any reason but not any other alarm condition (e.g about DTC,MXC & GNS) occurs then POC alarm is received by DMS but subscribers are expected to continue their service facilities as before this alarm. In this case craftperson is required to check the circuits before deciding to take the alarmed POCs off.

If the problem occurs on the last available POC card then the modified DMS-X / LCM message can not be reported because E1 links go down. It means a Critical PM alarm for DMS and DDRM state is SYSB.

These type of problems are recovered on DDRM node itself. When the problem is recovered DDRM sends the modified DMS-X / LCM message to DMS if there is not another alarm or problem. The alarm indication on DMS MAP level is cleared. For the modified message format of these alarm and their recovery message see Appendix chapter of DMS_DDRM.

If a MXC recovery message for the alarmed MXC card which is on the same shelf with POC card is received then POC card alarm is reseated on DMS. In case the continuity of POC card alarm DDRM sends this alarm to DMS again.

1.2.8 - 48 v alarm

There are two -48v input of DDRM node and they have standby facility for each other. This alarm indicates that there is a problem with one of -48v inputs and its' standby facility does not exist.

DDRM sends the modified DMS-X / LCM message and it means a Minor PM alarm for DMS. A Minor PM alarm indication is seen on DMS and the state of DDRM node is changed to ISTB.

This alarm is not service effective and service facilities are not impacted for DDRM node and its's subscribers unless the standby -48v input has a problem.

If both cards are reported as alarmed, the modified DMS-X/LCM message can not be reported because E1 links go down and a Critical PM alarm is seen on DMS. The state of DDRM node is changed to SYSB on DMS MAP level.

If -48v input alarm for standby is received because of any reason but not any other alarm condition (e.g about DTC,MXC & GNS) occurs then this alarm is received by DMS but subscribers are expected to continue their service facilities as before this alarm. DMS will clear the alarm when standby 48V alarm recovery message is sent by DDRM while node status is ISTB/INSV.

These type of problems are recovered on DDRM node itself. When the problem with one of -48v input is recovered DDRM sends the modified DMS-X / LCM message to DMS.If there is not another alarm or problem the alarm indication on DMS MAP level is cleared and the state of DDRM is changed to INSV.

The recovery message is not expected from DDRM for the 2nd -48v input problem in case of all E1s are down since SBSY Test Phase clear all the alarms and node will have INSV if all 48V alarm conditions are remove. Generally, DDRM is expected to rescan the alarms after it gains the activity with RTS.

MXC recovery cleanup the 48V alarms.

1.2.9 Ring alarm

POC cards on DDRM node provide Ringing as well. POC cards on shelf 1-shelf 2 and shelf 3 -shelf 4 have standby facility for each other. If there is a problem with a Ring Generator of these POC cards then the alarm is generated. DDRM sends the modified DMS-X / LCM message and it means a **Minor PM** alarm for DMS. A **Minor PM** alarm indication is seen on DMS and the state of DDRM node is changed to ISTB.

This alarm is not service effective and service facilities are not impacted for DDRM node and it's subscribers unless the standby card has a Ringing generator problem. If then a 2nd Ring alarm is received from DDRM and it means a **Major PM** alarm for DMS. DDRM state is ISTB at this condition and ***continue to give service to the lines even if terminations are without ring.***

In this case the subscribers which are on the same shelf are not given Ringing facility. There is not a direct relation with Ringing Generator problem and MXC, GNS alarms.

If all Ringing Generators have problem for ringing application then it means a **Critical PM** alarm for DMS.

These type of problems are recovered on DDRM node itself. When the problem is recovered DDRM sends the modified DMS-X / LCM message to DMS. The alarm indication on DMS MAP level is cleared (If there is not another alarm or problem).

The details of this alarm is queried via "QueryPM FLT" command on PM level.

1.2.10 Hazard Alarms

If an overvoltage problem occurs on a subscriber with overvoltage option of DDRM then DMS is informed **via modified LCM Line Message.**When this message is received from DDRM the states of related lines will be set as HZD on DMS and existing Hazard DMS MTC is triggered. HZD condition is cleared after Modified Hazard DDRM Unsolicited message is received.

1.2.11 Severity on Display

The following existing LCM display is valid also for DDRM.

Table 4: Critical DDRM Alarm Display on DMS MAP

Alarm Display	CM	MS	IOD	Net	PM	CCS	Lns	Trks
	.	.	.	.	**nLCM** *C*	.	.	.

Indications on Display	“n” indicates the number of LCMs with alarms. “*C*” shows the alarm class “critical”.

Major DDRM Alarm Display on DMS MAP

Alarm Display	CM	MS	IOD	Net	PM	CCS	Lns	Trks
	.	.	.	.	nLCM *M*	.	.	.
Indications on Display	“n” indicates the number of LCMs with alarms. “*M*” shows the alarm class “major”.							

Line Alarm Display on DMS MAP

Alarm Display	CM	MS	IOD	Net	PM	CCS	Lns	Trks
	.	.	.	.	.	.	MCard *M*	.
Indications on Display	“*M*” shows the alarm class “major”.The number of alarm conditions reaches or exceeds the major class threshold.							

Hazard Line Alarm Display on DMS MAP

Alarm Display	CM	MS	IOD	Net	PM	CCS	Lns	Trks
	.	.	.	.	.	.	HZD *M*	.
Indications on Display	“*M*” shows the alarm class “major”.The number of alarm conditions reaches or exceeds the major class threshold.							

1.2.12 Existing Line alarms on DMS

The existing line alarms on DMS are valid for DDRM subscribers as well. See the following table.

Table 5: Supported DDRM Line Alarms

Alarm Status Code	DDRM Action	Description	Remarks
DF	No.	Two or more line circuits have SDIAG, DIAG, NDIAG, FAC, MSET, MCARD, IMIN, IMAJ, UCARD, or QDIAG type alarms that are in the same class.	
FAC	YES	The relevant facility of DIAG tests are out of service this is reported in DIAG tests: etc subscriber loop tests	
DIAG	Yes.	The threshold of line circuits that have failed the extended diagnostic has been reached or exceeded.	Raised as a result of DDRM Line Diagnostic Tests
HZD	Yes	Indicates that a line hazard such as leakage resistance or foreign line voltage has been detected on a card. It also indicates that the cut-off relay has been operated to isolate the line card.	Unsolicited Message from DDRM trigger this alarm or Raised as a result of DDRM Line Diagnostic Tests
IMAJ	Yes	The threshold of line circuits that have reported ICMO at the major rate has been reached or exceeded. ICMO (incoming message overload) is the state where LTC or LGC is receiving too many messages from line card.	This is part of results of DDRM Line Diagnostics (ltp:diag) DMS follows up these errors via Babbler Audits. If DDRM reports babbling via Babbling DDRM Alarm, this is raised.
IMIN	Yes	The threshold of line circuits that have reported ICMO at the minor rate has been reached or exceeded.	This is part of results of DDRM Line Diagnostics (ltp:diag)
MCARD	Yes	The threshold of line circuits that have reported missing line cards has been reached or exceeded.	This is part of results of DDRM Line Diagnostics (ltp:diag). This is also raised by LC Alarm Message.
MSET	Yes	The threshold of line circuits that have reported missing sets has been reached or exceeded.	Raised as a result of DDRM Line Diagnostic/Tests

Alarm Status Code	DDRM Action	Description	Remarks
PSDF	No	On or more line circuits have reported a PSPD type alarm, and one or more line circuits have reported SDIAG, DIAG, NDIAG, FAC, MSET, MCARD, IMIN, IMAJ, UCARD, or QDIAG type alarms, where all alarm types (including the PSPD type) are in the same class.	
PSPD	No	The threshold of lines with a permanent signal condition has been reached or exceeded. The cause may be either partial dialing of a digit sequence or an off-hook condition with no digits dialed.	This is triggered with LO trunks - related to callp on PLGC
QDIAG	No	The threshold of line circuits that are in the shower queue has been reached or exceeded.	
CMIN	No	The threshold of line circuits that have reported CP errors at the minor rate has been reached or exceeded.	
CMAJ	No	The threshold of line circuits that have reported CP errors at the major rate has been reached or exceeded.	

1.2.13 The other existing RLCM specific alarms which are not used for DDRM

The existing RLCM specific alarms which are not used for DDRM are listed below;

- RMM Minor
- ESA Minor
- ESA Critical
- EXT FSP RLCE frame Major

1.2.14 LOGs

Except LC Alarms (LC Configuration, Hazard, Babbling) each DDRM Exception Report are logged with PM179: PM179 Log format has the following information:

- Message Type (recovered or alarmed)
- Card Type
- Shelf
- Slot

- If alarm is LC, HW Status Value (note that this field is valid for Babbling and Hazard for ISN09. Online, Missing and Wrong Card may be printed, however it has no meaning.) is printed as second line.

1.2.15 Alarm Exceptions

- Unexpected values in the fields of exception reports cause PM116 Logs will be produced. SW Swerrs are produced to debug the unexpected value or range. In those cases message is ignored and not registered as alarm or recovered. Printing of PM116 matches the existing behavior of DMS against the RLCM exception reports.
- Any other problems in handling messages (etc exhaust resource due to excessive messages) causes PM116 again.
- After validation, RECOVER reports are accepted if only previous alarm status is TRIGGERED otherwise the message is ignored.No swerr is printed.PM116 is logged.
- After validation, TRIGGER message are received for a card which is already marked as ALARMed, this message is ignored. No Swerr is printed. PM116 is logged.

1.2.16 DDRM OM

This component refers a standard enhancements to pre-existing defined LCM OM definition. There is no requirement to have new OM types.

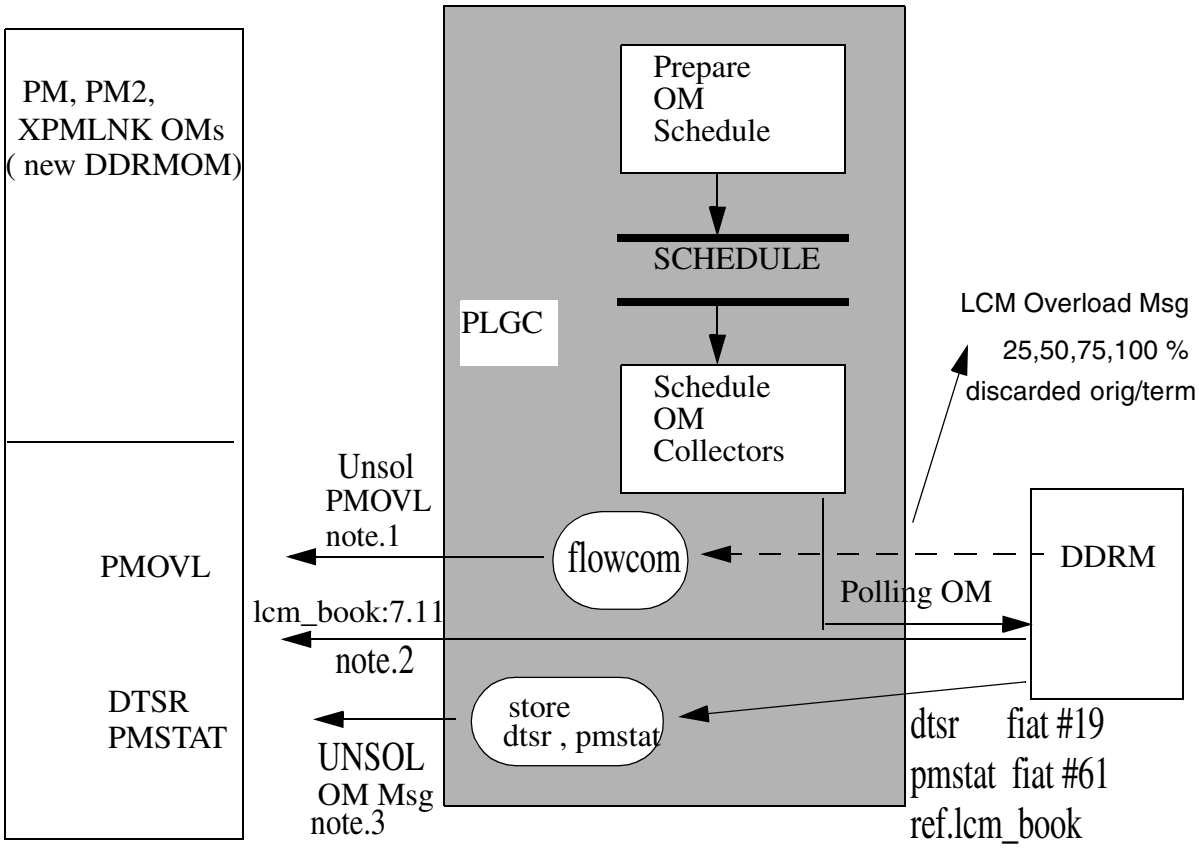
All exception alarms are pegged as PM OMs in the same way RLCM Alarms are received.

Existing DTSR and PMSTAT, PMOVL OM handling is given the following figure.

Among those OMs, Host PLGC sends regular query messages to collect the total calls for a period and delay-dial statistics from DDRM: remote is expected to calculate the dial delays with the help of timestamps of call-origination previously sent by host to DDRM in a message. For complete description, please refer to NTP and DMS_DDRM references. DDRM doesn’t provide those delays, so DTSRs are invalid for DDRM.

DMS is ready to produce DDRM PMOVL OMs in case DDRM simulates or actually gets an action for an overload condition as it produces the relevant messages as defined for RLCMs. DMS existing handling is kept but those OM formats are changed to cover new PM type.

Figure 3 OM Design MAP



Note.1--- Per denied originitaion and terminations XPMOVL

Note2--- This unsolicited message is sent to the XPM from the LCM to indicate that the LCM is being overloaded with call originations, terminations, etc. and thus not processing all DMSX messages that are being sent to it due to a lack of call processing resources.

Note3. (DTSR : Dial Tone Statistic Request Fiat #19) & (PMSTAT : Processor Occupancy Status existing LCM messages (LCM_BOOK fiat : mf_pmstat_re #61)) is handled if DDRM provides or need those messages.

1.3 Hardware Requirements or Dependencies

Figure 4 Logical view of DMS host and DDRM node

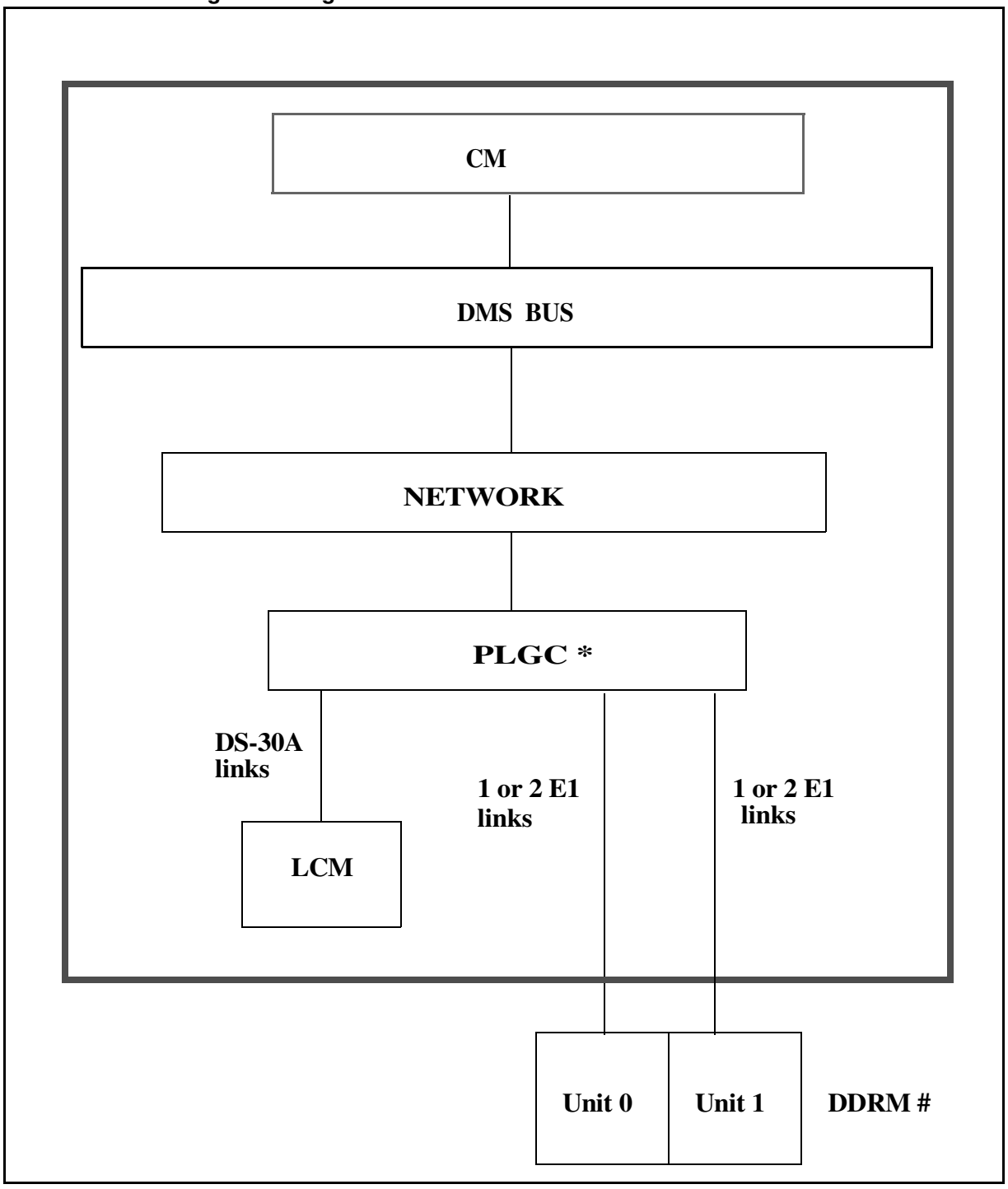
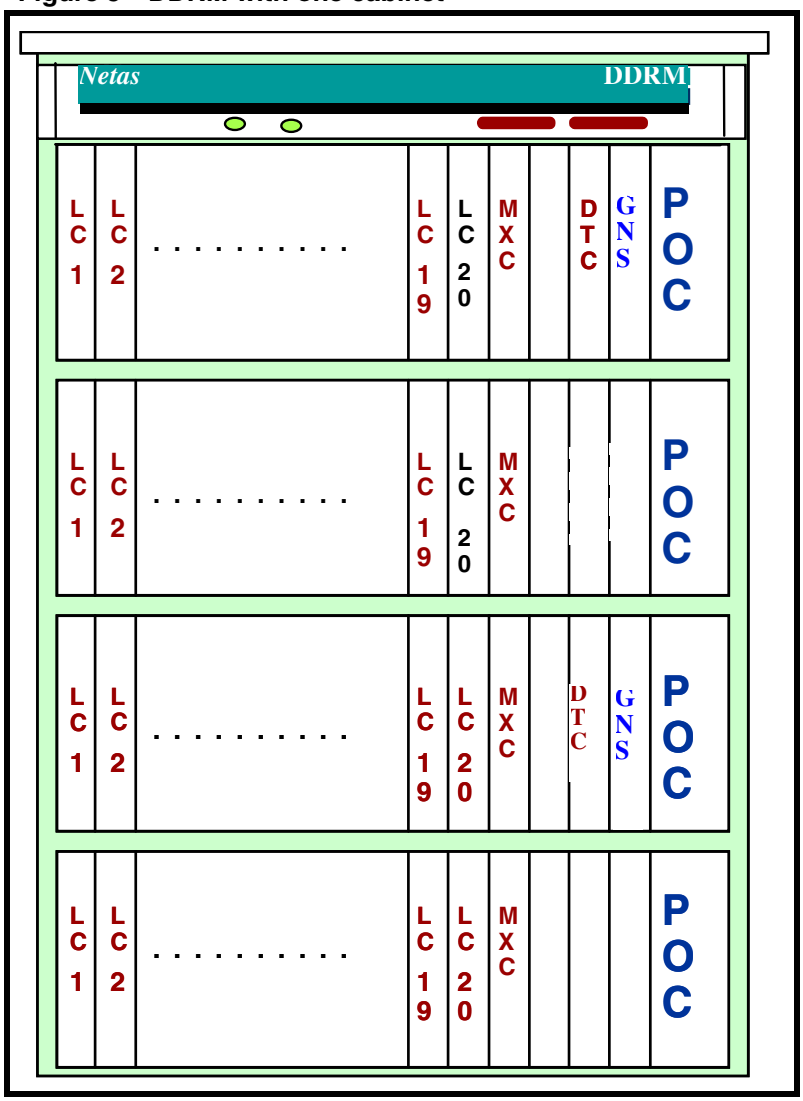


Figure 5 DDRM with one cabinet



1.4 Software Requirements or Dependencies

This feature needs DDRM Hardware and DDRM SW which works at least with single E1 links at worst case. Two-links configuration are needed for recovery phase since DMS doesn't change single UNIT of DDRM.

- A00006660 - for DDRM TABLE CONTROL and resources for ALARM
- A00006661 -for DDRM Maintenance RTS to query alarms.
- A00006662 - for Definition & Maintenance - Line Audits.
- A00006666 - for XPM support and Callp to handle alarms during INSV

Note: These 4 features are available in the (I)SN08 OSS Guide, PLN-i08-OSS.

1.5 Limitations and restrictions

- DMS Existing Audits or no new Audit/Recovery does not detect or recover the long-term alarmed condition. CraftPerson can refresh DDRM DMS alarms by RTS or TEST if both units are out of service when the alarms remains long-term because of any missing recovery message from DDRM.

1.6 Interactions

This activity impacts TEST and ESA Activities which are being implemented at ISN09: tests for allowable cards are exhibited if any LC alarm.

1.7 Glossary

Term	Description
DDRM	DMS Dicle Remote Module
DRX-4	Dicle Rural Exchange-4
DTC	Digital Trunk Card
ESA	Emergency Stand Alone
GNS	Group Network Switching
LC	Line Card
LCM	Line Concentrating Module
LTT	Line and Trunk Test Simulator
MTA	Metallic Test Access
MXC	Module Switching Controller
POC	Power Converter Card
RLCM	Remote Line Concentrating Module
TMS	Test Measurement and Signalling

Product = World Trade

A00006664 -- DDRM Line Testing

1: Applicable solution(s)

Int'l DMS

1.1 Introduction

DDRM (DMS Dicle Remote Module) project as a whole provides a platform which supports DDRM node as a remote line module of DMS like an RLCM (Remote Line Concentrating Module).

This feature is responsible for support of the LTP level test commands of the posted DDRM subscriber lines on a regular MMP switch for ISN09 stream.

1.2 Description

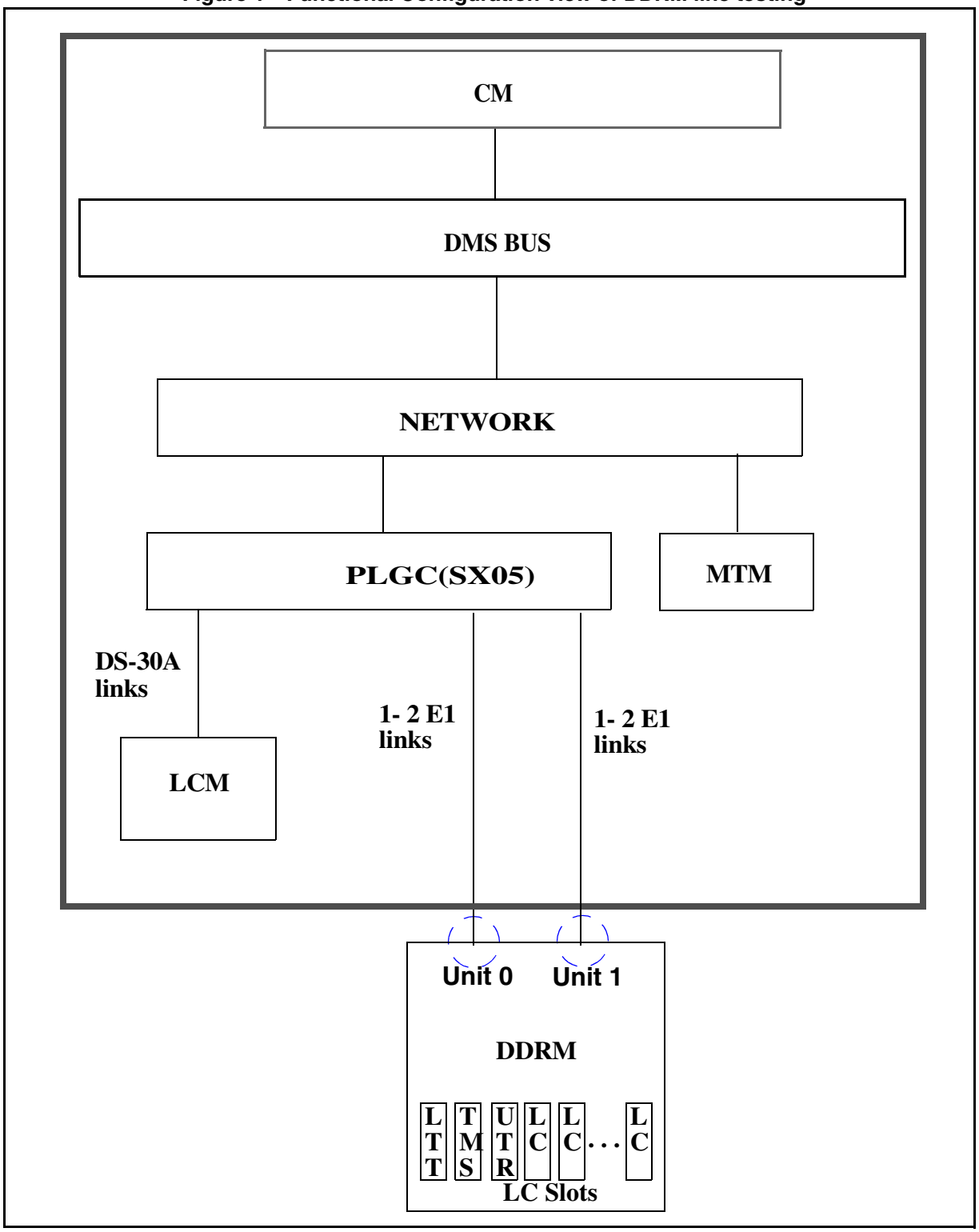
This feature provides support in DMS-MMP product for line testing available in DDRM. The main purpose of this feature is to create an interface between DMS and DDRM through E1 (PCM30) links to execute supported LTP and ALT level test commands for the posted DDRM subscriber lines.

Line test functions are accessed through the LTP (Line Test Position) level of MAPCI, facilitate the basic measurements and monitoring capabilities necessary to maintain DDRM subscriber lines from the DMS. DDRM is triggered to perform these functions by suitable DMSX messages via PCM30 interface.

Related metallic test measurements are performed by the LTT and TMS cards configured in DDRM node instead of RMM (Remote Maintenance Module) of RLCM (Remote Line Concentrating Module). Those are driven by DDRM software. The main responsibility of this feature is to form an interface between the DMS and DDRM node (i.e. requesting test proper test commands supported by DDRM, and receiving the results and interpreting them on DMS).

Functional configuration view is given in the following figure.

Figure 1 Functional Configuration view of DDRM line testing



1.2.1 Supported DDRM Line Tests

DDRM line tests which are issued commands on LTP MAP level in DMS are applicable for only testable line card types. For other DDRM line card types, the command is prompted like that:

‘**Command is not valid on this type of DDRM line.**’

The test items supported by DDRM lines are listed in the following table.

Table 1 The line types and the supported DDRM test items by them

Test Item	DRBLCN	DRMLCN	DRBLCP	DRDLCP	DRMLCP
Line Manual Busy	+	+	+	+	+
Return to service	+	+	+	+	+
Forced Release & Manuel Busy	+	+	+	+	+
Digit Test from subscriber	+	+	+	+	+
Line Test (LNTST)				+	+
DC Voltage				+	+
AC foreign voltage				+	+
Loop resistance test				+	+
Continuity (Capacitance test)				+	+
LTA-Line Test Access	+	+	+	+	+
Tone sending to subscriber	+	+	+	+	+
Ring voltage application/test				+	+
Line return loss	+	+	+	+	+
Weighted circuit noise	+	+	+	+	+
RlsConn-Release connection	+	+	+	+	+
Onhook balance network test(BAL)	+	+	+	+	+
Onhook/Offhook balance network test(BALNET)	+	+	+	+	+
Talk Line Test Access	+	+	+	+	+
Monitor Line Test Access	+	+	+	+	+
Line Card Diagnostic					

Test Item	DRBLCN	DRMLCN	DRBLCP	DRDLCP	DRMLCP
Loop Detector Test				+	+
Metering pulse level / frequency					+
Automatic Line Test					
ALTBAL	+	+	+	+	+
ALTDIAG				+	+
ALTLIT				+	+

DRBLCN: Basic Line Card

DRMLCN: Basic Line card with metering

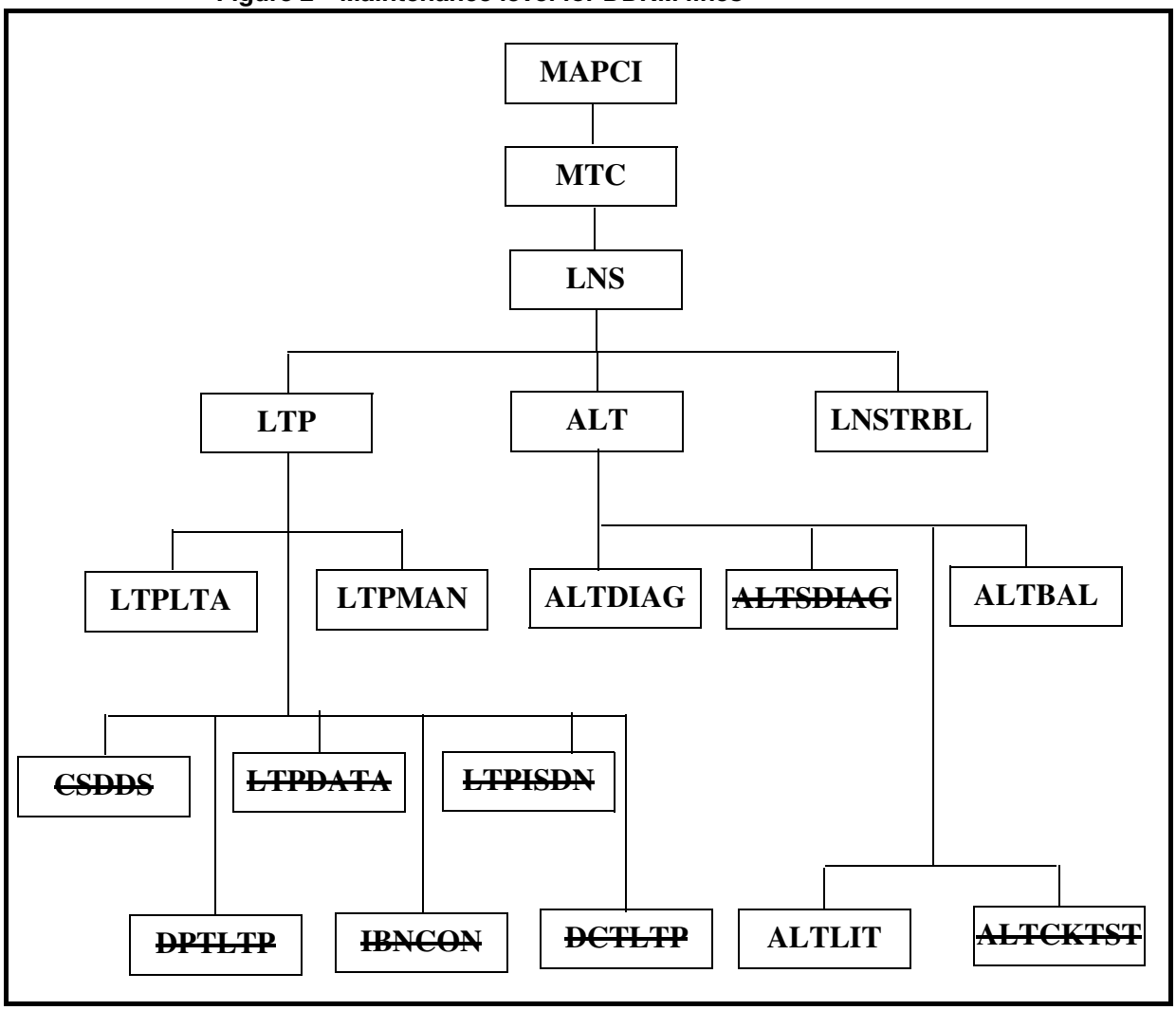
DRBLCP: Basic Line card with protection

DRDLCP: Basic Line card with test and over voltage

DRMLCP: Basic Line card with metering, test and over voltage

In DMS100-MMP product, the supported MAPCI;MTC;LNS levels are shown in the following figure. The levels and sublevels in strikethrough are not supported for DDRM subscriber lines.

Figure 2 Maintenance level for DDRM lines



The supported line tests for DDRM subscriber lines listed in Table 1, on page 2168 are located in MAPCI;MTC;LNS;LTP and MAPCI;MTC;LNS;ALT levels.

1.2.1.1 Line Test Position (LTP) Level

The following figure shows the supported LTP MAP level commands. Supported line tests listed in this figure are shown in **bold**.

Figure 3 Supported LTP level Commands (in bold)

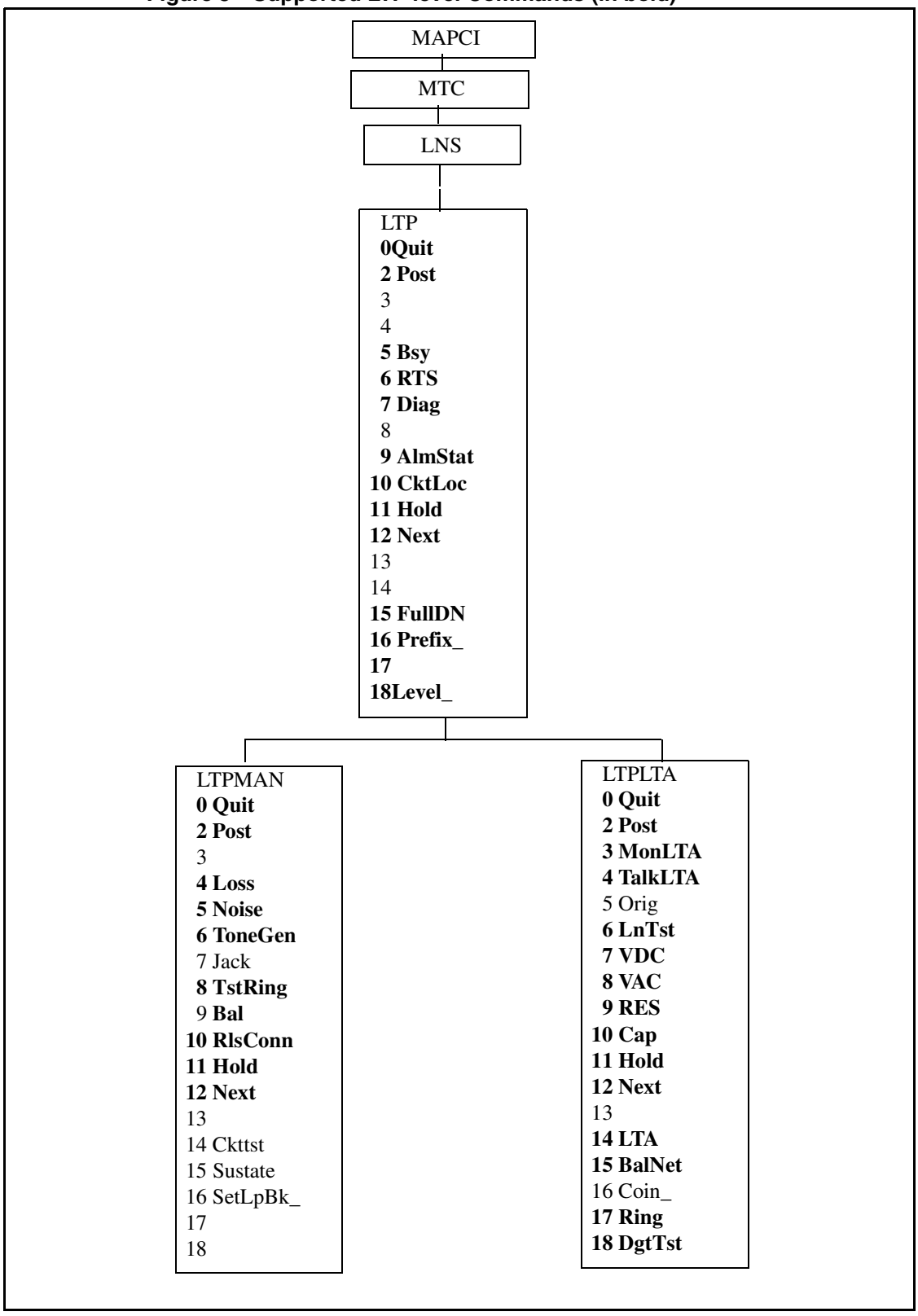


Table 2 A brief description of Supported LTP level commands for DDRM lines

Menu Item	Command	Function	Remarks
LTP 0	Quit	Return to the LNS level.	See Note 3 See Note 9
LTP 2	Post	Posts a line or set of lines to the LTP.	See Note 3 See Note 9
LTP 5	Bsy	Changes the state of the line in the control position, or optionally the complete set of posted lines, from IDL to MB.	See Note 1 See Note 9
LTP 6	RTS	The RTS command changes the state of the line in the control position, or optionally the complete set of posted lines, from MB to IDL.	See Note 1 See Note 9
LTP 7	Diag	Diagnose the posted line. The loop detector test checks the ability of a DDRM line circuit to recognize an off-hook condition on a loop-start line. Supervision circuity responses are checked by DMS-100 switch for the correct status changes. The metering test tests DDRM line cards for the presence and suitability of the signal provided by the metering tone card.	See Note 5 See Note 8
LTP 9	AlmStat	Query or set the lines (LNS) alarm thresholds.	See Note 3 See Note 9
LTP 10	CktLoc	Physical location of posted line card.	See Note 3 See Note 9
LTP 11	Hold	Moves the line in the control position to a spare hold position, and the next line from the posted set, if any, to the control position.	See Note2 See Note 3 See Note 9
LTP 12	Next	Moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the next line in the posted set. Replaces, saves or drops the replaced line.	See Note 2 See Note 3 See Note 9
LTP 15	FullDN	Display full national number.	See Note 3 See Note 9
LTP 16	Prefix_	Set/Clear DN Prefix.	See Note 3 See Note 9
LTP 18	Level_	Used to enter the various LTP levels.	See Note 3
Nonmenu Command	FRLS	This command is not visible at the LTP level. The FRLS command forcibly disconnects a line circuit from test equipment or any other circuit and changes its state to MB.	See Note 9

Menu Item	Command	Function	Remarks
LTPMAN 4	Loss	The LOSS command measures the insertion loss of a test tone sent from the subscriber end of a loop to the switch.	See Note 9
LTPMAN 5	Noise	The NOISE command measures the C-message weighted circuit noise on a subscriber loop.	See Note 9
LTPMAN 6	ToneGen	The TONEGEN command transmits a tone on a subscriber loop.	See Note 6
LTPMAN 8	TstRing	The TSTRING command tests the ringing relay in the line card for proper functioning.	See Note 8 See Note 9
LTPMAN 9	BAL	BAL command performs an on-hook balance network test on a subscriber loop. The command optionally updates the balance network value and loss pad value in the line circuit according to the test results.	See Note 9
LTPMAN 10	RlsConn	The RLSCONN command releases test equipment that is connected to line.	See Note 8 See Note 9
LTPLTA 3	MonLTA	The TALKLTA command connects a monitor circuit to a subscriber line.	See Note 9
LTPLTA 4	TalkLTA	The TALKLTA command connects a talk circuit to a subscriber line.	See Note 7
LTPLTA 6	LnTst	The LNTST command performs resistance, capacitance, and voltage tests on a line.	See Note 8 See Note 9
LTPLTA 7	VDC	The VDC command performs a dc voltage measurement on a subscriber loop.	See Note 8
LTPLTA 8	VAC	The VAC command performs an ac voltage measurement on a subscriber loop.	See Note 8
LTPLTA 9	Res	The RES command performs resistance measurements on a subscriber loop.	See Note 8
LTPLTA 10	Cap	The CAP command performs a capacitance measurement on a subscriber loop.	See Note 8
LTPLTA 14	LTA	Used with RLS parameter to release monitor connections to CPB lines.	See Note 8 See Note 9
LTPLTA 15	BALNET	The BALNET command performes a balance network test on a subscriber loop that is in either the onhook or ofhook mode.	See Note 9
LTPLTA 17	Ring	The RING command will send the appropriate signalling to the DDRM which will cause ringing to be sent to the subscriber.	See Note 5
LTPLTA 18	DgtTst	The DGTTST command tests the DIGITONE pad or dial on the subscriber station.	See Note 5 See Note 8

Menu Item	Command	Function	Remarks
Note 1: The BSY, RTS commands work as hidden commands from the subtending LTP levels, and operate the same as in the root LTP level. ***Note 2:*** The Hold and Next command on the subtending LTP levels operate the same as in the root LTP level. ***Note 3:*** The existing functionality remains for this command as respect of DDRM lines ***Note 4:*** Other LTP level menu commands aren't supported by DDRM lines. Other LTP nonmenu commands aren't supported by DDRM lines as well. ***Note 5:*** No optional parameter is supported for DDRM lines. ***Note 6:*** The metallic option for ToneGen is not supported for DDRM lines. ***Note 7:*** The battery option for TalkLTA is not supported for DDRM lines. ***Note 8:*** This command uses LTT/TMS test cards. ***Note 9:*** No parameter change has been done for this command.			

The diagnostic subtests for DDRM lines differs from the other POTS line types. The following subtests are supported by DDRM lines:

- loop detector test
- Metering test (only metering lines)

Other commands which are unsupported for posted DDRM lines are prompted on MAP like that:

'**Command is not valid on a DDRM line.**'

1.2.1.2 Automatic Line Testing (ALT) Level

The following figure shows the supported ALT MAP level commands. Supported line tests listed in this figure are shown in **bold**. Other sublevels apart from ALTLIT, ALTBAL and ALTDIAG are not supported for DDRM lines.

For ALT tests test results are categorized as follows for RLCM and LCM lines; PASS, FAIL, N/A and TOTAL, the sum of PASS + FAIL+ N/A . When a LIT test is run for a DDRM line, either PASS, FAIL or N/A is incremented. In case of a failure caused by incompatible line card types N/A is incremented, in all other failure scenarios FAIL is incremented.

Figure 4 Supported ALT level Commands (in bold)

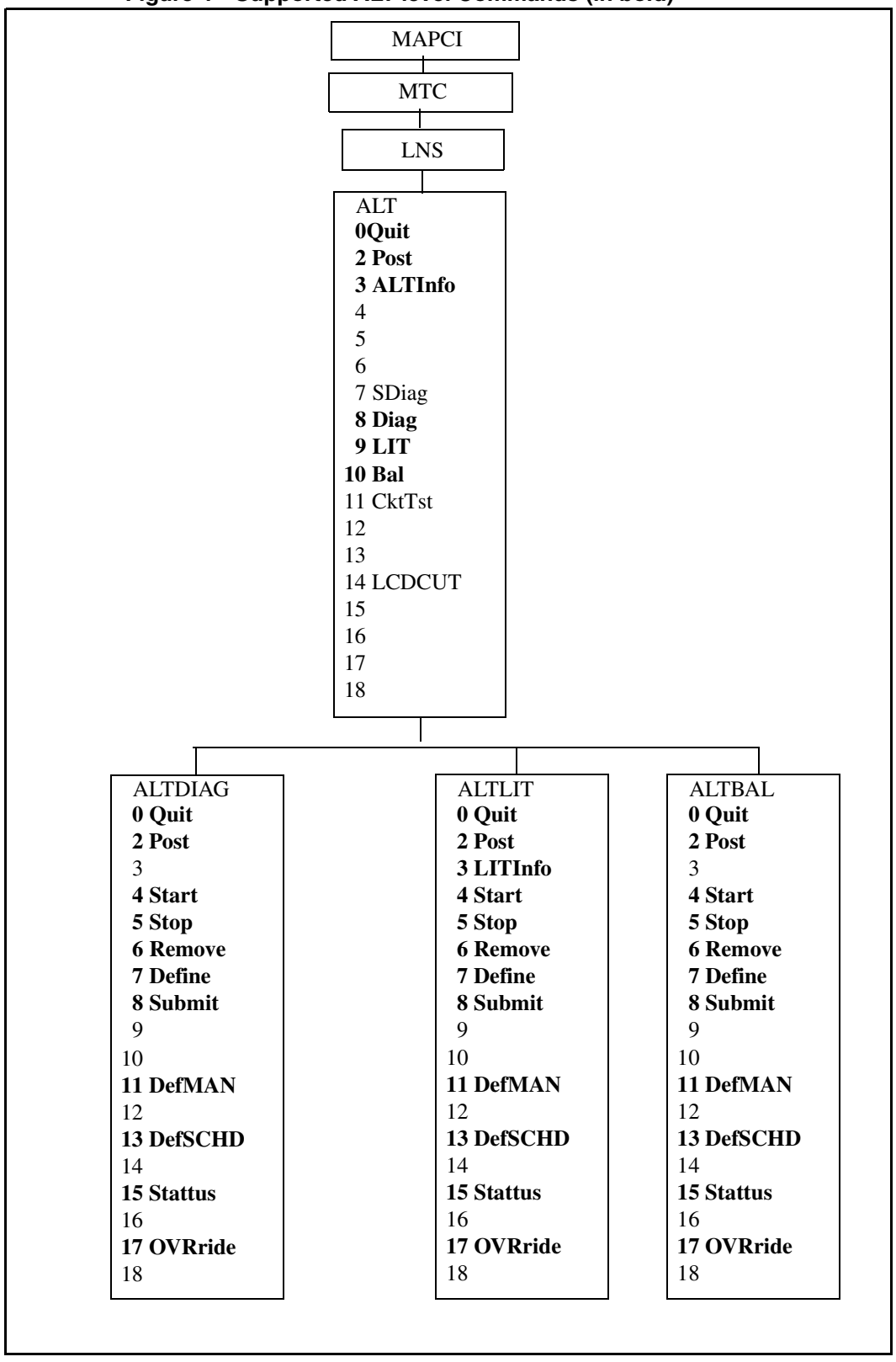


Table 3 A brief description of ALT level commands for DDRM lines

Menu Item	Command	Function	Remarks
ALT 0	Quit	The QUIT command causes the system to leave the current level and return to a higher level of the MAP.	See Note 1
ALT 2	Post	The POST command posts the scheduled ALT TESTID that is stored in memory (in Table ALTSCHED)	See Note 1
ALT 3	ALTInfo	The ALTINFO command checks test data stored in memory (Table ALTSCHED)	See Note 1
ALT 8	Diag	The DIAG command accesses the DIAG sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.	See Note 2
ALT 9	LIT	The LIT command accesses the LIT sublevel of ALT. If a TESTID is not entered as a parameter, a new TESTID must be defined with the DEFSCHD or DEFMAN command.	See Note 1
ALT 10	BAL	BAL command performs an on-hook balance network test on a subscriber loop. The command optionally updates the balance network value and loss pad value in the line circuit according to the test results.	See Note 1
ALTLIT 3	LITInfo	The LITINFO command displays the system default values for the LIT parameters.	See Note 1
ALTDIAG/ALTBAL/ALTLIT 4	Start	The START command sets the posted scheduled ALT test in a state such that it is ready to run at the next scheduled time.	See Note 1
ALTDIAG/ALTBAL/ALTLIT 5	Stop	The STOP command stops a test and changes the status of the TESTID.	See Note 1
ALTDIAG/ALTBAL/ALTLIT 6	Remove	The REMOVE command removes the data associated with the posted TESTID from memory (table ALTSCHED). If the TESTID is for a scheduled test, the system prompts for a YES or NO confirmation.	See Note 1
ALTDIAG/ALTBAL/ALTLIT 7	Define	The DEFINE command defines test data for the specified TESTID.	See Note 1
ALTDIAG/ALTBAL/ALTLIT 8	Submit	The SUBMIT command submits the defined test data for the posted TESTID into memory (table ALTSCHED).	See Note 1

Menu Item	Command	Function	Remarks
ALTDIAG/ALTBAL/ALTLIT 11	DefMAN	The DEFMAN command is used to assign a TESTID to the test that corresponds to the current ALT sublevel. For example, the DEFMAN command entered at the LIT level of MAP device number 7, will be assigned a TESTID of MANUAL07.	See Note 1
ALTDIAG/ALTBAL/ALTLIT 13	DefSCHD	The DEFSCHD command is used to assign a TESTID to the scheduled test that corresponds to the current ALT sublevel.	See Note 1
ALTDIAG/ALTBAL/ALTLIT 15	Stattus	The STATUS command checks the status of the posted TESTID.	See Note 1
ALTDIAG/ALTBAL/ALTLIT 17	OVRride	The OVRRIDE command overrides a scheduled test so that testing will not start until a specified day and time has passed.	See Note 1
Note 1: There is no change for this item. ***Note 2:*** DIAG test suits are changed for DDRM lines.			

1.2.2 Testing Procedures

DDRM line tests are categorized in 3 subset. Only Far-End Measurements require the involvement of the LTT and TMS cards. In other words measurements will be performed at DDRM. Other measurements are performed by DMS.

1.2.2.1 Near-End Measurements (LOSS, NOISE, TONEGEN)

These include the test commands which use the DMS-MTM testing facilities in LTPMAN sublevel. The result of the measurement resides till the craftperson releases the test.

Procedure for Near End Measurements

- Post DDRM line from the LTPMAN level.
- Perform the command. Observe the measurement on the MAP.
- Invoke RlsConn when complete to release test facilities.

1.2.2.2 Far-End Measurements (LNTST, VAC, VDC, RES, CAP, ALTLIT, TstRing)

Some tests require Metallic Test Access (MTA) provided by DDRM node. The LTP test commands are requested by LTP MAP level and DDRM performs them by using its LTT and TMS cards.

Procedure for Far End Measurements

- Post DDRM line from the LTPLTA level / for TstRing from LTPMAN level.
- Perform the command. Observe the measurements on the MAP.
- Invoke LTP RLS when complete to release test facilities (TstRing doesn't need manual release operation).

1.2.2.3 Line Monitoring (MonLTA, TalkLTA, Ring and DgtTst)

The LTPLTA commands MonLTA and TalkLTA establishes monitor and talk connections to DDRM subscriber lines in the MB and CPB state. If the line is in the MB state, a direct network connection between the headset and line is made. If the line is CPB, a connection between the line under test, the connected circuit, and the headset is set up through a 3-port conference circuit, and the line will enter the CPD state (DMS network connections to establish monitor/talk connections are used because of nonexistence of MONTALK card in DDRM).

The Ring command applies ringing current to a subscriber loop that has a monitor connection established. This enables the craftsperson at the switch monitoring a MB line to alert the subscriber or craftsperson in the field to go off-hook, allowing line quality to be monitored.

Procedure for DDRM line monitoring

1. Post DDRM line from LTPLTA level. If line is IDL, perform BSY command to place the line in the MB (Maintenance Busy) state.
2. Invoke MonLTA/TalkLTA command.
3. If line is CPB, connections through the 3-port circuit are made and line is monitored via the HSET. If line is MB, a network connection to the HSET is established, and the Ring command may now be entered to alert subscriber or craftsperson in the field.
4. To release connections, enter LTA RLS. The RTS command may be used for lines that are in the MB state.

   Note: DgtTst could not be invoked unless the talk connection is established. It may use DDRM testing facilities to detect digit tones.

New LTP level prompts are given in Table 4, on page 2178 for DDRM lines.

Table 4 New Prompts for LTP level Test Commands for DDRM lines

No	Prompt	Description	LTP level Test Commands
1	"Command is not valid on a DDRM line."	The test command is not supported for DDRM lines.	All apart from Table 2.

Table 4 New Prompts for LTP level Test Commands for DDRM lines

No	Prompt	Description	LTP level Test Commands
2	“Command is not valid on this type of DDRM line.”	When the command is performed for unsupported line card (The test command may be supported for line card types with metering or over voltage).	LCO, Diag, TstRing, RlsConn, LnTst, VDC, VAC, Res, Cap, LTA, DgtTst
3	“Line state INVALID, must be MB or CPB”	The line state should be MB or CPB when establishing monitor or talk connection.	MonLTA, TalkLTA
4	“Conference circuit not available”	The conference circuit could not be established for monitor or talk connection.	MonLTA, TalkLTA
5	“Test could not be executed because LTT and/or TMS is not in a proper state. “	LTT/TMS test cards are not available for testing.	LCO, Diag, , RlsConn, LnTst, VDC, VAC, Res, Cap, LTA, DgtTst

1.1 Hardware Requirements or Dependencies

1.1.1 DDRM Line Cards (DRBLCN, DRMLCN, DRBLCP, DRDLCP and DRMLCP)

DDRM line tests are performed on the DDRM specific line cards as shown in Figure 1.

1.1.2 DDRM Test Cards (LTT, TMS and UTR)

In order to perform line test commands for DDRM lines; LTT, TMS and UTR cards should be plugged in DDRM LC slots. VDC, VAC, RES, CAP, LNTST, TstRing, LIT and DgtTst require these cards.

1.1.3 HSET Circuit (NT5X30)

The HSET trunk referenced for DDRM line monitoring is provided by the standard 5X30 101 Communications Test Line Circuit Card. TalkLTA, Ring and DgtTst commands need HSET circuit.

1.1.4 TTT Circuit (NT2X96)

The TTT trunk referenced for DDRM lines is provided by the standard 2X96 Circuit Card. ToneGen, Loss and Noise commands need TTT circuit.

1.1.5 TTU Circuit (NT2X47)

The TTU trunk referenced for DDRM lines is provided by the standard 2X47 Circuit Card. Diag command needs TTU circuit.

1.2 Software Requirements or Dependencies

This feature depends on the following features:

- AT.00006664 DDRM Node Definition and Provisioning
- AT.00006661 DDRM Node Maintenance
- AT.00006662 DDRM Line Definition and Line Maintenance
- AT.00006663 DDRM Alarms and Audits
- AT.00006666 DDRM XPM Support and Monitoring

1.3 Limitations and restrictions

- LTP MAP level support of diagnostic tests is supported by this feature. The subtests are implemented by AT.00006662.
- The state should be set to MB or CPB before establishing monitor or talk connection.
- LCO command is not allowed to the DDRM lines. Because of the fact that DDRM hardware does not support this requirement.
- For DRDLCP and DRMLCP type of DDRM lines, when VAC/VDC/CAP/ RES test is applied with continuous parameter " **Continuous parameter is restricted for DDRM line.** " prompt is returned.
- Continuous parameter of diag test is not supported for DDRM lines.
- LTA command has three parameters. Namely IN, OUT, RLS. The expected behaviour in DMS is as follows; By LTA IN command mesaurements are done both on Line Card and on subscriber loop. By LTA OUT Line Card is isolated and mesaurements are done on subscriber loop. By LTA RLS the connections for tests are released. Due to the fact that DDRM is capable of performing tests only on subscriber loop, when LTA IN is performed " **LTA IN is not valid for DDRM lines, mesaurements can be done for LTA OUT only.** " prompt is returned.
- For LCM and RLCM lines 5 types of ALT subtests are available: ALTDIAG, ALTSDIAG, ALTBAL, ALTLIT, ALTCKTST. For DDRM lines ALTSDIAG is not supported because DDRM lines do not have two distinct DIAG sets. Other ALT subtests are available.
- When the LTT and/or TMS cards are not in a proper state for the tests which require the exsistence of LTT and TMS cards, " **Test could not be executed because LTT and/or TMS is not in a proper state.** " is returned.
- During the TSTRING test, ring will not be applied to the DDRM subscriber.

1.4 Interactions

1.4.1 AT.00006662 DDRM Lines Maintenance

The subtests of diagnostic are implemented by this feature.

1.4.2 AT.00006661 DDRM DDRM Node Maintenance

Existence of DDRM test cards in DDRM LC slots.

1.4.3 AT.00006663 DDRM Alarms and Audits

Existence of DDRM test cards in DDRM LC slots.

1.5 Applicable customer facing sections

Fault Management

- Logs _____
- Alarms _____

Configuration

- Data Schema _____
- User Interface __X__
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

1.6 Glossary

Term	Description
DMS	Digital Multiplex Switch
MMP	Multi Market Product
XPM	Extended Peripheral Module
CM	Central Module
RLCM	Remote Line Concentrating Module
RMM	Remote Maintenance Module
DDRM	DMS Dicle Remote Module
MTM	Maintenance Trunk Module
MAPCI	MAP Command Interpreter

Term	Description
LTP	Line Test Position
LTPLTA	LTP Line Test Access
LTPMAN	LTP Manual
LTT	Line and Trunk Test simulator
TMS	Test Measurement and Signaling

1.7 Recommended Reading/References

a. DMS_DDRM DDRM (DMS Dicle Remote Module) Spec Document
b. A00006638 DMS - DDRM HLD
c. A00006664 DDRM Node Definition and Provisioning
d. A00006661 DDRM Node Maintenance
e. A00006662 DDRM Lines Inventory
f. A00006663 DDRM Alarms and Audits
g. A00006665 DDRM ESA Support
h. A00006666 DDRM XPM Support and Monitoring
i. AR1625 GPP Line Maintenance Phase 2

Product = World Trade

A00006665 -- DDRM ESA Support

1: Applicable solution(s)

Int'l DMS

1.1 Description

DDRM (DMS Dicle Remote Module), is a rural area exchange developed for Turkey Market. Because of DDRM deployment on the field, it is requested to maintain and administer DDRM related operations over DMS switches. By this way the benefits of DDRM in Turkey market will be enhanced and the demands from the customer to reuse these switches as remote modules will be satisfied.

The Emergency Stand Alone feature (ESA) allows lines attached to the same remote peripheral (DDRM) to establish calls within the remote peripheral, when the remote peripheral is disconnected from its host peripheral (PLGC).

DDRM is not equipped with a special card supporting the ESA option. The ESA software runs on the DDRM main processor.

When operating in the ESA mode, DDRM offers limited services to subscribers. Only basic line-to-line calls (for both DP and DTMF lines) are supported. Subscriber features and AMA call recording are not supported in ESA. In normal operation of DDRM UTR on PLGC is used in order to receive tones. UTRD on DDRM is needed on DDRM in ESA mode in order to support tones so if UTRD is not datafilled in LCMINV table, ESA datafill will be prevented in LCMINV. If UTRD is not existing on the DDRM although it is datafilled, alarm will be raised by the ddrm alarms and audits component. If DDRM is in ESA mode, DDRM itself will take all the actions.

When connection of E1 links between DMS and DDRM is lost for any reason DDRM enters ESA-mode if ESA related datafill is appropriate on DMS. DDRM node continues intra-remote calls in ESA-mode based on the information received from DMS with static data download.The other facilities like inter-exchange calls, supplementary services, metering and billing are not supported in ESA mode. In the existing structure of DMS; " ESA module is defined, loaded and maintained from DMS. The loading and maintenance processes are not valid any more for DDRM node. For definition process only indication of ESA and UTRD configuration is set in the inventory table where DDRM node is defined. " A dedicated channel, channel 3 of primary link is used for ESA messaging between ESA processor and host XPM, PLGC. But because of the system restrictions on DDRM channel 3 is not used any more for ESA messaging. Instead DMS-X message channel, channel 1 is used.

1.1.1 Feature Synopsis

With A00006665 DDRM ESA Support activity, the following ESA functional components are covered:

- LCMINV table control component
- DDRM ESA Entry/Exit Component.
- DDRM ESA Static Data Component
- DDRM ESA Inservice Troubles Component

Basic Differences of DDRM ESA component from RLCM ESA component could be summarized as fallows:

1) DDRM doesn’t have ESA processor.

2) DDRM doesn't use channel 3 as messaging channel, instead it does use channel 1.

3) Unlike RLCM case, in DDRM case DMS doesn't download EXECS information since DDRM is supporting ESA on main processor.

4) DDRM doesn't need some tables, for ESA mode of operation, which are downloaded during static data download these are hunt group table, automatic line index table, prefix tables.

5)DDRM supplies tones by using UTRD in ESA mode, tones are supplied by tone & clock card in RLCM in ESA mode.

6) There is no need for XESAINV table in DDRM datafill on DMS since this table supports RLCM peripheral ESA processor related information.

7)For definition process only indication of ESA and UTRD configuration is set in the inventory table where DDRM node is defined.

8)UTR configuration - one LC slot on each shelf is generally used for UTR card and each shelf supports 152 subscribers. So 608 subscribers are supported for 4 shelf. It is not possible that one UTR card can serve all subscribers of a DDRM node during ESA mode. The subscribers which do not have UTR card on their shelves can not given their service facilities in ESA mode. But one UTR card is enough for line test facilites. In that case 632 subscribers aredefined for a DDRM node with 4 shelves.

1.1.2 ESA related configuration on DMS and LCMINV Table Control Changes

In the LCMINV table where DDRM node is defined there is a field which indicates ESA mode is supported or not. If the indication of ESA is Y then the related information for ESA is downloaded as static data from DMS to DDRM for basic intra-remote calls on DDRM. If the indication of ESA is N then ESA mode is not allowed on DDRM and the static data is not downloaded to DDRM. If ESA indication is changed from N to Y BSY/RTS of the RLCM is needed in order to download ESA data. XESAINV table is not needed for DDRM since it is used for ESA processor configuration in RLCM.

DMS will inform DDRM, if ESA equipment is available in the existing structure. if at least one UTRD and its datafil exists, DDRM will be ready to enter ESA mode after BSY/RTS operation. If ESA indication is N for DDRM this information is sent via a DMSX message in BSY/RTS time.

1.1.2.1 ESA related office parameters -

"LCM-ESA_ENTRY_BADCSIDE" and "RLCM_ESAENTRY_BADLINK" are used for DDRM ESA configuration. They are used to decide about ESA

entry, DDRM processor will wait for defined threshold times for BADCSIDE and BADLINK conditions specified by these two parameters.

RLCM_ESA_NOTIFY_TONE is an office paramater and controls whether the subscriber hears a distinctive dial-tone burst during ESA mode. When this parameter is set to Y then ESA specific tone is expected to be applied by DDRM. Its frequency will be a multiple of 450 Hz. ESA mode is expected to be in control on DDRM side if a UTRD related alarm is received from DDRM and ESA related datafill on DMS as in the expected way.

If the ESA related configuration and datafill is appropriate for ESA, ESA field in table LCMINV is set to Y, then static data for ESA mode is downloaded in BSY/RTS time. It is expected that DDRM should route the calls based on these information and based on line states which are previously downloaded. Office parameter "RLCM_ESASDUPD_HOUR" is used to set the start time to download ESA static data to all remotes on host site. For nightly audit to run RLCM_ESASDUPD_BOOL should be set to Y in table OFCENG and the ESA field in table LCMINV for the specific DDRM should be set to Y.

The downloaded static data over DMS-X signalling channel, channel 1 are; " DN for each defined subscribers of DDRM node " Translation tables " Tones - Dial tone, Ring Back tone, Congestion tone, Busy tone. Howler tone will be applied by DDRM itself. TNs are sent for each defined subscribers of DDRM node and sending of them are not based on ESA mode. They are sent as a step of line definition process.

1.1.3 ESA Entry

ESA mode is expected to be triggered automatically when the regular checks on communication links (monitoring the message channel to DMS, Monitoring E1 reception status etc) reveal a problem. In the existing structure of DMS there are two reasons to enter ESA mode; Badlink and Badcside. It should be noted that Badlink check is not specific for ESA. It is a generic control method to check E1 links (e.g E1 frame alignment) between host and remote. But Badcside is specific for ESA mode and a message is sent from remote site if the ESA mode indication is Y during DDRM definition on DMS. Badlink - The fault condition of unusable communication links triggers badlink. The communication links between remote node andDMSbecome unusable. The possible reasons for this fault condition are ; The links are severed between remote and the host The Peripheral side (P-side) message link (DS-1 card) of LTC is pulled out or DTC card on DDRM is pulled out.

The "RLCM_ESAENTRY_BADLINK" office parameter on remote site determines the desired delay timer between the failure of the C-side message link and the entry of ESA mode. The default value is 30 seconds and the value range is between 30 and 1000 second with 10 second intervals. If ESA-mode is entered because of Badlink problem then the existing behaviors of DMS for the state of remote nodes will be kept. Badcside this is for monitoring message

channel to DMS. Remote node checks to the host site periodically by means of looparound message in order to decide on ESA enterance. Upon receiving the host looparound message, the remote side knows that remote - CC communication is possible. When a failure is detected remote node waits for a delay before entering ESA-mode which is identified with an office parameter "LCM-ESA_ENTRY_BADCSIDE". Its default value is 15 minute and the range is between 1 minute and 60 minutes with 1 minute intervals.

1.1.4 ESA Exit

When the failure reasons which trigger ESA mode entry are recovered DMS requires exit from DDRM then DDRM node performs ESA exit operations. The active calls which are already set up in ESA mode are dropped after exiting ESA. This process is called as "cold exit". Warm exit is not supported by DDRM. There are two possible types to exit from ESA; System Exit and Manual Exit.

"RLCM_XPMESAEXIT" timeout value is used to decide System / Manual Exit procedures. Its default value is 0 and the value range is between 0 and 1000 with 10 second intervals.

System exit is an automatic exit from ESA-mode which is invoked by the host site without craftsperson interference. System exit is invoked if "RLCM_XPMESAEXIT" timeout value has a value except 0. DDRM will RTS automatically and return to normal mode of operation from from ESA mode and active calls which are established in ESA mode will be dropped.

Manual exit is a procedure which is initiated by the craftsperson. Manual exit is invoked if "RLCM_XPMESAEXIT" timeout value is 0(default value). Manual exit allows the craftsperson to view the number of calls on the remote site before RTSing the unit. This feature allows the craftsperson to delay the ESA exit if there are a large number of calls currently active. When E1 links are down DDRM state is seen as Cbsy until they are up again. If E1 link is started to be restored then the state of DDRM is returned to Sysb. If nothing is done by craftsperson, it will stay in SysB situation. But If BSY / RTS of DDRM is applied by the craftperson, DDRM will return to service.

After the ESA exit procedure, ESA processor on remote node sends operational measurements(OM), peg counts and the reason for ESA-mode entry back to DMS. These messages are "ESA Operational Measurements Reply to CC" and "ESA peg Counts Reply to CC". All of these information appears in PM171 log on DMS.

Table 6: The fields in PM171 log on DMS

FIELD	DESCRIPTION
ESA ENTER REASON	Enter Reason Description
VALUE	ESA Enter reason ID
ORIG_ATT_TOTAL ORIG_ATT	total origination attempts (Received Dial Tone)
ORIG_BLK (CHNL_BLK) (CHNL_BLK)	resources unavailable for origination Channel Blocked count in dialling state
ORIG_ABND	Dialling number or hung up before finishing diallig
DIAL_ERR	Error in DP or DT dialling
ORIG_SB (LINK_SB)	Originating facility goes system busy
XLA_ERR	Translation error of the dialling number
DIALLED_NUM_INV	The dialled number was not on the same RLCM or a timeout occured while dialling (took too long time to dial number
IA_TERM_ATT_TOTAL (TERM_ATT)	Termination attempt for intra-switched calls
IA_TERM_CUS (TERM_SUC)	termination successed for intra-switched (Number of calls asnwered)
IA_TERM_BLK (TERM_BLK)	intra-switched calls blocked due to lack of resources
IA_TERM_BSY	Intra-switched calls whose terminations were non-idle (busy,system busy, abondened etc)
IA_TERM_SB	Intra-switched calls whose terminations went system busy while processing the call (usually because of ring faults)
IA_TERM_NO_ANS	Intra-switched calls where there was no answer
RING_TMO	Ringing timeout

Table 6: The fields in PM171 log on DMS

FIELD	DESCRIPTION
COIN_FLT	Coin faults or failures
RING_BLK	Ring blocake in ringing state
TEST_REG	Test register failure in ringing state
CON_FAIL	Continuinty test fail while ringing
PRE_TRIP	Ringing fault message count in talking state
NO_IPC	No Inter peripheral Connection (IPC) buffer available
PREFIX USAGE	Usage counts for up to 16 entries in the POTS Prefix table. If no POTS prefix entry has been defined then this field is black

There is another statistics called as "DTSR statistics request". This is not specific for ESA mode. The number of calls that has over 3 seconds delay before given dial tone in each class is requested by DMS. The remote site sends "DTSR statistics Request Response" to DMS by means of a DMSX message.

1.1.5 DDRM ESA Static Data Download Subcomponent

DDRM ESA static data includes:

1. ESA tables
   - node table
   - terminal type table
   - digit collection table
   - multi-ring table
2. ESA translation tables

The ESA translation table download sequence is:

- translation data collection
- translation data download

ESA translation tables required by the DDRM are:

- Line terminal data table
- Extension header table

- Extension table
- Digit translation tables (EFG and ABCD tables)
- Tone table
- Office parameter table

DDRM ESA data downloading is triggered by:

- a successful DDRM RTS
- a DDRM ESA nightly audit

1.1.6 DDRM Node Maintenance Component

This component consists of fallowing subcomponents:

1. DDRM RTS sequence — This component invokes DDRM ESA Exit during DDRM RTS (both *manual* and *system*).
2. DDRM SYSRTS sequence —
   The LCM SYSRTS sequence is activated during the C-side host RTS. This invokes the LCM RTS sequence.
3. DDRM ESA Static Data request handling — This handles maintenance requests submitted for the DDRM ESA Static Data download.
4. DDRM Nightly Audit request handling —
   This supplies the interface between DDRM Nightly Audit and the existing LCM maintenance processes.

1.1.7 ESA Inservice Troubles

If the Static Data is not updated for the DDRM ESA or a problem occurs during Static Data download, the status of DDRM is changed to the appropriate ISTB.

LCM ISTB types do not now have a value which indicates Static Data problems. This is because LCM peripherals software do not contain Static Data tables. RLCM ESA is a separate node, and its ESA Static Data ISTB is only displayed in the ESA PM level.

The ISTB reasons will include:

- Static Data mismatch with CC
- Invalid ESA translation data

1.2 Hardware Requirements or Dependencies

UTRD which receives tones in ESA mode, is needed in order to enter ESA mode.

1.3 Software Requirements or Dependencies

For successful deployment of this activity following activities are required:

- A00006660 - DDRM Node Definition and Provisioning

  ESA is defined by node definition made in LCMINV table. CM checks ESA field information and UTRD datafill and existence.. When ESA field is changed nightly audit needs to be triggered which will download ESA data If necessary.

- A00006661 - DDRM Node Maintenance

  ESA data will be downloaded by by sucesfull RTS and by nightly audit. These are triggered by node maintenance..

- A00006663 - DDRM Alarms and Audits

  If UTRDis non-existent on DDRM major alarm will be raised. ESA enterence will be prevented by checking alarm status..

- A00006666 - DDRM XPM Support and Monitoring

  DDRM ESA related messages will pass through XPM.

Also:

- DDRM node, internal software

  CM part o f ESA needs proper reply messages from DDRM internal software in order to function. Also, call processing in ESA mode will be handled by DDRM ESA software.

1.4 Limitations and restrictions

DDRM ESA will not be triggered if UTRD is non-existent. Also UTRD datafill is needed in order to datafill ESA field in LCMINV table. Automatic line index, hunt group and prefix tables are not downloaded in static data since they are not needed.

1.5 Interactions

a. A00006660 DDRM NODE DEFINITION AND PROVISIONING
b. A00006666 DDRM XPM SUPPORT AND MONITORING
c. A00006661 DDRM NODE MAINTENANCE
d. A00006663 DDRM ALARMS and AUDITS

1.6 Applicable customer facing sections

Fault Management

Logs _____

Alarms _____

Configuration

- Data Schema _____
- User Interface _____
- Element Management _____
- Security _____
- Service Order _____
- Office Parameters _____

Accounting (includes AMA billing) _____

Performance (includes operational measurements) _____

1.7 Glossary

Term	Description
DDRM	DMS Dicle Remote Module
DRX-4	Dicle Rural Exchange-4
ESA	Emergency Stand Alone
LCM	Line Concentrating Module
RLCM	Remote Line Concentrating Module
UTRD	Universal Tone Receiver for DDRM

1.8 Recommended Reading/References

e. DMS_DDRM DDRM (DMS Dicle Remote Module) Spec Document
f. A00006638 DMS - DDRM HLD
g. A00006664 DDRM Node Definition and Provisioning
h. A00006661 DDRM Node Maintenance
i. A00006662 DDRM Lines Inventory
j. A00006663 DDRM Alarms and Audits
k. A00006665 DDRM ESA Support
l. A00006666 DDRM XPM Support and Monitoring

Product = World Trade

A00007289 -- RT Selector Enhancement for Metering

1: Applicable solution(s)

Int'l DMS

1.1 Purpose

The purpose of this feature is to optionally remove the incompatibility of metering behavior between DMS-100I and DMS-100 MMP systems, when RT selector is used in XXRTE routing tables.

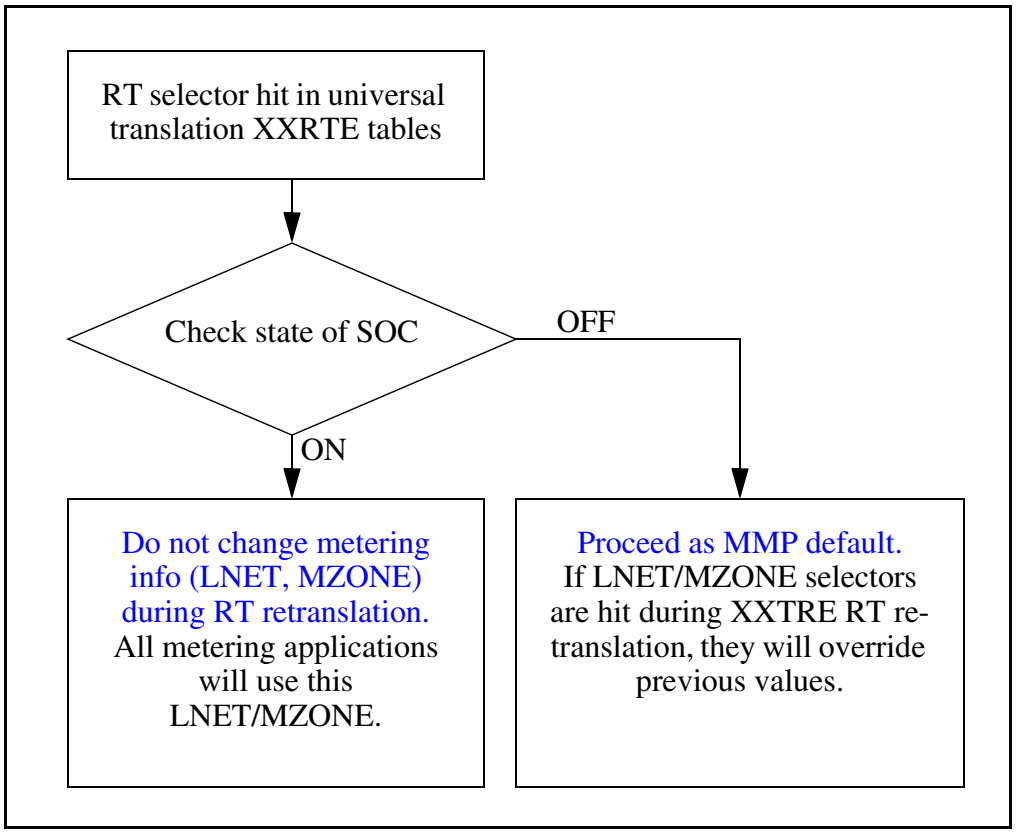
1.2 Introduction

The RT selector in XXRTE tables causes a re-translation to take place with new digits, which are supplied as parameters to the selector. During the translation of these new digits, it is likely that LNET/MZONE values different than those encountered before RT was hit will be encountered. Default MMP behavior is that the new LNET/MZONE will overwrite the previous ones, so that at the end of translation, the values that are last hit (i.e. the ones hit within retranslation) will be used for metering. On the other hand, DMS-100I product does not let re-translation overwrite LNET/MZONE, so at the end of the translation, the values which are hit before RT will be the ones which will be used for metering.

This activity implements a SOC optionality (METR0018). If the SOC state is ON and the translation is in XXRTE RT-based retranslation, DMS-100 MMP product will preserve LNET and MZONE during the retranslation, in the same way as DMS-100I.

1.2.1 Behavioral Diagram

Table 1 Feature flowchart



1.3 Hardware Requirements or Dependencies

This feature is meant to be used in DMS-100 MMP offices of Turk Telekom.

1.4 Software Requirements or Dependencies

This feature will work on DMS-100 MMP products, provided that the SOC is set to ON.
This feature may optionally be used in DMS-100 MMP markets that use metering.

1.5 Interactions

The effect of this feature is limited to metering behavior of RT selector in XXRTE routing tables. Other RT selectors (for example, RT selector in OFRT table), or other selectors which cause re-translation (like GRX and IBNRT) are not effected.

Only the metering behavior of XXRTE RT selector is affected.

Metering is affected such that RT re-translation of XXRTE tables do not override LNET/MZONE.

Any application that uses/reads LNET/MZONE after/during translations will be indirectly effected (if translations use XXTRE-RT, and the SOC state is ON).

There are no changes in TRAVER behavior.

1.6 Applicable customer facing sections

Table 2 Customer facing sections

Fault Management	**N/A**
Logs	N/A
Alarms	N/A
Configuration	
Data Schema (SOC)	X

1.7 Glossary

Term	**Description**
XXRTE	The routing tables of Universal Translation, i.e PXRTE, FARTE, etc.
DMS-100I	The DMS-100 International product.
DMS-100 MMP	The DMS-100 Multi-Market product, the product in which this feature will be in use.
LNET	Logical Network - A parameter used in metering.
MZONE	Metering Zone (or Destination Zone) - A parameter used in metering.

2: Configuration for A00007289

2.1 SOC

This feature is activated and deactivated by the SOC option METR0018. The details of the SOC are listed below.

Table 1 SOC

SOC option name:	METR0018
SOC option title:	Retrans Selector
SOC option control type:	State

Table 1 SOC

New SOC option?	Yes
SOC option order code	METR0018
Option defined in DRU:	WT
Affected products:	MMP / GMP

Product = World Trade

A00008429--Ringback When Free (RBWF) Enhancements

Functional Description

1: Applicable Solution(s)

Int'l DMS

1.1 Description

1.1.1 Introduction

Throughout this document,

- RBWF is used as a general term for RAG flavors which are Nodal RAG and BTUP Call Back When Free (CBWF) for this activity.
- The subscriber that invokes the RBWF service is known as the RAGOR. The subscriber that was busy when a call was made to it, resulting in the RBWF service being invoked against it, is known as the RAGEE.

This activity enhances the Nodal RAG (Ring Again) and BTUP Call Back When Free (CBWF) flavours of existing RAG Service (based on two new SOCs introduced by this activity).

This activity is implemented in ISN09 release and any functionality introduced by this activity is only available in INTL TDM loads.

In the "Background Information" section existing RAG functionality is summarized, and in the "Functional Overview" section RBWF enhancements introduced by this activity are explained.

1.1.2 Background Information

The RAG feature allows a RAGOR to set a Ring Again request against a RAGEE, if the RAGEE is busy, and be recalled when the RAGEE becomes

idle. Once the RAGEE becomes free then the RAGOR is automatically rung back. Once the RAGOR picks up the ringing call then the RAGEE is rung and the call continues as a normal call.

The activation and deactivation of RAG feature is as follows:

1. The RAGOR encounters a busy signal. The RAGOR activates the RAG feature (either by single digit activation mechanism, or by dialling RAG feature code after FLASH). The RAGOR goes on-hook.
2. When the RAGEE becomes idle, the RAGOR receives a special ring back tone.
3. The RAGOR goes off-hook. The switch places the call, and the call continues as a normal call. The system deactivates the RAG feature.

Interrogation functionality of RAG service does not exist before this activity.

After a specified amount of time, RAG automatically reactivates if the RAGOR does not answer the ring back. To cancel a RAG request, the RAGOR can go off-hook and dial the RAG feature code.

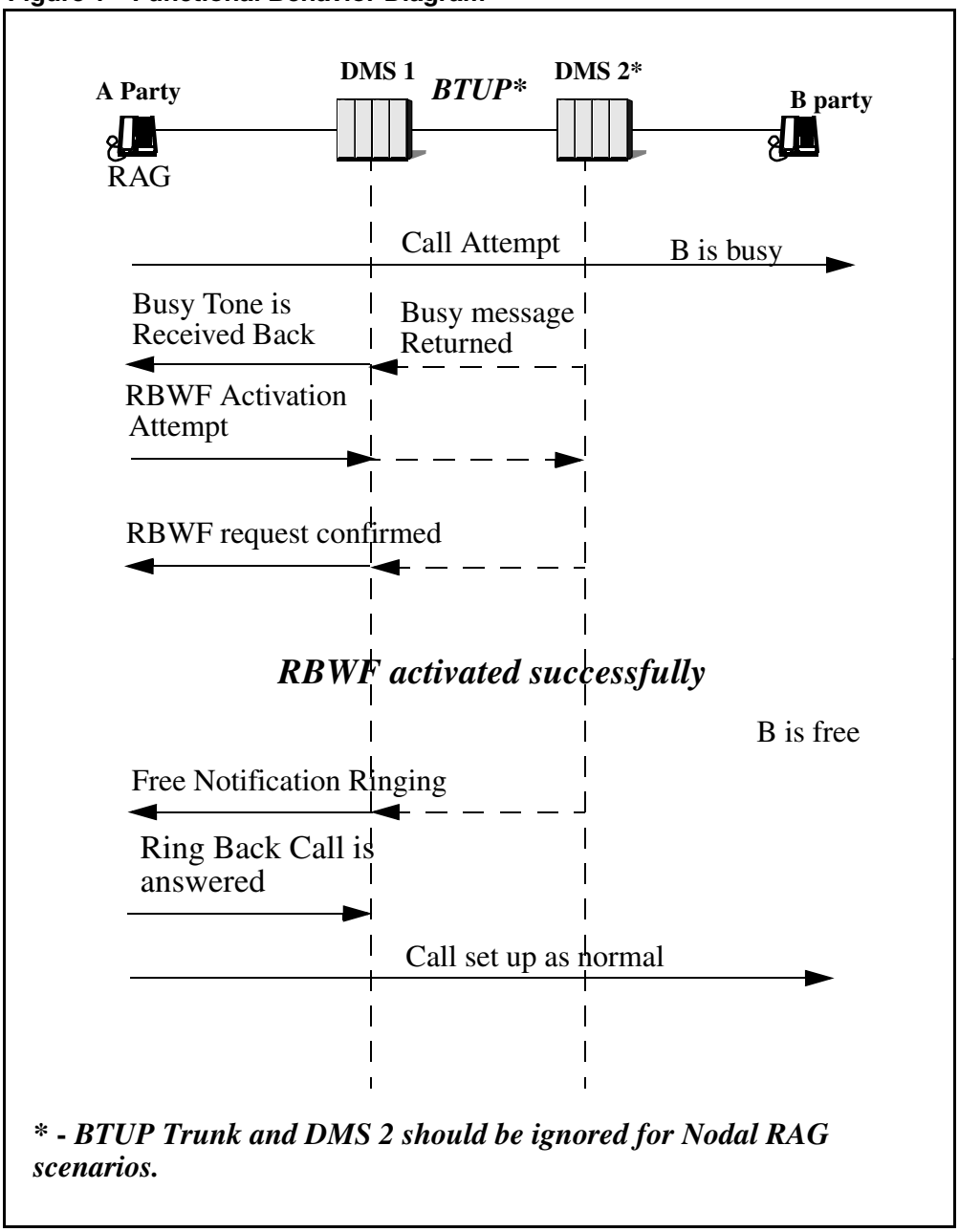
Ring Again Cancellation Timer deactivates the RAG requests when the busy party remains off-hook for a specified amount of time.This timer is datafilled in table CUSTSTN, with RAGCANTO field of RAGTIM option for nodal RAG (0, 2 TO 30 mins), and in table CUSTNTWK, with ORIGDUR (5 TO 180 mins) and TERMDUR (5 TO 185 mins) fields of NTWRAG option for BTUP CBWF.

Only one RBWF request can be active for RAGOR. If RAGOR attempts to activate a new RBWF request, when there already exists an active RBWF request, new RBWF request overwrites the existing one.

For Nodal RAG, RBWF activation is not allowed for inter-group calls, if INTRAGRP=N.

Following figure shows the activation and call setup sequence for RBWF services.

Figure 1 Functional Behavior Diagram



Please refer to related NTPs and the references given at the end of the document, for further information on existing Nodal RAG and BTUP CBWF functionality.

1.1.3 Functional Overview

This feature provides the following functionalities/enhancements to RBWF Services:

- Number of RBWF requests that can be activated by a RAGOR is increased from 1 to N, which is datafillable up to 6.
- Cancellation command results in cancellation of all active RBWF requests cancelled.
- Interrogation functionality is newly introduced by his activity, and interrogation results in announcement of all active RBWF requests of the RAGOR.
- Individual datafillable dialling sequences for RBWF deactivation, and interrogation are provided.
- Billing for nodal RBWF calls is supported.
- Nodal RBWF functionality is improved so that RBWF can work between different customer groups, regardless of the INTRAGRP flag.
- Range of existing Ring Again Cancellation Timer for Nodal RBWF calls is extended from 30 to 185 mins. This timer allows the end user to set a limitation how long each nodal ring again request can remain active at the switch. This limit is set on a customer group basis (RAGCANTO field of RAGTIM tuple in table CUSTSTN). Please note that this timer is individually started for each RBWF request, and expiry of this timer for a RBWF request causes deactivation of that request only.

RBWF enhancements implemented by this activity are controlled with two new SOC options, so that existing functionality is not affected when these SOCs are IDLE. Two new SOC options introduced by this activity are SVBI Multiple RBWF and SVBI RBWF Enh. Please refer to Section “Providing Optionality for RBWF Enhancements”.

Please note that multiple RBWF functionality is designed considering that only Nodal RAG and BTUP CBWF flavours of RBWF are used in the switch. It is strongly recommended that SVBI0037 SVBI Multiple RBWF SOC should not be turned ON in the switches where other flavours of RBWF (i.e. DPNSS, TCAP CBWF, CCBS etc) are being used. Turning this SOC ON might cause unexpected behavior if RBWF flavours other than nodal RAG and BTUP CBWF are being used.

In addition, some new options in tables ISERVOPT and AMAOPTS are introduced in order to control the functionality. All of these options are discussed in next sections.

Please note that this activity does not change the call topology and BTUP signalling of existing RBWF services.

1.1.3.1 Providing Optionality for RBWF Enhancements

Main functionalities of this activity are controlled by two new SOC options, SVBI Multiple RBWF and SVBI RBWF Enh. Both of these SOCs are state SOCs, which can be either in SOC_ON or SOC_IDLE state.

SVBI Multiple RBWF SOC controls the following:

- Allowing N RBWF request to be activated by the RAGOR.
- Rejecting N+1th request.

Table 1 SVBI0037 Multiple RBWF SOC

SOC Group	SVBI
SOC Option Name	SVBI0037
SOC Option Title	Multiple RBWF
SOC Option Control Type	State
New SOC Option?	Yes
Option defined in DRU	WT22
Affected Products	DMS100 - MMP

If SVBI0037 Multiple RBWF SOC is turned OFF when RAGOR has more than one active RBWF requests, these requests are completed normally after SOC is turned OFF. If RAGOR attempts to activate a new request after SVBI0037 SOC is turned OFF, new RBWF request overwrites the first RBWF request activated before.

SVBI RBWF Enh SOC controls the following:

- Allowing nodal RBWF between different customer groups via ignoring INTRAGRP flag.
- Billing of nodal RBWF usage.
- Deactivation and interrogation functionalities with new dialling sequences.

  Note: If only SVBI RBWF Enh SOC is ON, then there should be at most one RBWF request to announce or cancel - however if there are more than one (because the SVBI Multiple RBWF SOC was on when they were activated) then all requests are announced / cancelled.

Table 2 SVBI0036 RBWF Enh SOC

SOC Group	SVBI
SOC Option Name	SVBI0036
SOC Option Title	RBWF Enh
SOC Option Control Type	State

Table 2 SVBI0036 RBWF Enh SOC

New SOC Option?	Yes
Option defined in DRU	WT22
Affected Products	DMS100 - MMP

Please note that datafilling of any option, which is introduced by this activity, is allowed even if these SOCs are IDLE. But new functionalities are only available when related SOC(s) is ON.

1.1.3.2 RBWF Activation, Interrogation and Cancellation Through Translation Tables

In the existing implementation, if single digit activation mechanism is not used, RBWF services are activated and deactivated via using the same dialling sequence (ex. *37#), datafilled in translation tables.

Figure 2 Existing Datafill for RAG act and deact access codes

```
TABLE IBNXLA
KEY                        RESULT
-----------------------------------------
FTRSTAR  37       FEAT N N RAG
```

This activity provides different dialling sequences for RBWF activation and deactivation, and also introduces RBWF Interrogation functionality in INTL TDM product. In order to provide this, two new IBN_LOG_FEATURES “RAGD” and “RAGINT” are introduced to be used in table IBNXLA.

Access codes for RBWF act, deact and interrogation are datafillable in table IBNXLA, and following figure shows a datafill example for using *37# for activation, #37# for deactivation and *#37# for interrogation of RBWF.

Figure 3 New datafills for RBWF act, deact and interrogation access codes

```
TABLE IBNXLA
KEY                        RESULT
-----------------------------------------
FTRSTAR  37       FEAT N N RAG
FTROCT   37       FEAT N N RAGD
FTRSTAR  C37      FEAT N N RAGINT
```

RAGINT and RAGD are datafillable in table IBNXLA, even if RBWF Enh SOC is IDLE. But please note that, NACK tone is given if subscriber attempts to use deact/interrogation with these dialling sequences, when RBWF Enh SOC is IDLE.

Behavior of the RBWF service during RBWF act, deact and interrogation are explained in the following flowcharts:

Figure 4 Flow Chart for RBWF Activation

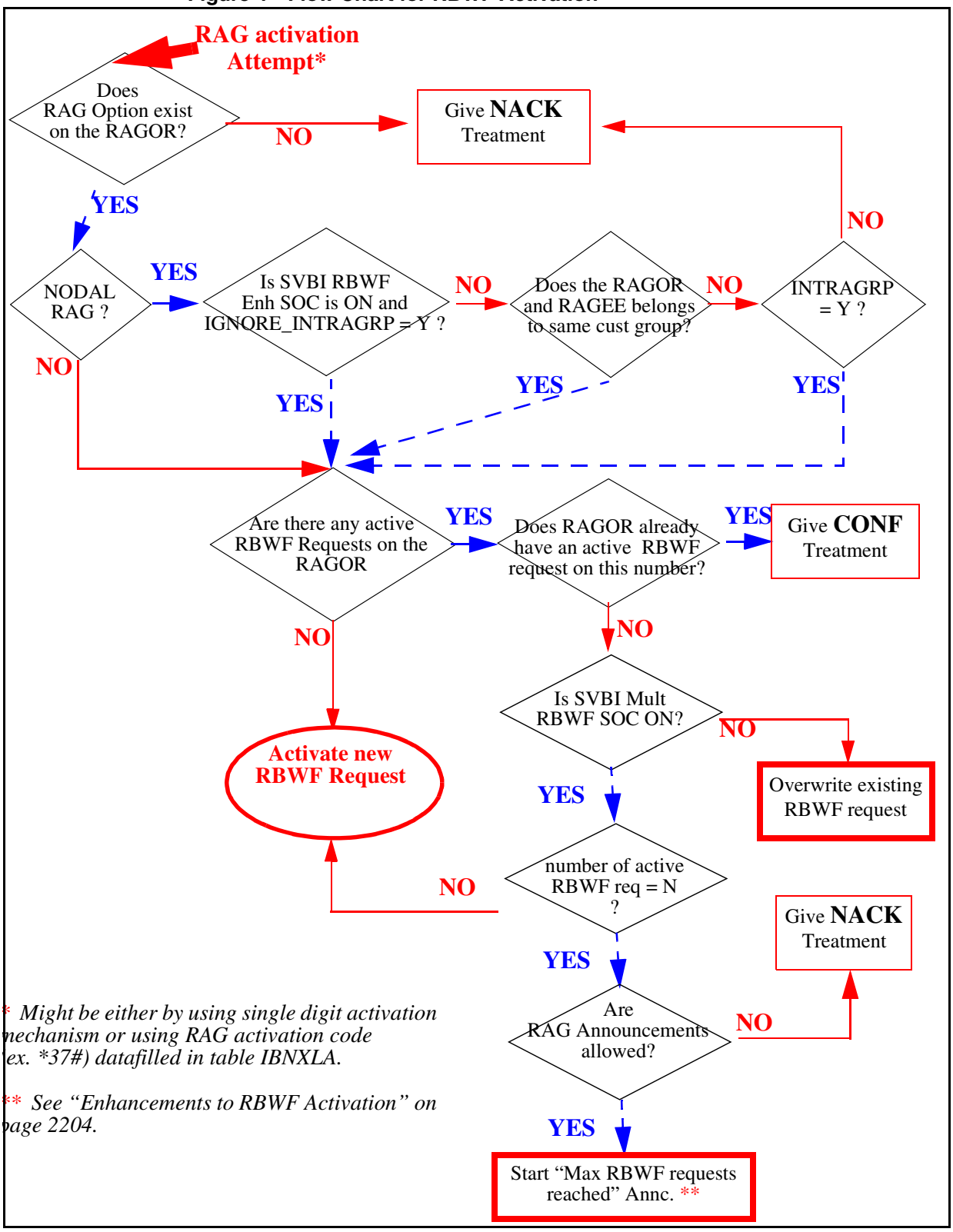


Figure 5 Flow Chart for RBWF Deactivation

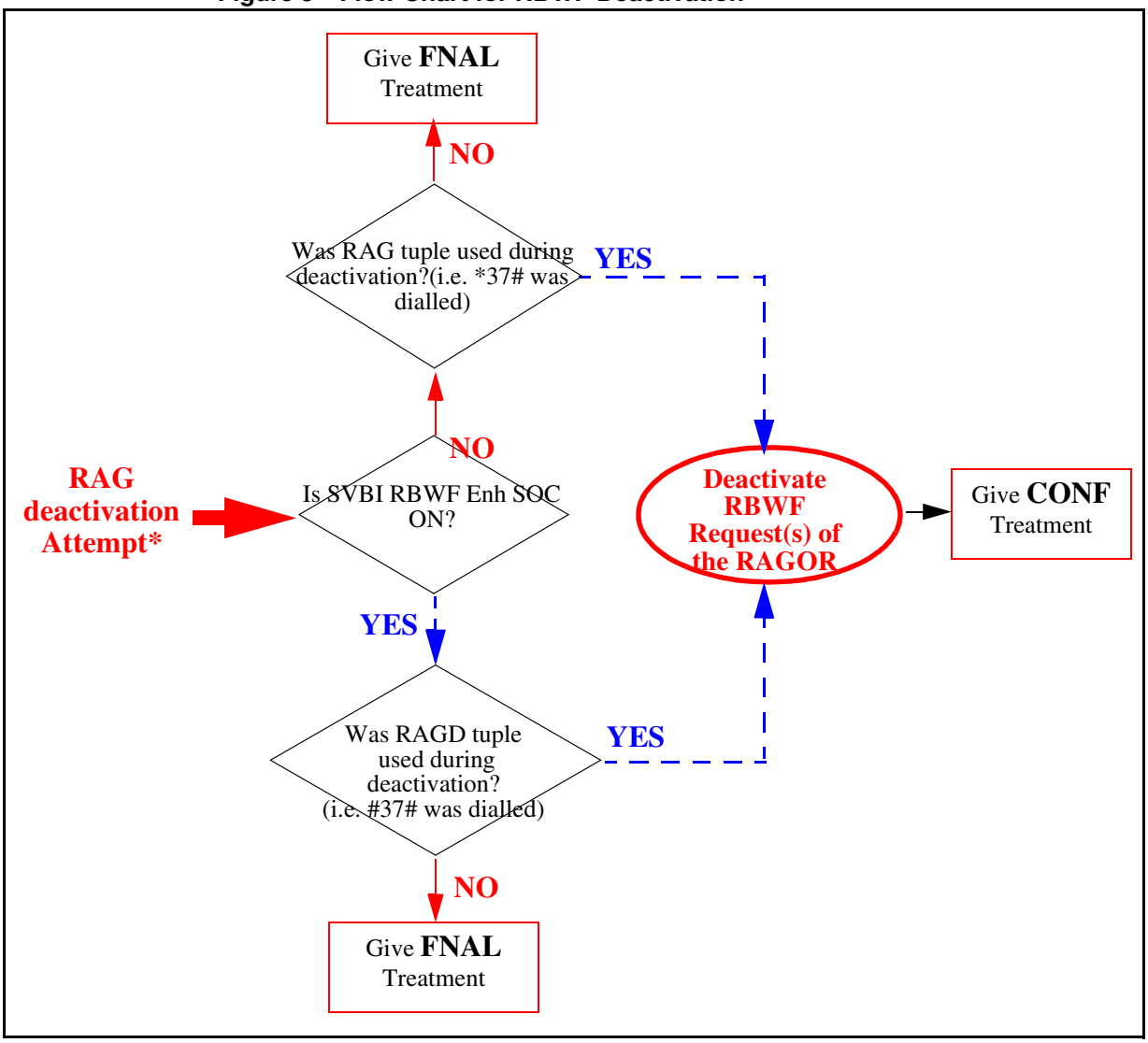
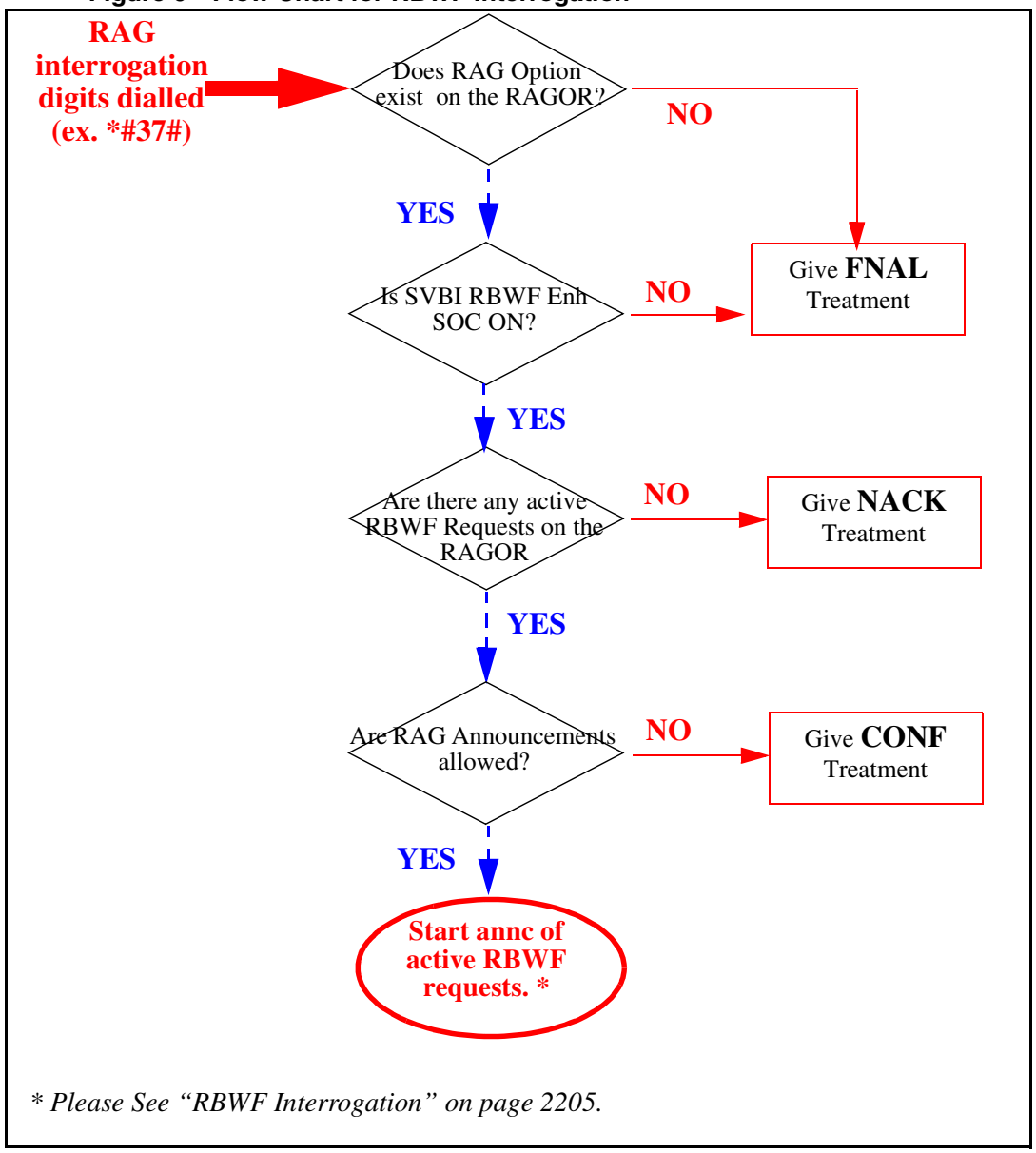


Figure 6 Flow Chart for RBWF Interrogation



** Please See "RBWF Interrogation" on page 2205.*

1.1.3.3 RBWF Activation and Cancellation on EBS Lines

In the existing implementation, RAG key on EBS sets is used for both activation and cancellation. If it is hit any time when there is an active RBWF request, RBWF cancellation is performed. Hitting RAG key when there are no RBWF requests is considered as RBWF activation.

This behavior is changed by this activity, since hitting RAG key for activating a new RBWF request (when there already exists one), should be taken as RAG activation, not cancellation.

If SVBI0037 Multiple RBWF SOC is ON,

- **hitting RAG key when RAGOR is not involved in a call (ON-HOOK), is considered as RAG cancellation attempt.**
- **hitting RAG key, when a busy destination is encountered, is considered RAG activation attempt.**

Please note that existing behavior is not changed if SVBI0037 Multiple RBWF SOC is IDLE.

1.1.3.4 Enhancements to RBWF Activation

In current implementation of RBWF, any RAGOR can have only one active RBWF request at a time. By this activity, a RAGOR can have N active RBWF requests, where N is datafillable in table ISERVOPT. If SVBI Multiple RBWF SOC is IDLE, RAGOR can have only one active RBWF request as it is now.

1.1.3.4.1 New Service Option for Multiple RBWF Requests

A new option RBWFENH is defined in table ISERVOPT. This option has two subfields: MAX_RBWF_REQ and IGNORE_INTRAGRP.
MAX_RBWF_REQ determines the maximum number of RBWF requests that can be activated by a RAGOR simultaneously. It takes values between 1 and 6. Its default value is 5, if not datafilled.

Please note that if SVBI Multiple RBWF SOC is IDLE, only one RBWF request is allowed as it is now, even if MAX_RBWF_REQ is different than one. If user attempts to datafill MAX_RBWF_REQ with a value greater than 1 when SVBI Multiple RBWF SOC is IDLE, a warning msg is displayed, however datafill is allowed.

Figure 7 Datafill Sample for MAX_RBWF_REQ in table ISERVOPT

```
TABLE: ISERVOPT

 RBWFENH             RBWFENH 5 Y
```

1.1.3.4.2 Increasing Number of RBWF Requests up to N

In the existing implementation, only one active RBWF request is allowed for a RAGOR.By this activity number of RBWF requests allowed for a RAGOR is increased up to N.

- *Ragging on the same number twice:*

In the existing implementation of NODAL RAG, if RAGOR attempts to rag on the same number again, just CONF tone is given without resetting the existing RBWF request (i.e. timers are not reset). This behavior is not modified by this activity. If current RAGEE number is one of the active RBWF requests of the RAGOR, just CONF tone is given.

In the existing implementation of BTUP CBWF, active RBWF request is cancelled when user attempts to activate a new one, even if incoming request is for the same number. This behavior is changed by this activity, as to be consistent with NODAL RAG implementation.

- *Ragging on a new number:*

In the existing implementation, if any other number is requested, active RBWF request is cancelled and new request is accepted.

By this activity, if SVBI Multiple RBWF SOC is ON, active RBWF requests are not cancelled, instead a new RBWF request is activated. If max number of RBWF requests were already reached, new request is rejected with an announcement.

1.1.3.4.3 Rejection of N+1th RBWF request

If max number of RBWF requests allowed are reached, new RBWF request of the RAGOR should be rejected if SVBI Multiple RBWF SOC is ON. If RAG announcements are allowed (datafilled in ANNC_CONF field of RAG tuple in ISERVOPT), new request is rejected with an announcement, otherwise NACK tone is given. Following is a rejection announce sample:

Figure 8 RBWF Request Rejection Announcement sample

```
"The maximum number of ringback requests are registered
against your line.No further ringback requests can be
accepted at the moment"
```

1.1.3.5 Enhancements to RBWF Deactivation

When the RAGOR attempts to cancel his/her RAG requests, via dialling the cancellation digits, all of the active RAG requests of this RAGOR are cancelled.

1.1.3.6 RBWF Interrogation

Interrogation functionality of RBWF is being introduced by this activity. If all criteria in the interrogation flowchart are met (i.e. SVBI Mult RBWF SOC is ON, RAG Annc allowed, etc), successful interrogation results in announcement of all active RBWF Requests. Provided announcement is like the following:

Figure 9 Interrogation Announcement sample for an agent having 3 active RBWF requests

```
"Telephone Number 01483 8207308 is waiting for ringback.
 Telephone Number 436 7854 is waiting for ringback.
 Telephone Number 436 7945 is waiting for ringback."
```

1.1.3.7 RBWF Announcements

RBWF announcements are custom announcements that consist of a number of simple phrases, in English, datafilled in table ANNPHLST (See Appendix for sample announcement datafill). Each simple phrase has a corresponding recording on the EDRAM card.

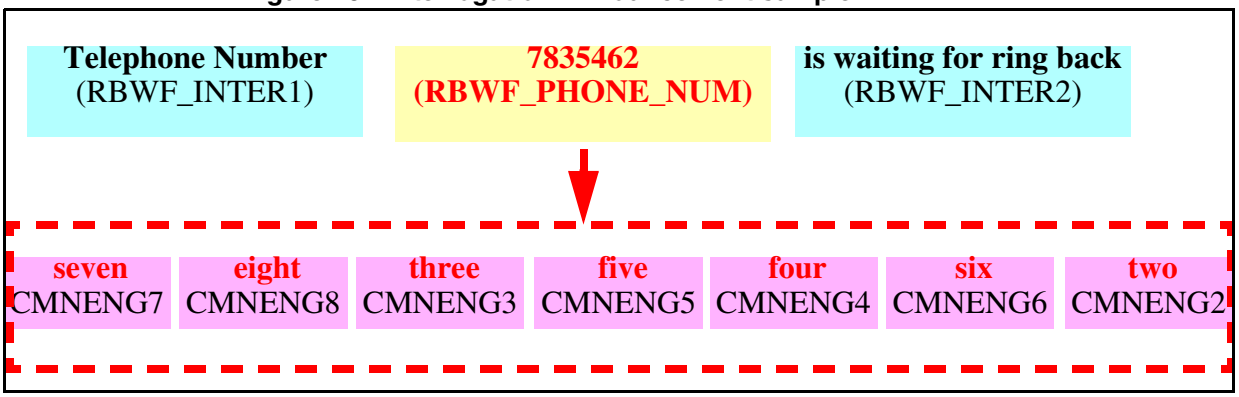
- *RBWF Interrogation Announcement*

RBWF interrogation announcement is provided as a result of successful RBWF interrogation, and includes the RAGEE telephone numbers which were activated by the RAGOR requesting the interrogation.

There are two simple phrases introduced for RBWF interrogation announcement, which are RBWF_INTER1 and RBWF_INTER2. RBWF_PHONE_NUM is a compound phrase, which corresponds to the RAGEE number. RBWF_PHONE_NUM does not have a constant recording on EDRAM, and its components (i.e. combination of simple phrases) are determined at run time according to the digits of the RAGEE number.

Tuple datafilled in ANNPHLST is repeated for “number of existing RBWF requests of RAGOR” times. Please note that announcement given strictly depends on datafill sequence.

Figure 10 Interrogation Announcement sample

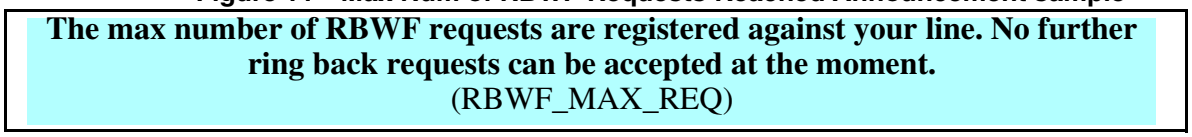


- *Max Num of RBWF Requests Reached Announcement*

This announcement is given when RAGOR attempts to initiate a new RBWF request, and RAGOR already has N active requests (N - Max Num of RBWF allowed).

There are one simple phrase introduced for RBWF request rejection announcement, which is RBWF_MAX_REQ.

Figure 11 Max Num of RBWF Requests Reached Announcement sample



Following is the list of phrases which are introduced by this activity.

Table 3 List of English Phrases introduced

Phrase Name	Recording
RBWF_INTER1	Telephone Number
RBWF_INTER2	is waiting for ring back
RBWF_PHONE_NUM	Compound Phrase - RBWF request number
RBWF_MAX_REQ	The max number of RBWF requests are registered against your line. No further ring back requests can be accepted at the moment.

For the announcement of telephone number, existing basic English phrases for digits 0 to 9 should also be recorded properly, which are the phrases CMNENG0 to CMNENG9.

Table 4 List of English Digits Phrases CMNENG0 to CMNENG9

Phrase Name	Recording
CMNENG0	Zero
CMNENG1	One
CMNENG2	Two
CMNENG3	Three
CMNENG4	Four
CMNENG5	Five
CMNENG6	Six
CMNENG7	Seven
CMNENG8	Eight
CMNENG9	Nine

Please see Appendix for sample datafill of RBWF Announcements.

1.1.3.8 Billing of Nodal RBWF Calls

Billing of BTUP CBWF calls was already implemented by an activity “AJ4955- BTUP CBWF Billing”. Billing of BTUP CBWF calls are controlled by BTUP_CBWF_BILL option in table AMAOPTS. If it is ON, service

feature ID field of AMA record is marked with value “029”. Please note that 029 is a reserved value for RAG feature.

Billing of nodal RBWF calls are implemented by this activity in the same manner, via marking the Service Feature ID field with value 029. This functionality is controlled with SVBI RBWF Enh SOC and a new option, “NODAL_RAG_BILL” in table AMAOPTS.

Both SVBI RBWF Enh SOC and NODAL_RAG_BILL option must be ON in order to enable billing of Nodal RBWF calls.

Figure 12 Sample Datafill For NODAL_RAG_BILL option in Table AMAOPTS

```
TABLE AMAOPTS
OPTION                SCHEDULE
-----------------------------
NODAL_RAG_BILL        ON
```

Usage of Nodal RAG is reported in AMA record in the following scenarios:

1. RAGOR ignores ring back call
2. RAGOR answers ring back call and disconnects immediately before or after the RAGEE is rung.
3. Ringing is applied to the RAGEE and RAGEE does not answer.
4. A complete call setup occurs between RAGOR and the RAGEE, and call is disconnected by either party after the conversation ends.

Please note that for cases 2 to 4 service feature ID field of AMA record is marked with value “029”, if all criteria are met for generating AMA record (i.e. datafills, translations, SOC options for billing etc). But For case 1, AMA record is generated at any condition, independent of billing datafills.

Figure 13 AMA Record Sample for an Answered RBWF call

HEX ID:	AA	
STRUCTURE CODE:	40510C	
CALL CODE:	006C	STATION PAID [1]
SENSOR TYPE:	036C	DMS 100F
SENSOR ID:	0754019C	(FROM OFFICE PARM)[2]
REC OFFICE TYPE:	036C	DMS 100F
REC OFFICE ID:	0754019C	
DATE:	80204C	DECEMBER 03, 2004
TIMING IND:		
TIMING GUARD FLAG	0	UNUSED
SHORT CLD PARTY OFF-HOOK IND 0		SHORT CLD PARTY OFF-HOOK
LONG DUR/SERV PTY CAPABILITY IND 0		UNUSED
UNUSED	0	
UNUSED	0C	
STUDY IND:		
STUDY TYPE A	0	UNUSED
STUDY TYPE B	0	UNUSED
STUDY TYPE C	0	UNUSED
TEST CALL IND	0	UNUSED
UNUSED	0	
ORIG/TERM NANP NUM IND	0	UNUSED
OPERATOR SERV IND	0C	UNUSED
CLD PTY OFF-HK:	**0C**	**CLD OFF-HOOK DETECTED**
SERVICE OBSERVED:	0C	NONE
OPER ACTION:	0C	ANI, CUSTOMER DIALED CALL
SERVICE FEATURE:	**029C**	
SIG DIGITS NEXT FIELD:	010C	
ORIG OPEN DIGITS 1:	00007835462C	
ORIG OPEN DIGITS 2:	FFFFFFFFFF	
ORIGINATING CHARGE INFO:	FFFF	
DOMESTIC/INTL INDICATOR:	1C	DOMESTIC
SIG DIGITS NEXT FIELD:	010C	
TERM OPEN DIGITS 1:	00007835478C	
TERM OPEN DIGITS 2:	FFFFFFFFFF	
CONNECT TIME:	1439387C	14:39:38.7
ELAPSED TIME:	000000019C	000000:01.9
MODULE CODE:	042C	CALL RECORD SEQUENCE NUM

1. The call code will be as set by translations
2. As datafilled in OFFICE_ID_ON_AMA_TAPE in OFCENG

1.1.3.9 Ignoring INTRAGRP flag for Nodal RBWF Calls

In the existing RBWF Service, Nodal RBWF between different customer groups does not work when INTRAGRP is N. By this activity RBWF Service functions independent of INTRAGRP flag.

Allowing Nodal RBWF to work between different customer groups even when INTRAGRP flag is N, is controlled with SVBI RBWF Enh SOC and IGNORE_INTRAGRP field of RBWFENH tuple in ISERVOPT.

Default value of IGNORE_INTRAGRP is Y if RBWFENH tuple is not datafilled in table ISERVOPT.

Both SVBI RBWF Enh SOC and IGNORE_INTRAGRP field of RBWFENH tuple in ISERVOPT must be Y, in order to allow Nodal RBWF to work between different customer groups regardless of INTRAGRP flag.

Figure 14 Sample Datafill For RAG tuple in table ISERVOPT

```
SOPTSKEY                                                SOPTSVAR
--------------------------------------------------------------
RBWFENH                                              RBWFENH 5 Y
>
```

1.1.3.10 Increasing Cancellation Timer for Nodal RBWF Calls

Ring again cancellation timer allows the end user to set a limit on how long a nodal or network ring again request can remain active. This value is datafillable through tables CUSTSTN for nodal RAG and CUSTNTWK for network RAG.

Currently range of nodal RAG Cancellation timer (RAGCANTO field of RAGTIM tuple) is 2 to 30, or 0 and range of network RAG Cancellation timer is 5 to 180 mins for ORIGDUR and 5 TO 185 mins for TERMDUR (fields of NTWKRAG option).

The range for RAG Cancellation Timer is extended up to 185 by this activity, so that it includes the value 45.

This functionality is not controlled by any of the SOCs or any other option.

Figure 15 Sample Datafill For RAGTIM tuple in table CUSTSTN

```
TABLE CUSTSTN
CUSTNAME     OPTNAME                                      OPTION
--------------------------------------------------------------
CUSTRAG      RAGTIM                                RAGTIM 8  45
```

1.2 Hardware Requirements or Dependencies

This feature uses the Enhanced Digital Recorded Announcement Machine (EDRAM) to provide the announcement as a result of successful RBWF interrogation. Simple phrases needed for RBWF announcements can be loaded into EDRAM as voice files.

1.3 Software Requirements or Dependencies

Are the same as the ones required by Nodal RAG and BTUP CBWF.

1.4 Limitations and restrictions

This activity is tested and supported for INTL TDM loads only.

All limitations and restrictions that apply to Nodal RAG and BTUP CBWF Services also applies to this activity.

1.5 Interactions

Billing Interaction

When this feature is enabled, the option UNANS_LOCAL in table AMAOPTS is overridden which controls the reporting of unanswered AMA records having Service Feature field because it is necessary to report the BTUP CBWF usage when Ragee or Ragor do not answer.

This feature interacts with AMAREQD option in table CUSTSMDR (feature AJ4226 - The option that controls the generation of AMA management reporting), in the following way:

If the translations do not provide billing trigger and feature AJ4226 (AMA Time To Answer) is active then management reported record for answered/unanswered BTUP-CBWF calls will have the SERVICE FEATURE field marked with 029C. If neither translations nor AMAREQD trigger an AMA record then this feature does not produce an AMA record.

Other Interactions:

All interactions that apply to Nodal RAG and BTUP CBWF are also valid for this activity.

1.6 Glossary

AMA	Automatic Message Accounting
BTUP	British Telecom National User Part
CBWF	Call Back When Free
CONF	Confirmation

NACK	Negative Acknowledgement
NRAG	Network Ring Again
OM	Operational Measurement
PLM	Product Line Management
RAG	Ring Again
RBWF	Ring Back When Free
SVBI	Service Base International

1.7 Recommended Reading/References

a. AG4664 - CBWF using BTUP NEEDs
b. AE0440 - DPNSS CBWF
c. AE0328 - DPNSS CBWF Call Processing
d. AJ04955 - BTUP CBWF Usage Billing
e. A59017799 - RBWF Activation Consistency
f. AJ5518 - Single Digit Activation of RBWF

Appendix A for A00008429: Datafill for RBWF Announcements

This appendix describes changed datafill required for RBWF announcements on an EDRAM card. For complete information, refer to *NTP-297-1001-527 Digital Recorded Announcement Machine DRAM and EDRAM Guide*.

Table CLLI

This table is used to define new CLLIs for two announcement groups. Field TRKGRSIZE defines the total number of members in each group.

Figure 16 Table CLLI

```
TABLE CLLI
CLLI    ADNUM TRKGRSIZ                              ADMININF
-------------------------------------------------------------
RBWFANN   800        4                           MULTIPLE_RBWF
```

Table ANNS

This table assigns the CLLI name defined in table CLLI to an announcement type. Field CLLI contains the CLLI name. For RBWF service, field ANTYPE

must be datafilled with RBWF. Announcement is repeated for number of times defined by MAXCYC field.

Figure 17 Table ANNS

```
TABLE ANNS
CLLI  ANNARCH TRAFSNO   CYTIME MAXCYC                    DATA
-------------------------------------------------------------
RBWFANN    ALL      1       1     1       RBWF    25       1
```

Table ANNMEMS

This table contains the assignments for each announcement member in the announcement group defined in table ANNS. Each tuple here corresponds to one trunk member in its group at MAP TTP level. For custom announcement such as RBWF, hardware type must be DRAM, only one track can be datafilled in field TRACKLIST and the track number must be 0.

Figure 18 Table ANNMEMS

```
TABLE ANNMEMS
ANNMEM      HDWTYPE           CARD
-----------------------------------------------------------
RBWFANN 1   DRAM              DRA   0        DTM    0 14 $
```

Table ANNPHLST

Each tuple in this table defines one custom announcement. For RBWF Announcements, RBWFANN tuple with index 1 corresponds to Max RBWF Requests Reached, and RBWFANN tuple with index 2 corresponds to RBWF Interrogation announcements.

Figure 19 Table ANNPHLST

```
ANNPHKEY          PHSLIST
-------------------------------------------------------------
RBWFANN 1        RBWF_MAX_REQ $
RBWFANN 2        RBWF_INTER1 RBWF_PHONE_NUM RBWF_INTER2 $
```

Please note that announcement provided strictly depends on the datafill of this table. Phrases are announced in the order they are datafilled in this table.

Product = World Trade

A00008477--Increase Size of Table MSGRTE

Functional Description

1: Applicable Solution(s)

Int'l DMS

1.1 Description

This feature provides the expansion of the MSGRTE table size up to 100,000 tuples by adding a new table MSGRTE2.

1.1.1 Table MSGRTE2

New table MSGRTE2 is used for routing and processing of facility messages of some protocols (e.g. PRA, DPNSS, etc.) in a manner identical to that performed by the existing table MSGRTE (Please refer to FN section of AD1315 for more details about the functional model of the table MSGRTE). The selection of which table will be active is achieved by the SOC XLAS0057 as described in the section 2.2.3.

New table MSGRTE2 has the same format as the table MSGRTE, and shares the same functionality provided by the MSGRTE table. The difference, and hence the need for a new table, is that the new table supports up to 100,000 entries while the existing table has a limit of 32K-1 digilator blocks.

Table MSGRTE2 is indexed by a three field key consisting of the Network identifier (NETID), and two digit strings (FROMDIGS and TODIGS). The data in the table is a list of routes made up of one to four route elements. Each element consists of one Message Route Selector (MSGRTSEL) such as LOCAL, PRA, SS7 and DPNSS. Each selector has its own special refinement. A sample of new table MSGRTE2 is shown below in Figure 1:

Figure 1 Sample Datafill of Table MSGRTE2

```
TABLE: MSGRTE2
MSGRTKEY
MSGRTRES
-------------------------------------------------
PUBLIC 12345 12345 ( SS7 ANSIAB_ROUTES 4 0 NEWNET NEWPUB) $
```

1.1.2 Structure of Table MSGRTE2

The structure of table MSGRTE2 is shown in Table 1.

Table 1 Structure of Table MSGRTE2

Field	Subfield or Refinement	Range of Values	Description
MSGRTKEY			*Message Route Key* This is the key to table MSGRTE2 and consists of subfields NETID and DIGRANGE.
	NETID	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES
	DIGRANGE		*Digit Range* This field consists of subfields FROMDIGS and TODIGS.
	FROMDIGS	Alphanumeric (vector up to 10 characters, 0 to 9, A to F)	*From Digits* Digit string for the lower bound of the digit range to which the route list applies
	TODIGS	Alphanumeric (vector up to 10 characters, 0 to 9, A to F)	*To Digits* Digit string for the upper bound of the digit range to which the route list applies
MSGRTRES			*Message Route Result.* The list of routes used to transmit messages. Up to four routes can be datafilled.
	MSGRTSEL	DPNSS, LOCAL, PRA or SS7	*Message Route Selector* • DPNSS if TCAP NRAG messages are sent over DPNSS virtual trunks. • LOCAL if the message terminates on this switch. • PRA if the message is routed out on a specified PRA-D channel. • SS7 if a the message is routed over a specific SS7 route set.

Each Message Route Selector such as DPNSS, LOCAL, PRA and SS7 has its own special refinement.

1.1.2.1 MSGRTSEL = LOCAL

If the entry for field MSGRTSEL is LOCAL, the refinement is as follows.

Table 2 Structure of LOCAL refinement

Field	Subfield or Refinement	Range of Values	Description
	DELDIGS	0 to 15	*Delete Digits* Number of deleted digits from the destination address
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits* Digit string prefixed to the destination address

1.1.2.2 MSGRTSEL = DPNSS

If the entry for field MSGRTSEL is DPNSS, the refinement is as follows.

Table 3 Structure of DPNSS refinement

Field	Subfield or Refinement	Range of Values	Description
	ISUPTRK	Alphanumeric (up to 16 characters)	*ISUP Trunk CLLI Name*
	DELDIGS	0 to 15	*Delete digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix digits*
	OPTIONS	NEWNET	*DPNSS Option*
	NETNAME	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES

1.1.2.3 MSGRTSEL = PRA

If the entry for field MSGRTSEL is PRA, the refinement is as follows.

Table 4 Structure of PRA refinement

Field	Subfield or Refinement	Range of Values	Description
	TRKCLLI	Alphanumeric (up to 16 characters)	*Trunk Common Language Location Identifier* Trunk CLLI name
	DELDIGS	0 to 15	*Delete Digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits*
	OPTIONS	NEWNET or NEWTOR	*PRA Options* • NEWNET for a new network and datafill subfield NETNAME. • NEWTOR for a new type of route and datafill subfield TYPEOFRT.
	NETNAME	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES
	TYPEOFRT	PUB or PVT	*Type of Route* • PUB for a public route. • PVT for a private route.

1.1.2.4 MSGRTSEL = SS7

If the entry for field MSGRTSEL is SS7, the refinement is as follows.

Table 5 Structure of SS7 refinement

Field	Subfield or Refinement	Range of Values	Description
	DPC	Alphanumeric (up to 16 characters)	*Destination Point Code*
	DELDIGS	0 to 15	*Delete Digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits*
	OPTIONS	NEWNET	*SS7 Option*
	NETNAME	String up to 32 characters	*Network Identifier* datafilled in table NETNAMES

1.1.3 Activation of the Feature

Activation of the feature is controlled by SOC XLAS0057.

MSGRTE and MSGRTE2 tables are not effective at the same time - both tables could be datafilled but only one of them will be in effect. The selection of which table will be used is achieved through the SOC option XLAS0057. When the state of the SOC option is ON, MSGRTE table will be disabled and call processing will begin to use the new table MSGRTE2. When the SOC option is IDLE, MSGRTE2 table will be disabled and the MSGRTE table will be in effect.

When the state of the SOC is changed, a warning message will be displayed to inform the user about which table is in use. When the state of the SOC option is changed to ON, following warning message will be displayed 'Table MSGRTE will not be effective, instead MSGRTE2 table will be used.'. When the state of the SOC is changed to IDLE following message will be displayed 'Table MSGRTE2 will not be effective, instead MSGRTE table will be used

Datafill changes can be made independently to either MSGRTE or to MSGRTE2, the system does not keep these tables synchronized. When making a change (e.g. add, delete, update) to the inactive table (as defined by status of SOC XLAS0057) then a warning message will be displayed. The warning message will not be displayed for other operations that does not cause a change (pos, list, etc.) in the table.

1.2 Hardware Requirements or Dependencies

Not Applicable.

1.3 Software Requirements or Dependencies

Not Applicable.

1.4 Limitations and restrictions

Not Applicable.

1.5 Interactions

Not Applicable.

1.6 Applicable customer facing sections

Fault Management

Logs	N/A
Alarms	N/A

Configuration

Data Schema	X

User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Software Optionality Control	X
Office Parameters	N/A
Accounting (includes AMA billing)	N/A
Performance (includes operational measurements)	N/A

1.7 Glossary

Term	Description
PRA	Primary Rate Access
SS7	Signaling System No7
DPNSS	Digital Private Network Signaling System
TCAP	Transaction Capabilities Application Part
NRAG	Network Ring Again

2: Configuration for A00008477

2.1 Hardware and Software Requirements

N/A.

2.2 Initial Configuration

N/A.

2.3 Data schema (DS) (CM, MIBS, RDB)

2.3.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
MSGRTE2	New	New

2.3.2 Table/MIB/Remote Database Schema information

2.3.2.1 Name: MSGRTE2

Message Routing Table (2)

2.3.2.1.1 Functional description

New table MSGRTE2 is used for routing and processing of facility messages of some protocols (e.g. PRA, DPNSS, etc.) in a manner identical to that performed by the existing table MSGRTE (Please refer to FN section of AD1315 for more details about the functional model of the table MSGRTE). This table determines if the message terminates on the current switch or is sent to another switch. This is done through the use of the origination and destination information elements.

New table MSGRTE2 has the same format as the existing table MSGRTE, and shares the same functionality provided by the MSGRTE table. The difference, and hence the need for a new table, is that the new table supports up to 100,000 entries while the existing table has a limit of 32K-1 digilator blocks. The selection of which table will be active is achieved by the SOC XLAS0057.

2.3.2.1.2 Usage sequence and implications (CM Only)

Datafill order of the new table MSGRTE2 is the same as the current datafill order of the existing table MSGRTE.

The following tables must be datafilled before the table MSGRTE2:

- NETNAMES
- TRKMEM
- C7RTESET

All network names in the table MSGRTE2 must already exist in table NETNAMES. Table MSGRTE2 is indexed by the NETID datafilled in Table NETNAMES, so this table must be datafilled before the table MSGRTE2. When an entry tried to deleted from the table NETNAMES, table MSGRTE2 is checked if there is a datafill with the specified NETID. The deletion from NETNAMES table is not allowed if the specified NETID is also datafilled in Table MSGRTE2.

To datafill a DPNSS selector, a source ISUP trunk CLLI must be specified along with a DPNSS selector, and the ISUP trunk CLLI must exist in tables TRKGRP and TRKSGRP.

2.3.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
MSGRTE2	0	100,000*	Memory is allocated dynamically on per tuple

* ***Note:*** *Table MSGRTE2 supports up to 100,000 tuples depending on the amount of the available free memory. The maximum number of tuples may vary due to compression and expansion of tuples.*

2.3.2.1.4 Table Fields

The following table lists fields for the Table MSGRTE2.

Table 3 Table MSGRTE2 field descriptions

Field	New or Changed	Subfield or Refinement	Range of Values	Description
MSGRTKEY	New			*Message Route Key* This is the key to table MSGRTE2 and consists of subfields NETID and DIGRANGE.
		NETID	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES
		DIGRANGE		*Digit Range* This field consists of subfields FROMDIGS and TODIGS.
		FROMDIGS	Alphanumeric (vector up to 10 characters, 0 to 9, A to F)	*From Digits* Digit string for the lower bound of the digit range to which the route list applies
		TODIGS	Alphanumeric (vector up to 10 characters, 0 to 9, A to F)	*To Digits* Digit string for the upper bound of the digit range to which the route list applies

Field	New or Changed	Subfield or Refinement	Range of Values	Description
MSGRTRES	New			*Message Route Result.* The list of routes used to transmit messages. Up to four routes can be datafilled.
		MSGRTSEL	DPNSS, LOCAL, PRA or SS7	*Message Route Selector* • DPNSS if TCAP NRAG messages are sent over DPNSS virtual trunks. • LOCAL if the message terminates on this switch. • PRA if the message is routed out on a specified PRA-D channel. • SS7 if a the message is routed over a specific SS7 route set.

Each Message Route Selector such as DPNSS, LOCAL, PRA and SS7 has its own special refinement.

MSGRTESEL = LOCAL

If the entry for field MSGRTSEL is LOCAL, the refinement is as followed.

Table 4 Structure of LOCAL Refinement

Field	Subfield or Refinement	Range of Values	Description
	DELDIGS	0 to 15	*Delete Digits* Number of deleted digits from the destination address
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits* Digit string prefixed to the destination address

MSGRTESEL = DPNSS

If the entry for field MSGRTSEL is DPNSS, the refinement is as followed.

Table 5 Structure of DPNSS Refinement

Field	Subfield or Refinement	Range of Values	Description
	ISUPTRK	Alphanumeric (up to 16 characters)	*ISUP Trunk CLLI Name*
	DELDIGS	0 to 15	*Delete digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix digits*
	OPTIONS	NEWNET	*DPNSS Option*
	NETNAME	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES

MSGRTESEL = PRA

If the entry for field MSGRTSEL is PRA, the refinement is as followed.

Table 6 Structure of PRA Refinement

Field	Subfield or Refinement	Range of Values	Description
	TRKCLLI	Alphanumeric (up to 16 characters)	*Trunk Common Language Location Identifier* Trunk CLLI name
	DELDIGS	0 to 15	*Delete Digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits*
	OPTIONS	NEWNET or NEWTOR	*PRA Options* • NEWNET for a new network and datafill subfield NETNAME. • NEWTOR for a new type of route and datafill subfield TYPEOFRT.

Field	Subfield or Refinement	Range of Values	Description
	NETNAME	String up to 32 characters	*Network Identifier* Network name datafilled in table NETNAMES
	TYPEOFRT	PUB or PVT	*Type of Route* • PUB for a public route. • PVT for a private route.

MSGRTESEL = SS7

If the entry for field MSGRTSEL is SS7, the refinement is as followed.

Table 7 Structure of SS7 Refinement

Field	Subfield or Refinement	Range of Values	Description
	DPC	Alphanumeric (up to 16 characters)	*Destination Point Code*
	DELDIGS	0 to 15	*Delete Digits*
	PREDIGS	Numeric or N (vector of up to 11 characters)	*Prefix Digits*
	OPTIONS	NEWNET	*SS7 Option*
	NETNAME	String up to 32 characters	*Network Identifier* datafilled in table NETNAMES

2.3.2.1.5 Datafill example

The following example shows sample datafill for table MSGRTE2.

Figure 2 Sample Datafill of Table MSGRTE2

```
TABLE: MSGRTE2
MSGRTKEY
MSGRTRES
-------------------------------------------------------------
PUBLIC 12345 12345 (SS7 ANSIAB_ROUTES 4 0 (NEWNET NEWPUB) $)$
```

2.3.2.1.6 Table release history update

Table is newly created.

2.3.2.1.7 Supplementary information

None.

2.4 Service Orders (SO) (CM & SESM)

N/A

2.5 Software optionality control (SOC)

Table 8 SOC

SOC option name:	XLAS MSGRTE2
SOC option title:	XLAS
SOC option control type:	STATE
New SOC option?	Yes
SOC option order code	XLAS0057
Option defined in DRU:	WT
Affected products:	ISN09

MSGRTE and MSGRTE2 tables are not effective at the same time - both tables could be datafilled but only one of them will be in effect. The selection of which table will be used is achieved through the SOC option XLAS0057. When the state of the SOC option is ON, MSGRTE table will be disabled and call processing will begin to use the new table MSGRTE2. When the SOC option is IDLE, MSGRTE2 table will be disabled and the MSGRTE table will be in effect.

2.6 Element Management

N/A.

2.7 Security

N/A.

2.8 Configuration Walkthrough

N/A.

Product = World Trade

A00008484--IN Terminating Trigger Feature Interactions

Functional Description

1: Applicable Solution(s)

Int'l DMS

1.1 Description

1.1.1 Introduction

The CustomNet product has remained largely unchanged for a number of years. Users are demanding the enhanced services provided on various VoIP platforms without wanting to change from their existing CustomNet service.

The whole project provides the vehicle to enhance CustomNet so the user can retain existing functionality whilst adding new functionality from various application server platforms to provide features such as:

- Presence
- Instant Messaging
- Document sharing/collaboration
- Click to Call
- Find-me/Follow-me

Most enhanced features to be delivered from the application servers can be mapped into one of three call models:

- Call Notification (supports Presence, Call Logs, etc)

This model involves informing the application servers that the user is involved in a call and with whom. It is applied on all originating calls and is the default model for terminating calls.

- Call Routing (supports Find-me/Follow-me, Call Screening, etc)

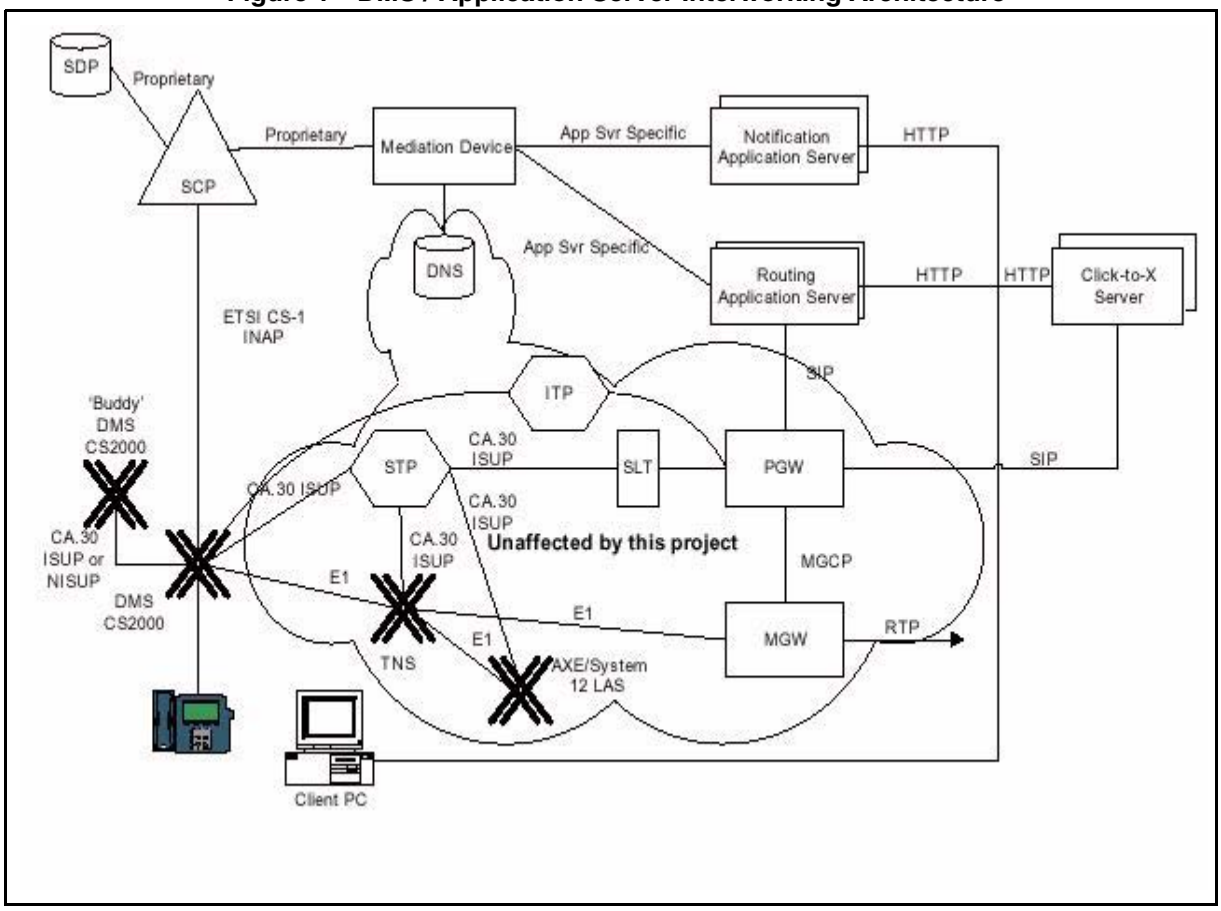
This model is only applicable for incoming calls and even then, only for a certain set of services under a limited set of conditions. The routing information must be either a single destination or a sequence (e.g. forwarding on busy or no answer).

- Click-to-X (supports Click-to-call, some forms of conferencing, etc)

Where an application server must initiate calls then this model applies.

The architecture, as seen in figure “DMS / Application Server Interworking Architecture” on page 2227, consists of several elements that essentially convert events in the DMS/CS2000 switch captured through traditional IN triggers (TDP-3, originating EDPs, TDP-12, terminating EDPs) and convert them to messages for interworking with the application servers.

Figure 1 DMS / Application Server Interworking Architecture



These call models however, do not support many low-level line based features which are best supported from the access exchange which implies a co-existence between IN and non-IN features (which are listed in table “Feature list” on page 2227) which is the subject of this part of the whole project.

Table 1 Feature list

Feature Name
Account Codes
Additional Directory Number
Authorization Codes
Automatic Call Back (RAG)
Automatic Dial (AUD)
Busy Verification
Call Barring (Network Class Of Service)

Feature Name
Call Forward All Calls (CFI)
Call Forward Busy - Block Internal (CBI)
Call Forward Busy (CFB)
Call Forward Extensions
Call Forward No Answer (CFD)
Call Hold
Call Park (PRK)
Call Pick Up Group (CPU)
Calling Name Delivery
Calling Name Display
Calling Number Delivery
Calling Number Display
Camp-On (MBSCAMP)
Class Of Service Restrictions
Conference 6 (CNF C06)
Date & Time
Direct Call Park (DCPK)
Direct Station Select/Busy Lamp Field (BLF)
Directed Call Pick Up (DCPU)
Display Queued Calls
Do Not Disturb
Flexible Console Alerting
Intercom Group (GIC)
Key Short Hunt (KSH)
Last Number Redial (LNR)
Last Number Redial from Set (LNRA)
Multiple Appearance Of Directory Numbers (MDN)
Music on Hold (KSMOH)
Permanent Hold (HLD) Including Music on Hold

Feature Name
Speed Call Long (SCL)
Speed Call Short (SCS)
Transfer, Hold & 3 way Conference (CXR)

1.1.2 Interaction Model

Since non-IN features listed may involve multi-leg calls (i.e. CXR) it is best to describe the interactions based on the scenarios where calls are a combination of basic call and IN call.

1.1.2.1 Basic Call

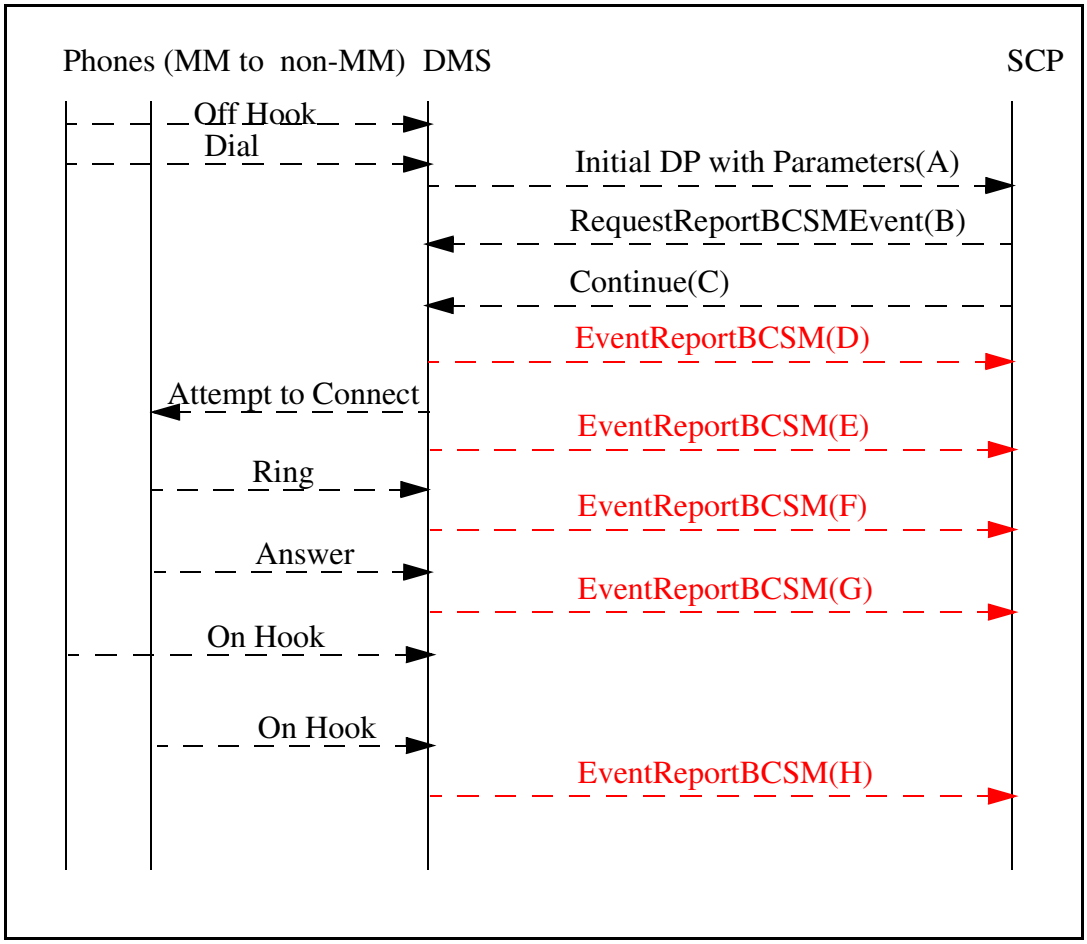
Neither TDP-3 nor TDP-12 triggering occurs.

1.1.2.2 IN Call

Multiple IN dialogs (i.e. TDP-3 and TDP-12 together) for a single call at the same time are not supported. An IN call may be thought as one of the followings:

1.1.2.2.1 MM to non-MM

In this case TDP-3 triggering occurs.



(A) Initial DP with Parameters:

The parameters sent to the SCP are SERVKEY, CLI, CDPA, EVENT_TYPE, OCN, RDN and RD_INFO.

EVENT_TYPE in this scenario is INFOANAL which means TDP-3. OCN, RDN and RD_INFO is to be used for call forward cases.

(B) RequestReportBCSMEvent:

The originating BCSM events armed by the SCP are EDP-4(N), EDP-5(N), EDP-6(N), EDP-7(N), EDP-9(N, for port1 and port 2) and EDP-10(N). Since the only functions of interest for originating calls are those associated with the Call Notification model, Notify and Continue EDPs are used for Presence, Call Logs, etc.

(C) Continue

Since the only functions of interest for originating calls are those associated with the Call Notification model, Continue is sent for Presence, Call Logs, etc.

(D) EventReportBCSM:

At this point EDP-4(Route Select Failure) or EDP-10(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(E) EventReportBCSM:

At this point EDP-5(Busy) or EDP-10(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(F) EventReportBCSM:

At this point EDP-6(No Answer) or EDP-10(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(G) EventReportBCSM:

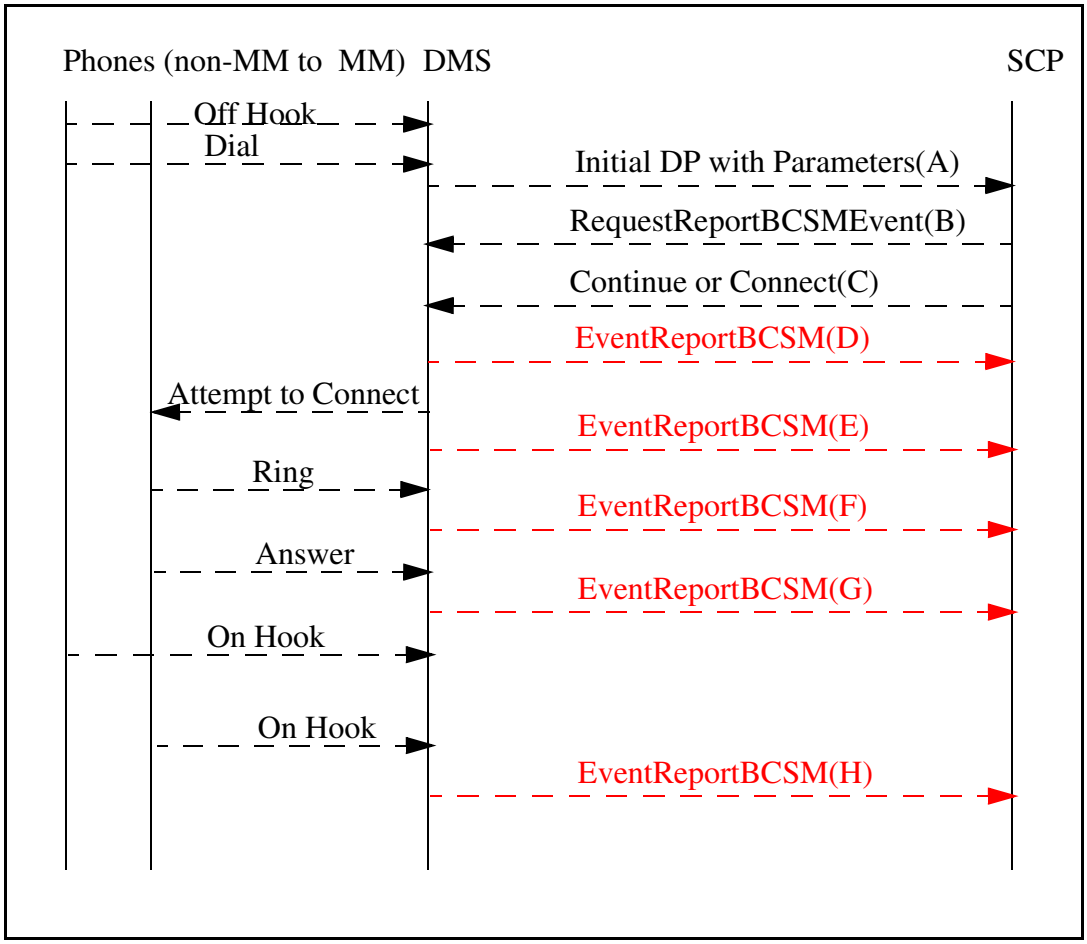
At this point call is answered and EDP-7(Answer) is encountered. EventReportBCSM is sent to SCP to notify that the call has been answered.

(H) EventReportBCSM:

At this point either the calling party or the called party on hooked and EDP-9(Disconnect) is encountered. EventReportBCSM is sent to SCP to notify that the call has been ended by the calling party (EventReportBCSMEvent for port 1) or the called party (EventReportBCSMEvent for port 2).

1.1.2.2.2 Non-MM to MM

In this case TDP-12 triggering occurs.



(A) Initial DP with Parameters:

The parameters sent to the SCP are SERVKEY, CLI, CDPA, EVENT_TYPE, OCN, RDN and RD_INFO.
EVENT_TYPE in this scenario is TERMATT which means TDP-12.
OCN, RDN and RD_INFO is to be used for call forward cases.

(B) RequestReportBCSMEvent:

If Connect is to be sent after RequestReportBCSMEvent then the originating BCSM events armed by the SCP are EDP-4(N), EDP-5(R, N), EDP-6(R, N), EDP-7(N), EDP-9(N, for port1 and port 2) and EDP-10(N). If Continue is to be sent after RequestReportBCSMEvent then the terminating BCSM events armed by the SCP are EDP-13(R, N), EDP-14(R, N), EDP-15(N), EDP-17(N, for port1 and port 2) and EDP-18(N). Terminating calls make use of both the Call Notification and Call Routing models and in order to requery Interrupted EDPs are used for busy and no answer cases along with Notify and Continue EDPs.

(C) Continue or Connect

Terminating calls make use of both the Call Notification and Call Routing models and there are 3 possibilities for Call Routing model (Call Notification is similar to that used for originating calls except for the use of TDP-12 and terminating EDPs) as follows:

After querying the AS;

- if the destination number is that of the terminating MM user itself then the SCP issues a Continue message.
- if the destination number is not that of terminating MM user itself then the SCP issues a Connect message to connect the call directly.
- if the call is to be routed through AS then the SCP issues a Connect message with the AS as the destination number.

(D) EventReportBCSM:

At this point EDP-4(Route Select Failure) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(E) EventReportBCSM:

At this point (EDP-5, EDP-13)(Busy) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended. For busy cases if the EDP is interrupted then requery is also possible.

(F) EventReportBCSM:

At this point (EDP-6, EDP-14)(No Answer) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended. For no answer cases if the EDP is interrupted then requery is also possible.

(G) EventReportBCSM:

At this point call is answered and (EDP-7, EDP-15)(Answer) is encountered. EventReportBCSM is sent to SCP to notify that the call has been answered.

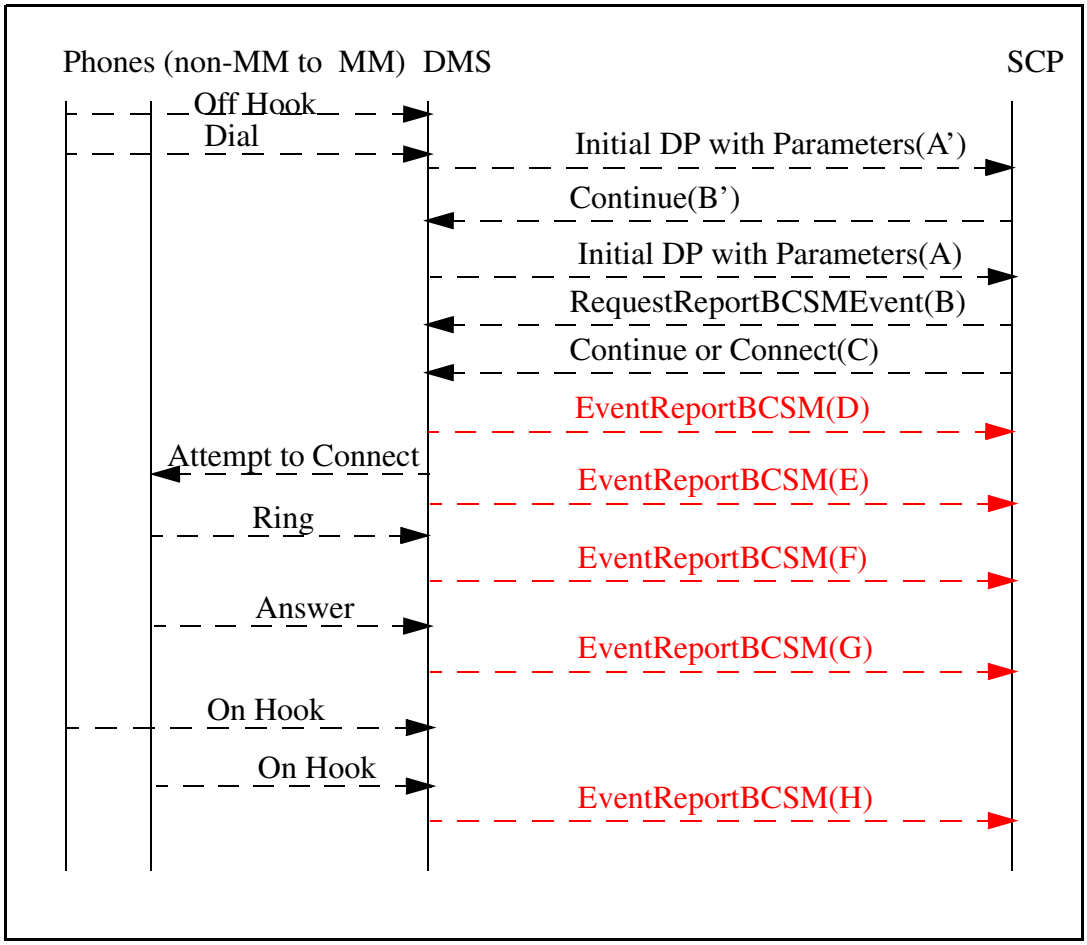
(H) EventReportBCSM:

At this point either the calling party or the called party on hooked and (EDP-9, EDP-17)(Disconnect) is encountered. EventReportBCSM is sent to SCP to notify that the call has been ended by the calling party (EventReportBCSMEvent for port 1) or the called party (EventReportBCSMEvent for port 2).

1.1.2.2.3 MM to MM

This case involves both the TDP-3 triggering and the TDP-12 triggering but since two open IN dialogs can not co-exist a workaround is proposed as follows:

After TDP-3 triggering, the SCP, by the help of the SDP, checks the calling and called parties for whether both are multimedia users in the same switch or not. If so (it is in this case) then SCP will not arm EDPs (this lets TDP-12 triggering) and the multimedia session will be provided by TDP-12 and terminating EDPs.



(A') Initial DP with Parameters:

The parameters sent to the SCP are SERVKEY, CLI, CDPA, EVENT_TYPE, OCN, RDN and RD_INFO.

EVENT_TYPE in this scenario is INFOANAL which means TDP-3. OCN, RDN and RD_INFO is to be used for call forward cases.

(B') Continue

Since at this point, the SCP, by the help of the SDP, determines that the calling and called parties both are multimedia users in the same switch and the only functions of interest for originating calls are those associated with the Call Notification model, Continue is sent for Presence, Call Logs, etc without sending RequestReportBCSMEvent.

(A) Initial DP with Parameters:

The parameters sent to the SCP are SERVKEY, CLI, CDPA, EVENT_TYPE, OCN, RDN and RD_INFO.
EVENT_TYPE in this scenario is TERMATT which means TDP-12.
OCN, RDN and RD_INFO is to be used for call forward cases.

(B) RequestReportBCSMEvent:

If Connect is to be sent after RequestReportBCSMEvent then the originating BCSM events armed by the SCP are EDP-4(N), EDP-5(R, N), EDP-6(R, N), EDP-7(N), EDP-9(N, for port1 and port 2) and EDP-10(N). If Continue is to be sent after RequestReportBCSMEvent then the terminating BCSM events armed by the SCP are EDP-13(R, N), EDP-14(R, N), EDP-15(N), EDP-17(N, for port1 and port 2) and EDP-18(N). Terminating calls make use of both the Call Notification and Call Routing models and in order to requery Interrupted EDPs are used for busy and no answer cases along with Notify and Continue EDPs.

(C) Continue or Connect

Terminating calls make use of both the Call Notification and Call Routing models and there are 3 possibilities for Call Routing model (Call Notification is similar to that used for originating calls except for the use of TDP-12 and terminating EDPs) as follows:

After querying the AS;

- if the destination number is that of the terminating MM user itself then the SCP issues a Continue message.
- if the destination number is not that of terminating MM user itself then the SCP issues a Connect message to connect the call directly.
- if the call is to be routed through AS then the SCP issues a Connect message with the AS as the destination number.

(D) EventReportBCSM:

At this point EDP-4(Route Select Failure) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended.

(E) EventReportBCSM:

At this point (EDP-5, EDP-13)(Busy) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended. For busy cases if the EDP is interrupted then requery is also possible.

(F) EventReportBCSM:

At this point (EDP-6, EDP-14)(No Answer) or (EDP-10, EDP-18)(Abandon) may be encountered. EventReportBCSM is sent to SCP to notify that the call has ended. For no answer cases if the EDP is interrupted then requery is also possible.

(G) EventReportBCSM:

At this point call is answered and (EDP-7, EDP-15)(Answer) is encountered. EventReportBCSM is sent to SCP to notify that the call has been answered.

(H) EventReportBCSM:

At this point either the calling party or the called party on hooked and (EDP-9, EDP-17)(Disconnect) is encountered. EventReportBCSM is sent to SCP to notify that the call has been ended by the calling party (EventReportBCSMEvent for port 1) or the called party (EventReportBCSMEvent for port 2).

As seen from the figure above, MM to MM case may be summarized in terms of the MM to non-MM and non-MM to MM cases as follows:

- MM to non-MM case (TDP-3 triggering occurs however no RequestReportBCSMEvent is sent).
- non-MM to MM case (TDP-12 triggering occurs).

1.1.3 Feature Interactions

1.1.3.1 Account Codes

No impact.

1.1.3.2 Additional Directory Number

No impact.

1.1.3.3 Authorization Codes

No impact.

1.1.3.4 Automatic Call Back (RAG)

A off-hooks and dials B (busy) which results in the following IN call.

IN Call	
A	B(busy)

ERB(s) reported: Busy
Remaining EDP(s): If reported ERB is R then EDPs armed for port 1 remain. If reported ERB is N then no EDPs remain.

If B is busy, (EDP-5(N), EDP-13(N)) is encountered and Busy EventReportBCSM is sent to SCP to notify that the call has ended and A hears busy tone. A activates RAG and on-hooks. When B on-hooks, A rings and after A off-hooks B is called automatically as if A dials B again which results in the following IN call.

IN Call	
A	B

This is the same as a normal IN call from A to B although it is a RAG generated call.

Limitation / Restriction:

If EDP-5(R) or EDP-13(R) is used then Busy ERB is reported but the caller does not hear busy tone (since the SSP waits instructions from the SCP, like connecting to a new destination) and can not use the RAG feature. However after Busy ERB is reported, if a Continue or EDP-5(N) or EDP-13(N) followed by a Continue or a Connect to a busy destination or EDP-5(N) or EDP-13(N) followed by a Connect to a busy destination is sent then it is still possible to invoke RAG. For Connect scenarios to another busy destination RAG is activated for the second call.

1.1.3.5 Automatic Dial (AUD)

No impact.

1.1.3.6 Busy Verification

This is an MSAC related feature and IN interaction with MSAC is not supported.

1.1.3.7 Call Barring (Network Class Of Service)

No impact.

1.1.3.8 Call Forward All Calls (CFI)

There are three possible scenarios as follows:

(a) Both the original and the forwarded calls are IN calls.

A off-hooks and dials B which results in the following IN call.

IN Call(1)	
A	B

This is a normal IN call although B does not ring. The call is treated as if A called another party if forwarded call does not produce a new IN trigger.

If B has CFI to C, then B does not ring and call is immediately transferred to C and if this transfer produces a new IN dialog then the first IN dialog is aborted except a TDP-12 does not abort a previous TDP-3.

For this new IN dialog there are call forwarding parameters present.

If trombone trunking is not used:

IN Call(2)	
A	C

The forwarded call produced a new IN trigger which aborts the previous one (only TDP-3 aborts a previous dialog). This is the same as a normal IN call from A to C.

If trombone trunking is used:

IN Call(2)	
A	Trunk

IN Call(3)	
Trunk	C

If the SCP decides to use a trombone trunk then the calling and the forwarded parties are tracked by two IN dialogs which are again the same as normal IN calls from A to trunk and trunk to C.

(b) The original call is an IN call but the forwarded call is not.

A off-hooks and dials B which results in the following IN call.

IN Call	
A	B

This is a normal IN call although B does not ring. The call is treated as if A called another party if forwarded call does not produce a new IN trigger.

If B has CFI to C, then B does not ring and call is immediately transferred to C and if this transfer does not produce a new IN dialog then the first IN dialog is used.

IN Call	
A	C

The forwarded call does not produce a new IN trigger. This is the same as a normal IN call from A to B except that C just replaces B.

Limitation / Restriction:

SCP does not understand that C has replaced B.

(c) The original call is not an IN call but the forwarded call is.

A off-hooks and dials B which results in the following basic call.

Basic Call	
A	B

This is a basic call which actually implies that both A and B are non-MM users. B again does not ring.

If B has CFI to C then B does not ring and call is immediately transferred to C and if this transfer produces an IN dialog then this IN dialog is used.

For this IN dialog there are call forwarding parameters present.

IN Call	
A	C

This is the same as a normal IN call from from A to C. B party may be ignored easily.

1.1.3.9 Call Forward Busy - Block Internal (CBI)

This is the same as the CFB case except that internal calls are blocked and are not forwarded. In other words, if the call is external then it is treated as CFBcase and if the call is internal it is treated as an IN call to a busy party.

1.1.3.10 Call Forward Busy (CFB)

There are three possible scenarios as follows (A, B or C may be trunks):

(a) Both the original and the forwarded calls are IN calls.

A off-hooks and dials B (busy) which results in the following IN call.

IN Call(1)	
A	B(busy)

This is a normal IN call except Busy ERB is not reported. The call is treated as if A called another party if forwarded call does not produce a new IN trigger.

If B has CFB to C and B is busy then call is immediately transferred to C without hitting (EDP-5, EDP-13)(Busy) and if this transfer produces a new IN dialog then the first IN dialog is aborted except a TDP-12 does not abort a previous TDP-3.

For this new IN dialog there are call forwarding parameters present.

If trombone trunking is not used:

IN Call(2)	
A	C

The forwarded call produced a new IN trigger which aborts the previous one (only TDP-3 aborts a previous dialog). This is the same as a normal IN call from A to C.

If trombone trunking is used:

IN Call(2)	
A	Trunk

IN Call(3)	
Trunk	C

If the SCP decides to use a trombone trunk then the calling and the forwarded parties are tracked by two IN dialogs which are again the same as normal IN calls from A to trunk and trunk to C.

(b) The original call is an IN call but the forwarded call is not.

A off-hooks and dials B (busy) which results in the following IN call.

IN Call	
A	B(busy)

This is a normal IN call except Busy ERB is not reported The call is treated as if A called another party if forwarded call does not produce a new IN trigger.

If B has CFB to C and B is busy then call is immediately transferred to C without hitting (EDP-5, EDP-13)(Busy) and if this transfer does not produce a new IN dialog then the first IN dialog is used. (EDP-5, EDP-13)(Busy) is still valid.

IN Call	
A	C

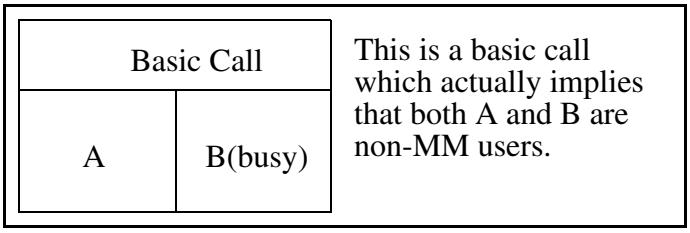
The forwarded call does not produce a new IN trigger. This is the same as a normal IN call from A to B except that C just replaces B.

Limitation / Restriction:

SCP does not understand that C has replaced B.

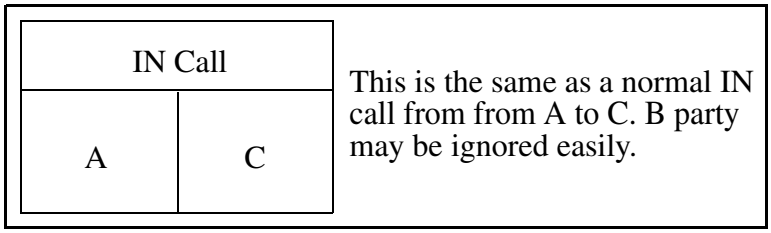
(c) The original call is not an IN call but the forwarded call is.

A off-hooks and dials B (busy) which results in the following basic call.



If B has CFB to C and B is busy then call is immediately transferred to C and if this transfer produces an IN dialog then this IN dialog is used.

For this IN dialog there are call forwarding parameters present.



1.1.3.11 Call Forward Enhancements

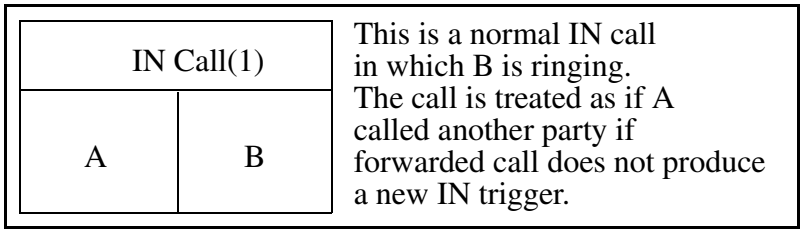
This is similar to other call forward cases as it enhances them. For the description of this feature please see Appendix section at the end of this document.

1.1.3.12 Call Forward No Answer (CFD)

There are three possible scenarios as follows (A, B or C may be trunks):

(a) Both the original and the forwarded calls are IN calls.

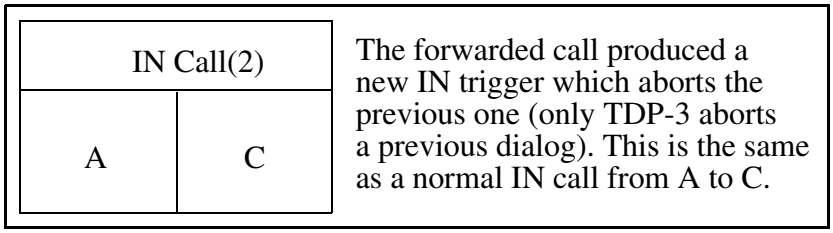
A off-hooks and dials B which results in the following IN call.



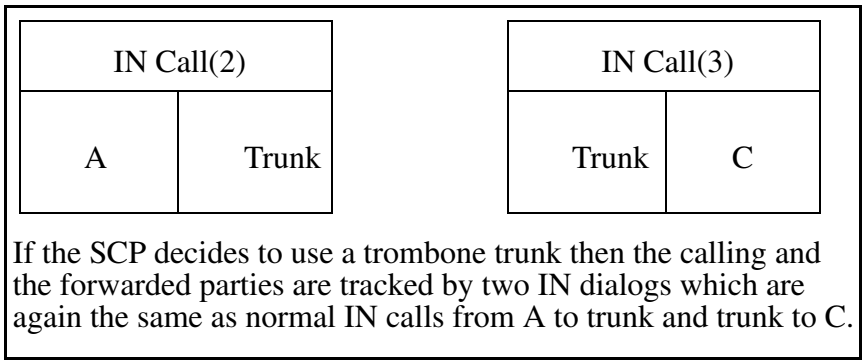
If B has CFD to C and B does not answer then call is transferred to C if EDP-6 timer > CFD timer and if this transfer produces a new IN dialog then the first IN dialog is aborted except a TDP-12 does not abort a previous TDP-3. If EDP-6 timer < CFD timer then EDP-6 has precedence and call forwarding will not occur. EDP-6 timer = CFD timer case is not supported.

For this new IN dialog there are call forwarding parameters present.

If trombone trunking is not used:

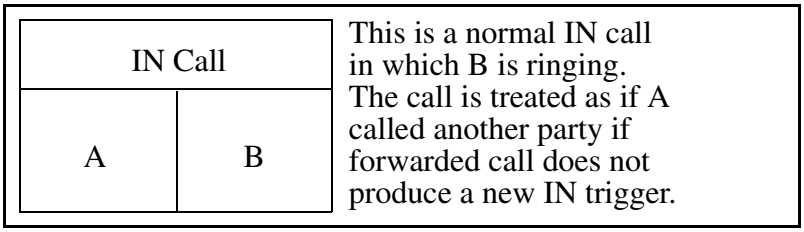


If trombone trunking is used:

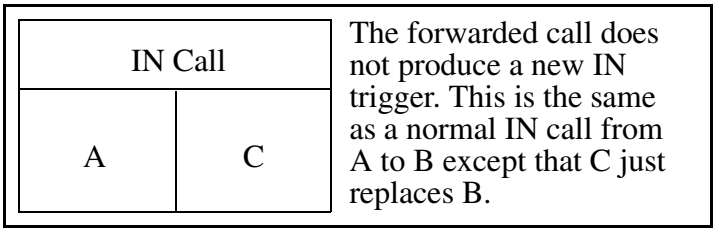


(b) The original call is an IN call but the forwarded call is not.

A off-hooks and dials B which results in the following IN call.



If B has CFD to C and B does not answer then call is transferred to C if EDP-6 timer > CFD timer and if this transfer does not produce a new IN dialog then the first IN dialog is used. EDP-6 is still valid. If EDP-6 timer < CFD timer then EDP-6 has precedence and call forwarding will not occur. EDP-6 timer = CFD timer case is not supported.



Limitation / Restriction:

SCP does not understand that C has replaced B.

(c) The original call is not an IN call but the forwarded call is.

A off-hooks and dials B which results in the following basic call.

Basic Call	
A	B

This is a basic call which actually implies that both A and B are non-MM users.

If B has CFD to C and C does not answer then call is immediately transferred to C and if this transfer produces an IN dialog then this IN dialog is used.

For this IN dialog there are call forwarding parameters present.

IN Call	
A	C

This is the same as a normal IN call from from A to C. B party may be ignored easily.

1.1.3.13 Call Hold

(a) The calling party activates CHD.

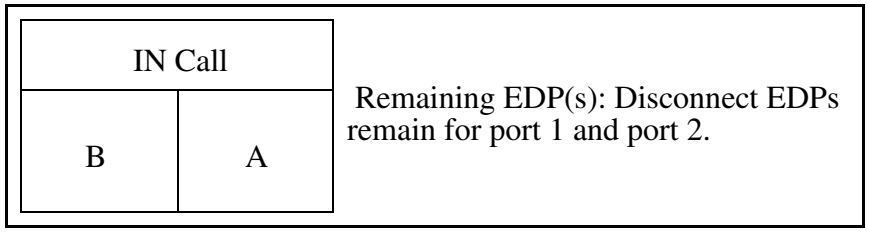
A and B are talking in an IN call as follows:

IN Call	
A	B

ERB(s) reported: Answer
Remaining EDP(s): Disconnect EDPs remain for port 1 and port 2.

A activates CHD and B is on hold. If A reactivates CHD, it returns back to the original call above.

If A on-hooks the controller is migrated to port 2 if it is not already on port 2 as follows and A is re-rung by B and A answers. This answer does not produce a new Answer ERB since it has already been reported.



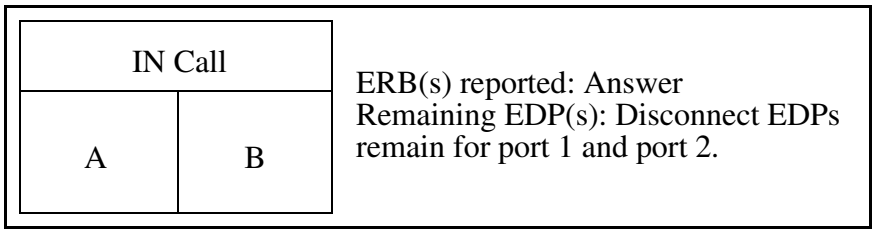
After this point if A on-hooks a Disconnect ERB is reported for port 2 and if B on-hooks a Disconnect ERB is reported for port 1.

If A does not answer the rering until timeout then a Disconnect ERB is reported for port 2.

While on hold if B on-hooks a Disconnect ERB is reported for port 1.

(b) The called party activates CHD.

A and B are talking in an IN call as follows:



B activates CHD and A is on hold. If B reactivates CHD, it returns back to the original call above.

If B on-hooks, the controller is not migrated to port 2 as it is already on port 2 and B is rering by A and B answers. This answer does not produce a new Answer ERB since it has already been reported.

After this point if A on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

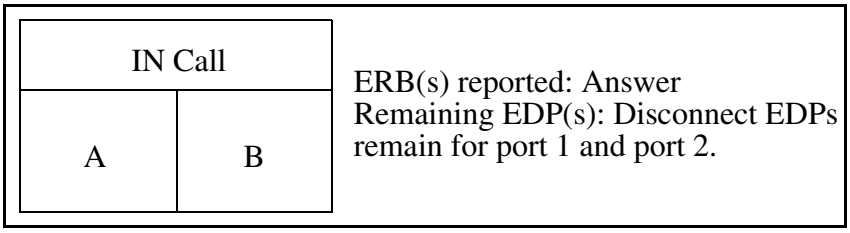
If B does not answer the rering until timeout then a Disconnect ERB is reported for port 2.

While on hold if A on-hooks a Disconnect ERB is reported for port 1.

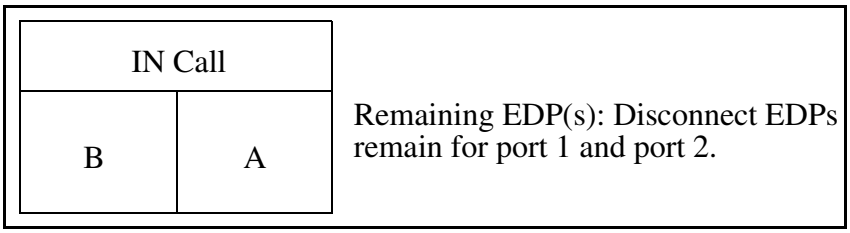
1.1.3.14 Call Park (PRK)

(a) The calling party activates PRK.

A and B are talking in an IN call as follows:



A activates PRK and B is parked. The parkee is migrated to port 1 if it is not already on port 1 as follows.

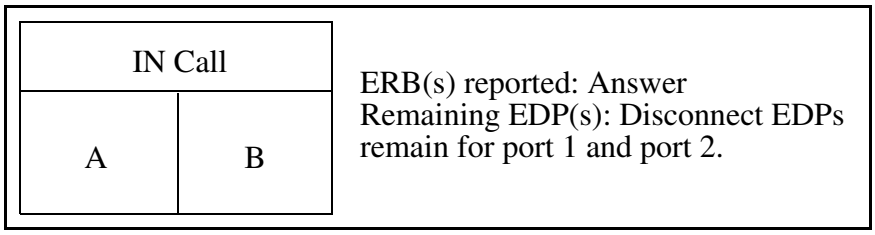


A reactivates PRK and retrieves B and after this point if A on-hooks a Disconnect ERB is reported for port 2 and if B on-hooks a Disconnect ERB is reported for port 1.

While parked if B on-hooks a Disconnect ERB is reported for port 1.

(b) The called party activates PRK.

A and B are talking in an IN call as follows:

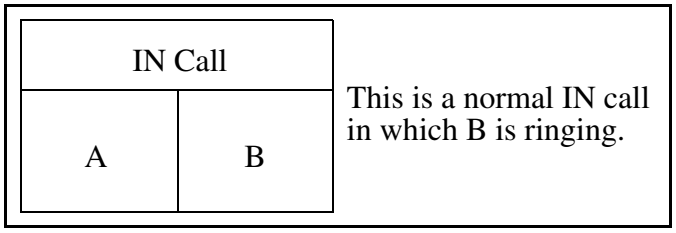


B activates PRK and A is parked. The parkee is not migrated to port 1 as it is already on port 1. B activates PRK and retrieves A and after this point if A on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

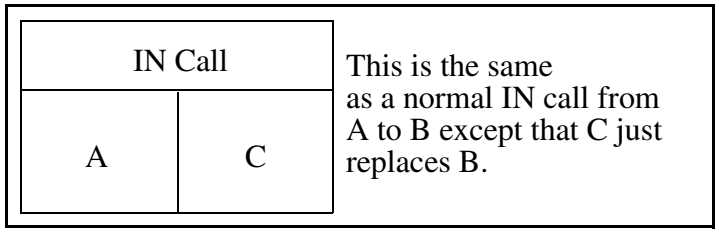
While parked if A on-hooks a Disconnect ERB is reported for port 1.

1.1.3.15 Call Pick Up Group (CPU)

A dials B which results in the following IN call.



Before B answers and EDP-6 timer expires, C activates CPU and an Answer ERB is reported. After this point if A on-hooks a Disconnect ERB is reported for port 1 and if C on-hooks a Disconnect ERB is reported for port 2.



Limitation / Restriction:

SCP does not understand that C has replaced B.

1.1.3.16 Calling Name Delivery

No impact.

1.1.3.17 Calling Name Display

No impact.

1.1.3.18 Calling Number Delivery

No impact.

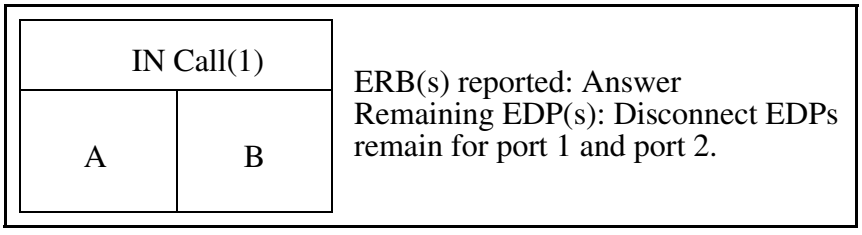
1.1.3.19 Calling Number Display

No impact.

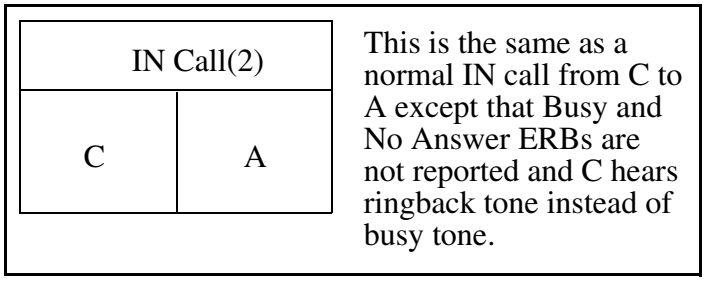
1.1.3.20 Camp-On (MBSCAMP)

(a) Both the call to be camped on and the call that camps on are IN calls.

A and B are talking in an IN call as follows:

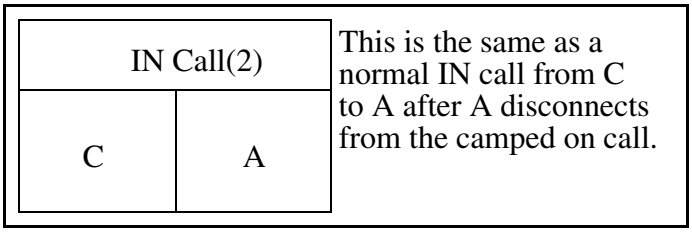


C has MBSCAMP and dials A and hears audible ringback tone instead of busy tone. A hears a special tone. Busy and No Answer ERBs are not reported.



If B on-hooks a Disconnect ERB is reported for port 2 from the first IN dialog. A on-hooks and rings. When A answers an Answer ERB is reported from the second IN dialog.

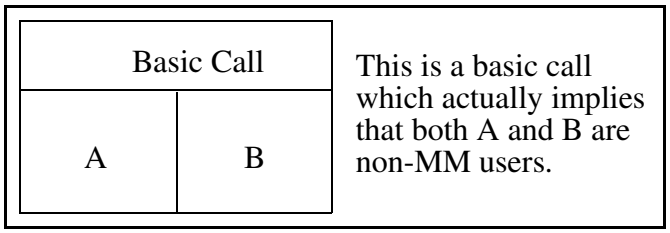
If A on-hooks a Disconnect ERB is reported for port 1 from the first IN dialog. A rings. When A answers an Answer ERB is reported from the second IN dialog.



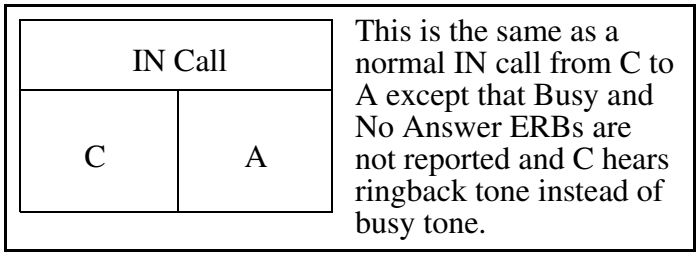
After this point if A on-hooks a Disconnect ERB is reported for port 2 and if C on-hooks a Disconnect ERB is reported for port 1.

(b) The call to be camped on is a basic call and the call that camps on is an IN call.

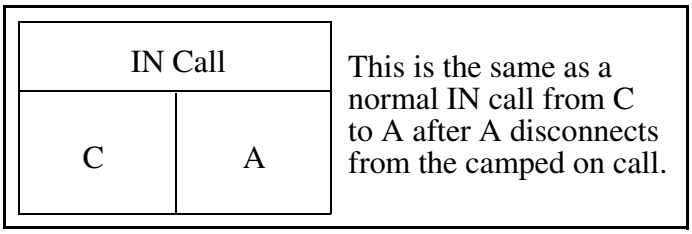
A and B are talking in a basic call as follows:



C has MBSCAMP and dials A and hears audible ringback tone instead of busy tone. A hears a special tone. Busy and No Answer ERBs are not reported.



A on-hooks. A rings. When A answers an Answer ERB is reported.



After this point if A on-hooks a Disconnect ERB is reported for port 2 and if C on-hooks a Disconnect ERB is reported for port 1.

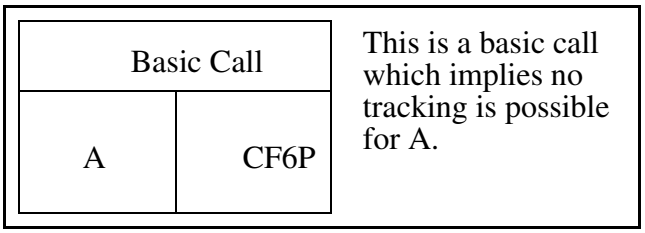
1.1.3.21 Class Of Service Restrictions

No impact.

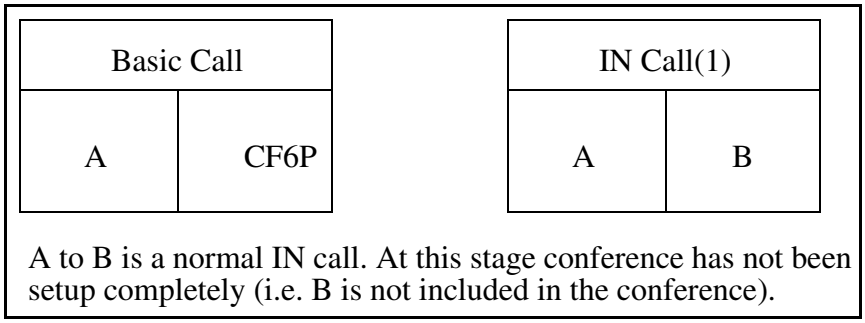
1.1.3.22 Conference 6 (CNF C06)

(a) The party which starts the conference directly activates CNF C06 without being active in a call.

A off-hooks and activates CNF C06 which results in the following basic call:

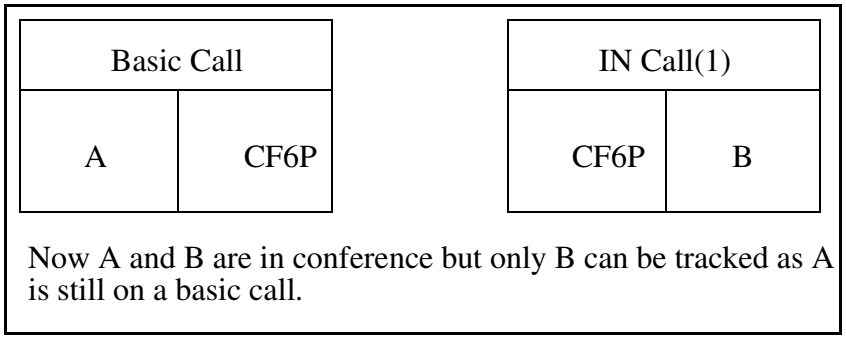


A flashes and dials B which results in the following topology:



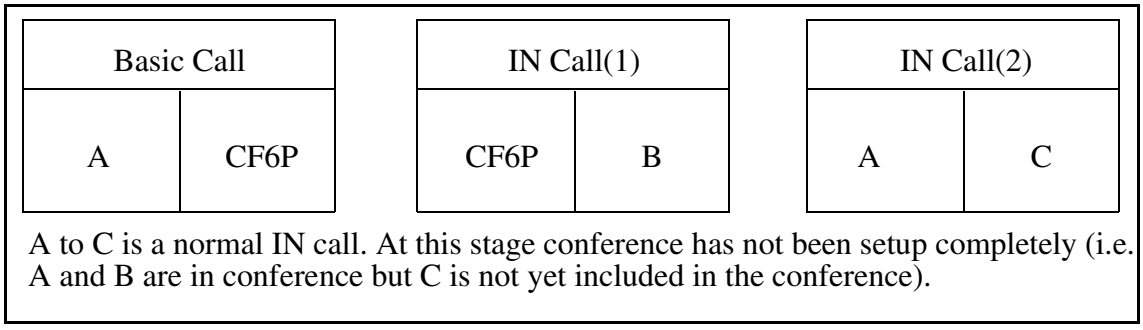
A to B is a normal IN call. At this stage conference has not been setup completely (i.e. B is not included in the conference).

A activates CNF C06 which actually sets up the conference as follows:



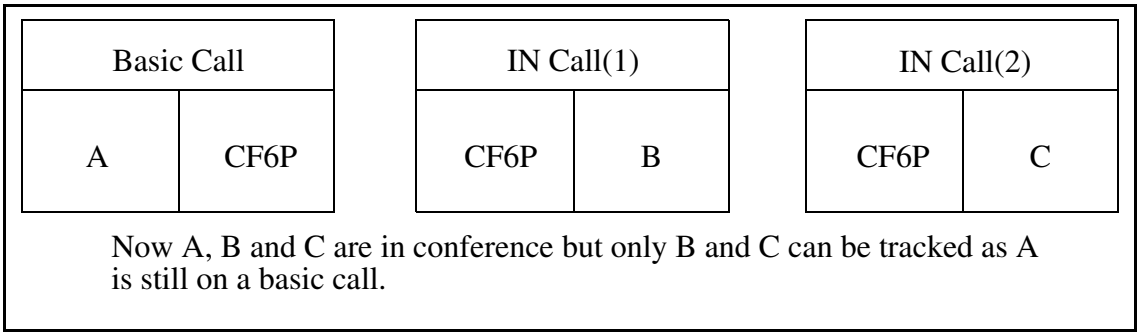
Now A and B are in conference but only B can be tracked as A is still on a basic call.

A flashes and dials C which results in the following topology. This case is similar to the case above where A flashes and dials B.



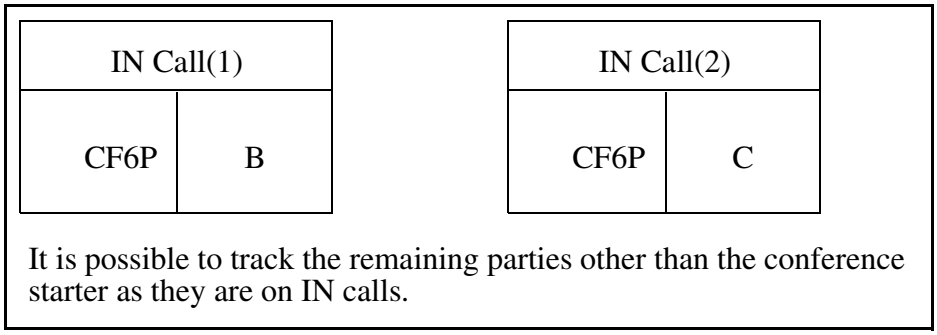
A to C is a normal IN call. At this stage conference has not been setup completely (i.e. A and B are in conference but C is not yet included in the conference).

A activates CNF C06 which actually sets up the conference for all parties (i.e. C is included to the conference).



D, E and F can attend the conference in the same way.

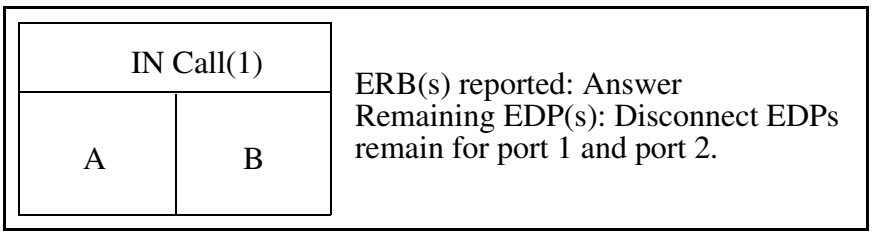
If A on-hooks no indication is sent to SCP since A is on a basic call. The remaining parties stay in conference.



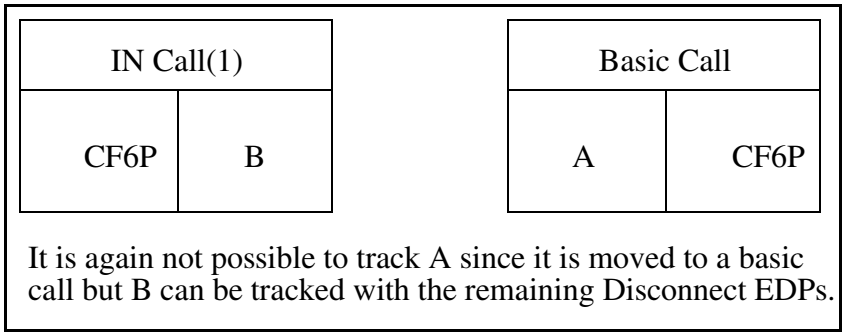
If B, C, D, E or F on-hooks a Disconnect ERB is reported for port 2.

(b) The party which starts the conference is already active in an IN call.

A and B are talking in an IN Call as follows:

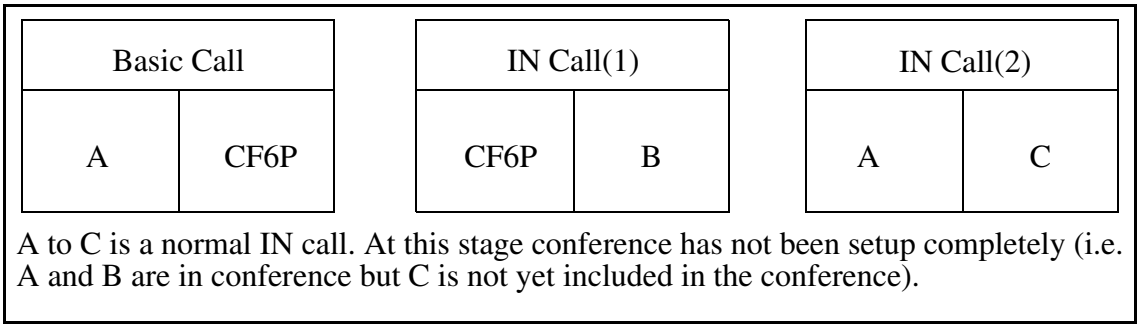


A activates CNF C06 which immediately sets up the conference.



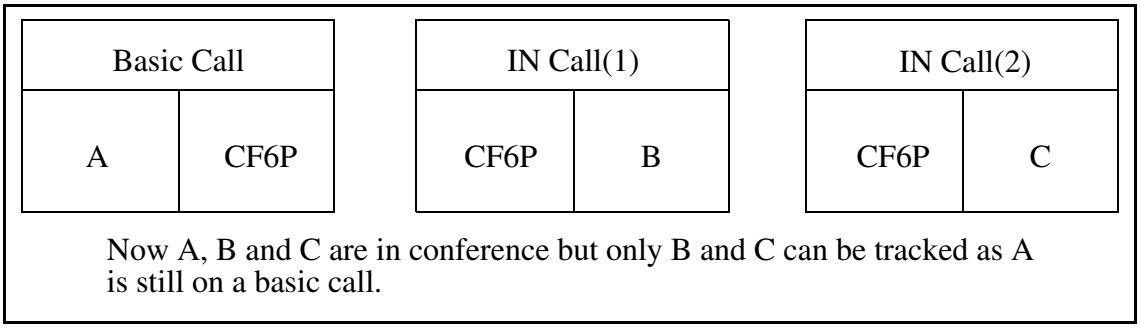
It is again not possible to track A since it is moved to a basic call but B can be tracked with the remaining Disconnect EDPs.

A flashes and dials C which results in the following topology. This case is similar to the case in (a) where A flashes and dials C.



A to C is a normal IN call. At this stage conference has not been setup completely (i.e. A and B are in conference but C is not yet included in the conference).

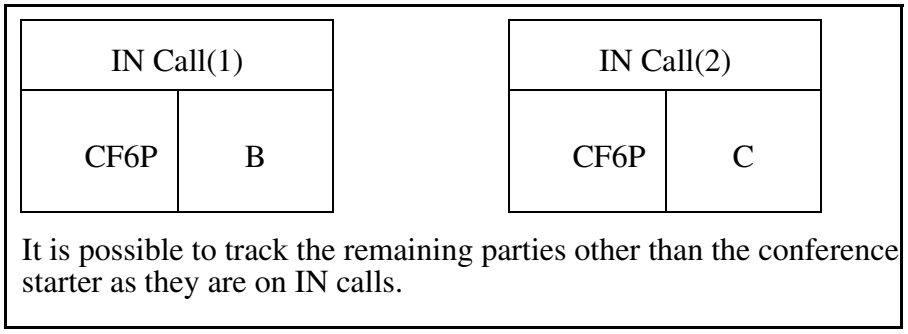
A activates CNF C06 which actually sets up the conference for all parties (i.e. C is included to the conference).



Now A, B and C are in conference but only B and C can be tracked as A is still on a basic call.

D, E and F can attend the conference in the same way.

If A on-hooks no indication is sent to SCP since A is on a basic call. The remaining parties stay in conference.



If B, C, D, E or F on-hooks a Disconnect ERB is reported for port 2.

Limitation / Restriction:

Since the party starting the conference resides on a basic call its state is not tracked correctly. The application servers see that the party invoked multiple calls but they do not understand that whether it on-hooked or not. However it is possible for application servers to understand whether other parties on-hooked or not. In scenarios where only 2 parties remain after the conference starter on-hooks, a Disconnect ERB is reported for port 1 for on-hooks of the remaining parties.

1.1.3.23 Console Queues

This is an MSAC related feature and IN interaction with MSAC is not supported.

1.1.3.24 Cut Through Dialling

This is an MSAC related feature and IN interaction with MSAC is not supported.

1.1.3.25 Date & Time

No impact.

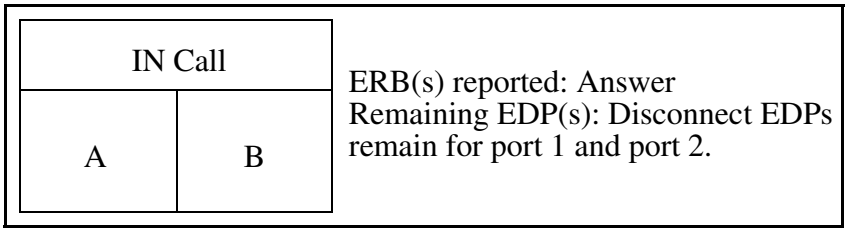
1.1.3.26 Direct (ICM)

Not supported. The architecture of this feature is very different and does not pass through normal translators or terminators and hence TDP-3 and TDP-12 triggering is not possible. For the description of this feature please see Appendix section at the end of this document.

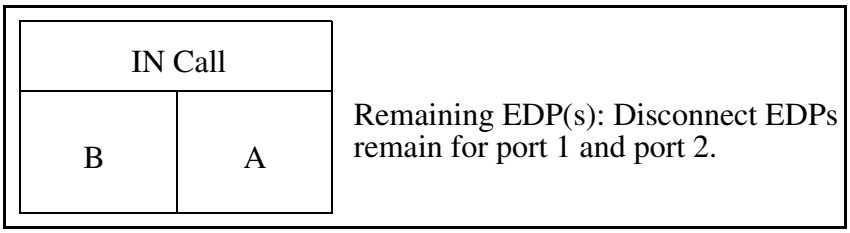
1.1.3.27 Direct Call Park (DCPK)

(a) The calling party activates DCPK.

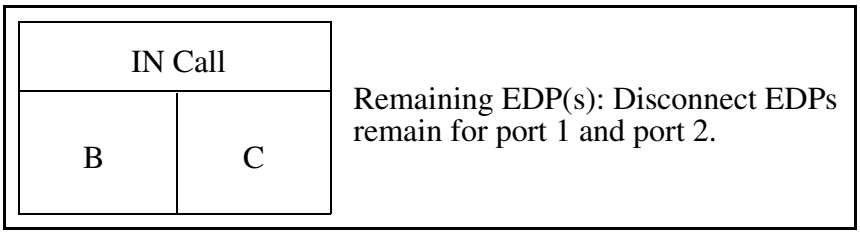
A and B are talking in an IN call as follows:



A activates DCPK and B is parked against C. The parkee is migrated to port 1 if it is not already on port 1 as follows.



C activates DCPK and retrieves B.

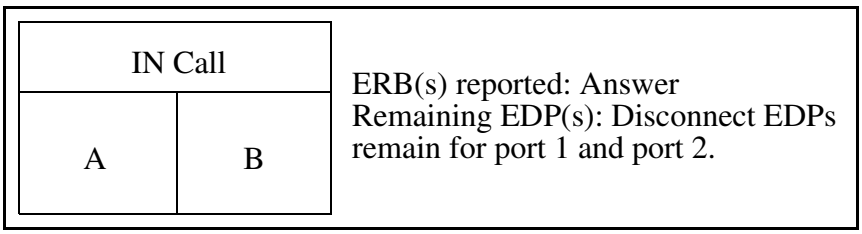


After this point if C on-hooks a Disconnect ERB is reported for port 2 and if B on-hooks a Disconnect ERB is reported for port 1.

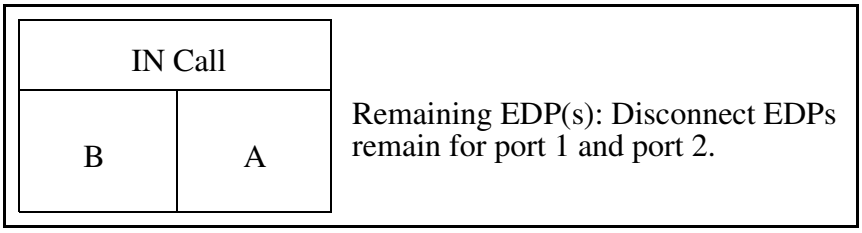
While parked if B on-hooks a Disconnect ERB is reported for port 1.

(b) The called party activates DCPK.

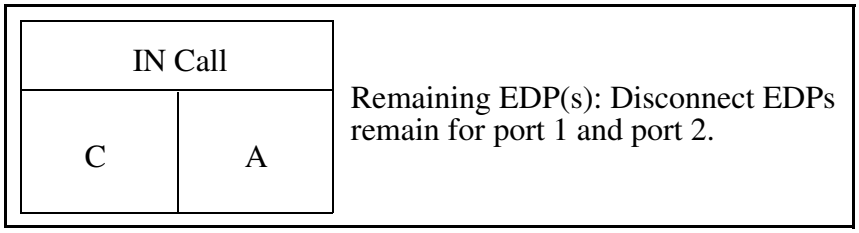
A and B are talking in an IN call as follows:



B activates DCPK and A is parked against C. The parkee is migrated to port 2 this time.



C activates DCPK and retrieves A.



After this point if A on-hooks a Disconnect ERB is reported for port 1 and if C on-hooks a Disconnect ERB is reported for port 2.

While parked if A on-hooks a Disconnect ERB is reported for port 1.

Limitation / Restriction:

SCP does not understand that C has replaced B.

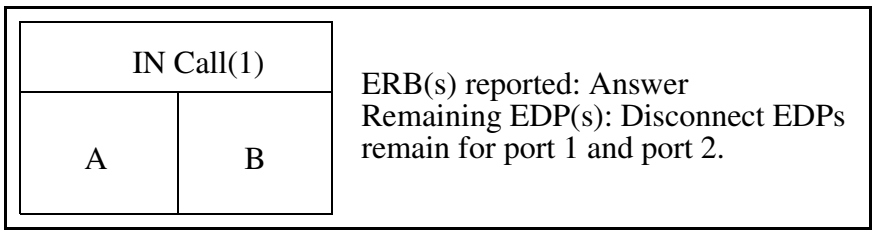
1.1.3.28 Direct Station Select/Busy Lamp Field (BLF)

For the description of this feature please see Appendix section at the end of this document.

This feature does not pass through normal translators and hence TDP-3 is not supported for BLF originated calls.

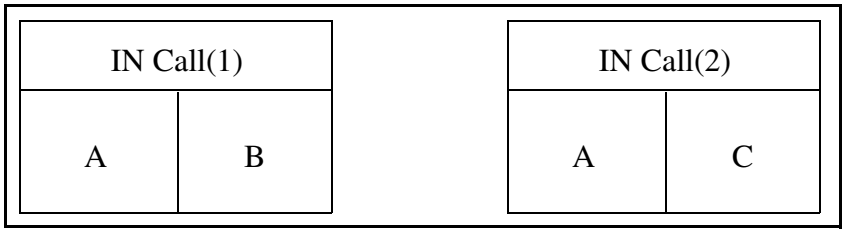
(a) BLF is used for call transfer.

A and B are talking in an IN call as follows:

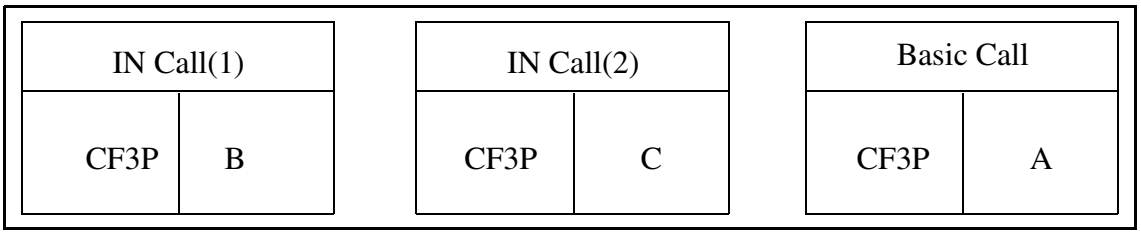


A has BLF for C and can see the status of C (i.e. when C is busy the lamp is on).

A hits Conf/Transfer key and then hits BLF key and C is dialled automatically. After this, it is similar to a CXR case.

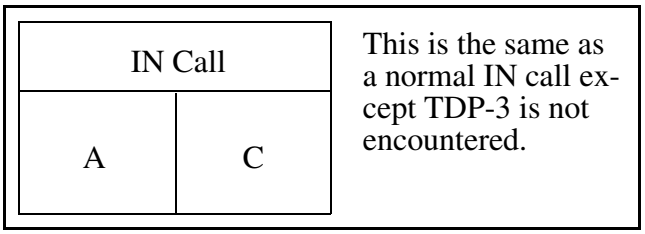


B hits Conf/Transfer key again.



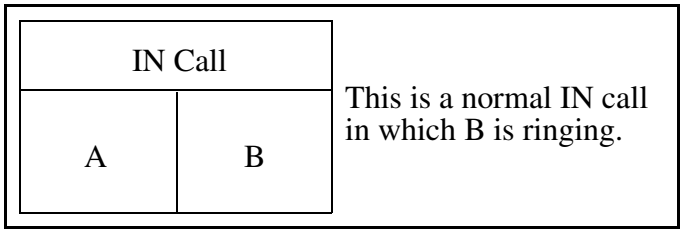
(b) BLF is used to for direct call.

A off-hooks and hits BLF key and C is dialled automatically.

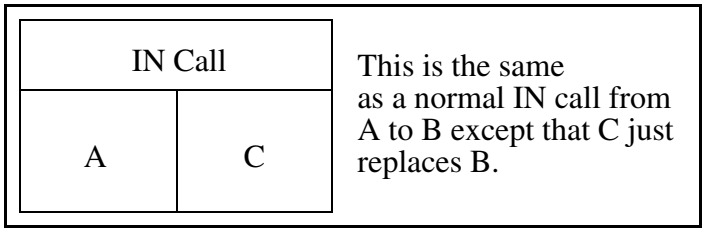


1.1.3.29 Directed Call Pickup (DCPU)

A dials B which results in the following IN call:



Before B answers and EDP-6 timer expires, C activates DCPU and an Answer ERB is reported.



After this point if A on-hooks a Disconnect ERB is reported for port 1 and if C on-hooks a Disconnect ERB is reported for port 2.

Limitation / Restriction:

SCP does not understand that C has replaced B.

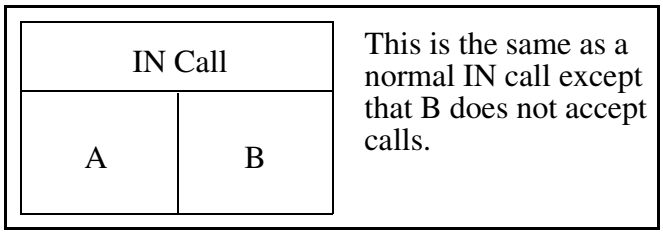
1.1.3.30 Display Queued Calls

No impact.

1.1.3.31 Do Not Disturb

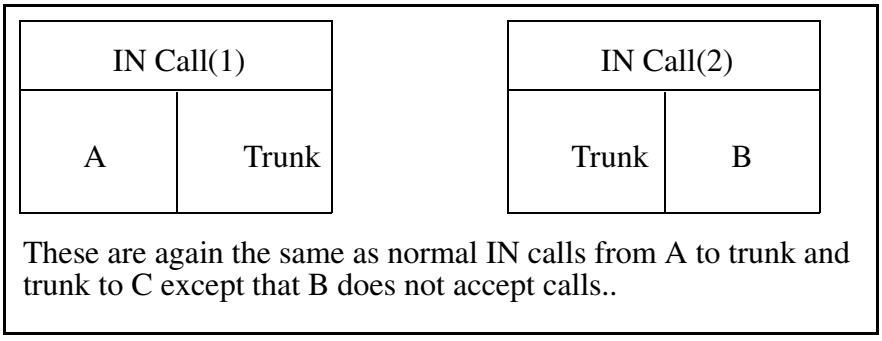
(a) Line to line call.

A dials B which results in the following IN call.



Call is not allowed to terminate and the IN dialog reports Busy ERB.

(b) Trunk to line call.



Call is not allowed to terminate and the second IN dialog reports Busy ERB. Also for the first IN dialog Busy ERB is reported to notify that the call has ended with the cause value privateNetworkServingRemoteUser.

1.1.3.32 Extend Calls

This is an MSAC related feature and IN interaction with MSAC is not supported.

1.1.3.33 Flexible Console Alerting

No impact.

1.1.3.34 Intercom Group (GIC)

Not supported. The architecture of this feature is very different and does not pass through normal translators or terminators and hence TDP-3 and TDP-12 triggering is not possible. For the description of this feature please see Appendix section at the end of this document.

1.1.3.35 Key Short Hunt (KSH)

For the description of this feature please see Appendix section at the end of this document.

A (key 1), B (key 2) and C (key 3) are keys of the business set and A and B are TDP-12 triggering datafilled. A is busy. D dials A which results in the following IN call.

IN Call		This is a normal IN call except Busy ERB is not reported. Next key in the hunt list will be tried.
D	A	

Busy ERB is not reported and B rings without TDP-12 triggering and when B answers Answer ERB is reported. After this point if D on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

IN Call		Next key in the hunt list which is not busy is terminated without any triggering. This is the same as a normal IN call from D to B.
D	B	

Limitation / Restriction:

SCP does not understand that C has replaced B.

1.1.3.36 Last Number Redial (LNR)

No impact.

1.1.3.37 Last Number Redial from Set (LNRA)

No impact.

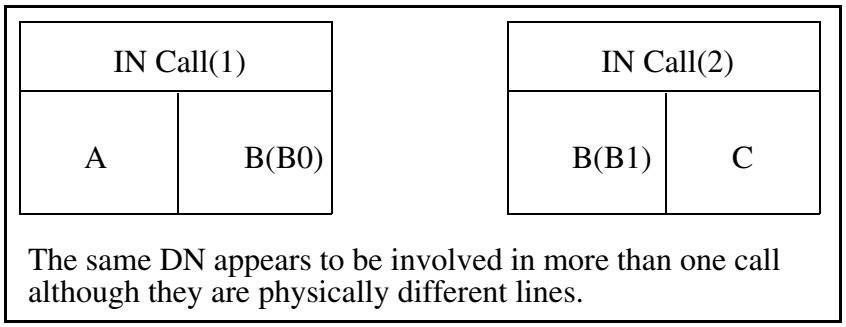
1.1.3.38 Multiple Appearance Of Directory Numbers (MDN)

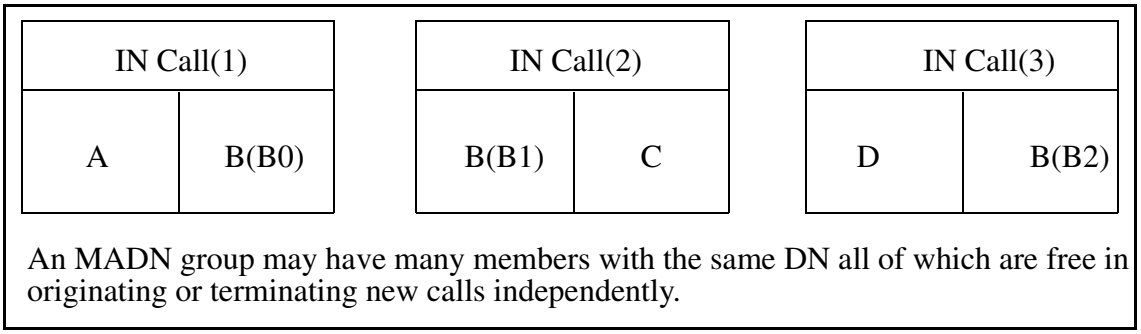
(a) SCA (Single Call Arrangement)

No impact.

(b) MCA (Multiple Call Arrangement)

All the MADN members have the same DN but when one of them is active others can also originate or can be terminated to as IN calls.

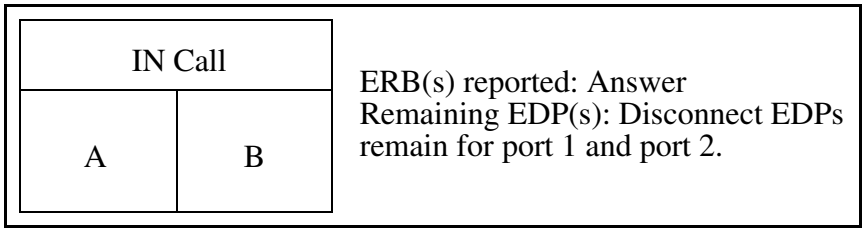




1.1.3.39 Music on Hold (KSMOH)

(a) The calling party activates KSMOH.

A and B are talking in an IN call as follows:

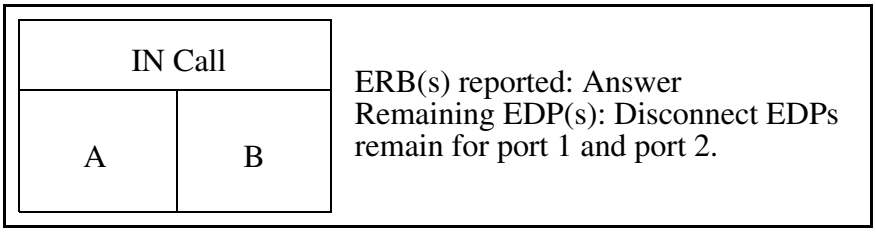


A activates KSMOH and B is on hold. A can retrieve B by pressing the DN key associated with the held call. After this point if A on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

While on hold if B on-hooks a Disconnect ERB is reported for port 2.

(b) The called party activates KSMOH.

A and B are talking in an IN call as follows:



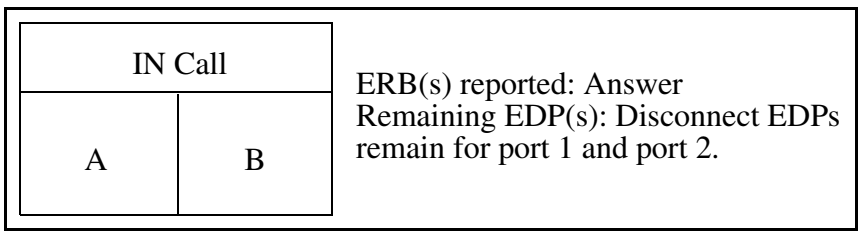
B activates KSMOH and A is on hold. B can retrieve A by pressing the DN key associated with the held call. After this point if A on-hooks a Disconnect ERB is reported for port 1 and if B on-hooks a Disconnect ERB is reported for port 2.

While on hold if A on-hooks a Disconnect ERB is reported for port 1.

1.1.3.40 Permanent Hold (HLD) Including Music on Hold

(a) The calling party activates HLD.

A and B are talking in an IN call as follows:



A activates HLD and on-hooks and B is on permanent hold. A off-hooks and retrieves B and after this point if B on-hooks a Disconnect ERB is reported for port 2 and if A on-hooks a Disconnect ERB is reported for port 1.

While on permanent hold if B on-hooks a Disconnect ERB is reported for port 1.

(b) The called party activates HLD.

A and B are talking in an IN call as follows:

IN Call		
A	B	ERB(s) reported: Answer Remaining EDP(s): Disconnect EDPs remain for port 1 and port 2.

B activates HLD and on-hooks and A is on permanent hold. B off-hooks and retrieves A and after this point if B on-hooks a Disconnect ERB is reported for port 2 and if A on-hooks a Disconnect ERB is reported for port 1.

While on permanent hold if A on-hooks a Disconnect ERB is reported for port 1.

1.1.3.41 Speed Call Long (SCL)

No impact.

1.1.3.42 Speed Call Short (SCS)

No impact.

1.1.3.43 Transfer, Hold & 3 way Conference (CXR)

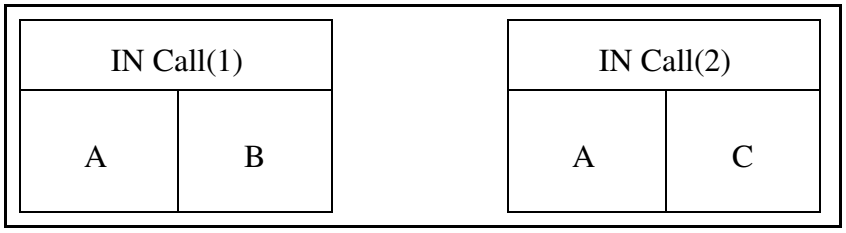
There are six scenarios as follows:

(a) Both the first call and the second call are IN calls and the calling party activates CXR.

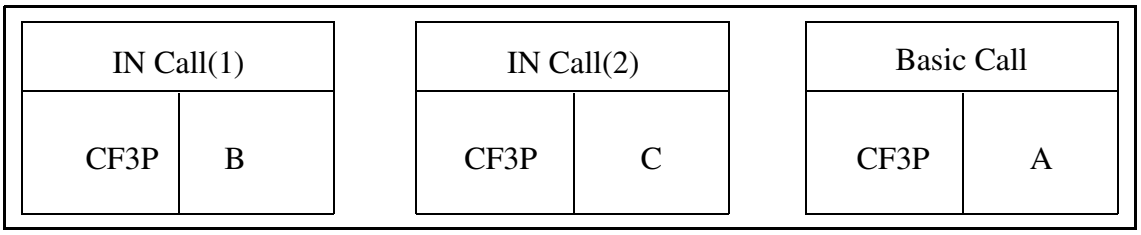
State 1

IN Call(1)		
A	B	ERB(s) reported: Answer Remaining EDP(s): Disconnect EDPs remain for port 1 and port 2.

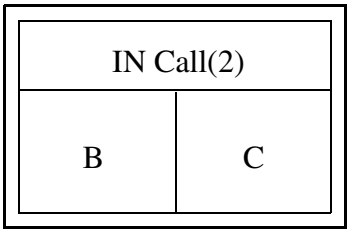
State 2



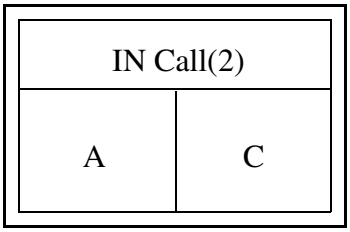
State 3



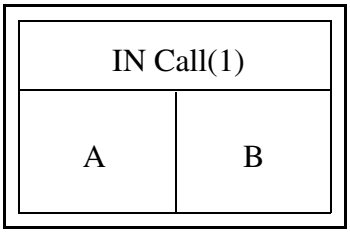
IN Call(1) -> EDP(9), EDP(17) for port 1: A on-hooked. Call was at State 2 or State 3.



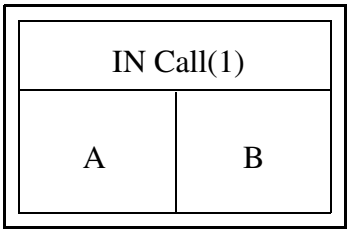
IN Call(1) -> EDP(9), EDP(17): B on-hooked. Call was at State 2 or State 3.



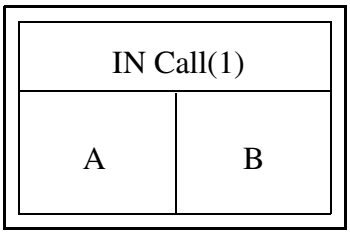
IN Call(2) -> EDP(4), EDP(5), EDP(6), EDP(13), EDP(14): Second call failed. Call was at State 2.



IN Call(2) -> EDP(9), EDP(17): C on-hooked. Call was at State 2 or State 3.

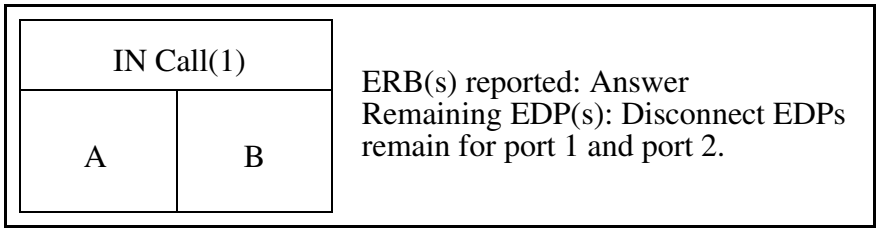


IN Call(2) -> EDP(9), EDP(17) for port 1: A flashed a second time during conference. Call was at State 3.

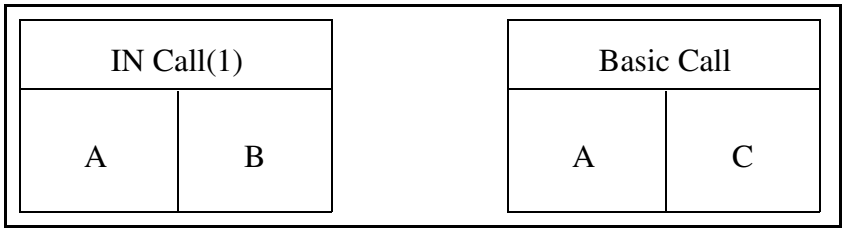


(b) The first call is an IN call, the second call is a basic call and the calling party activates CXR.

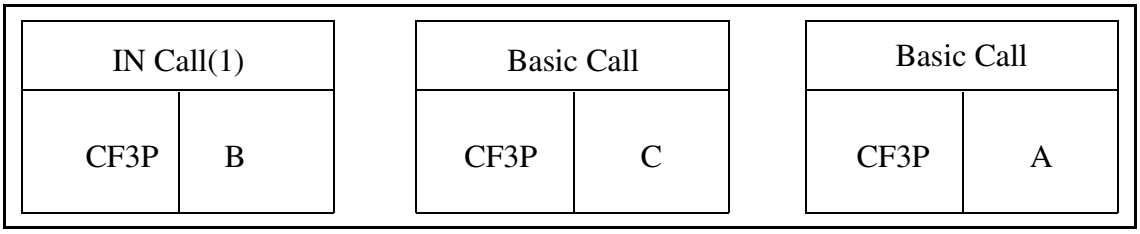
State 1



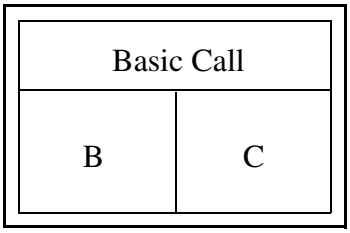
State 2



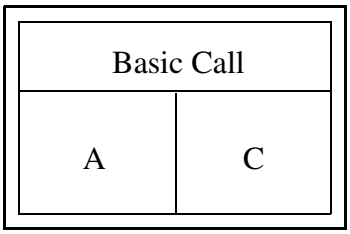
State 3



IN Call(1) -> EDP(9), EDP(17) for port 1: A on-hooked. Call was at State 2 or State 3.

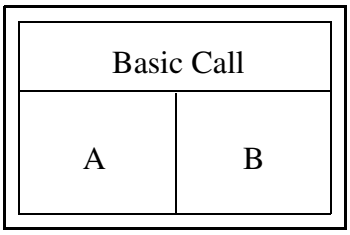


IN Call(1) -> EDP(9), EDP(17): B on-hooked. Call was at State 2 or State 3.

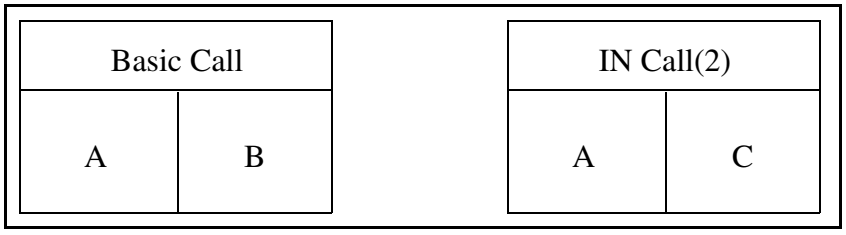


(c) The first call is a basic call, the second call is an IN call and the calling party activates CXR.

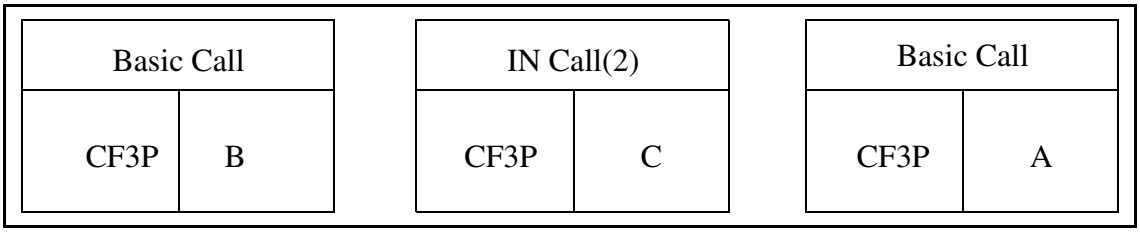
State 1



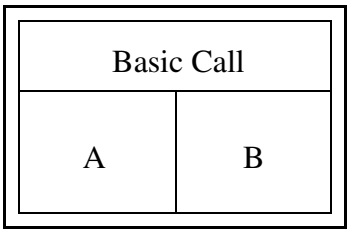
State 2



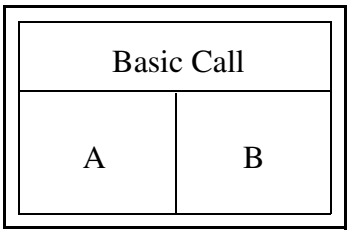
State 3



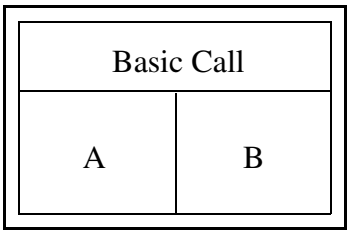
IN Call(2) -> EDP(4), EDP(5), EDP(6), EDP(13), EDP(14): Second call failed. Call was at State 2.



IN Call(2) -> EDP(9), EDP(17): C on-hooked. Call was at State 2 or State 3.

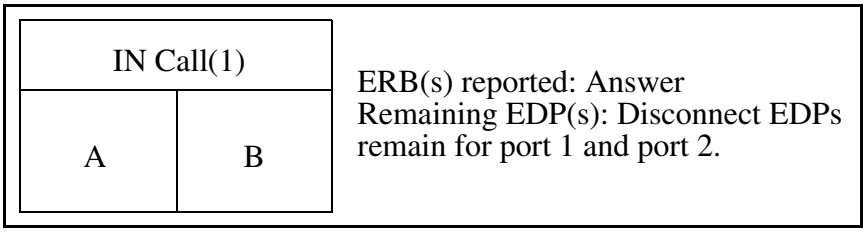


IN Call(2) -> EDP(9), EDP(17) for port 1: A flashed a second time during conference. Call was at State 3.

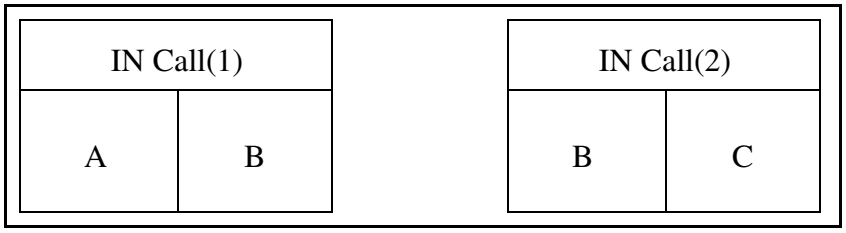


(d) Both the first call and the second call are IN calls and the called party activates CXR.

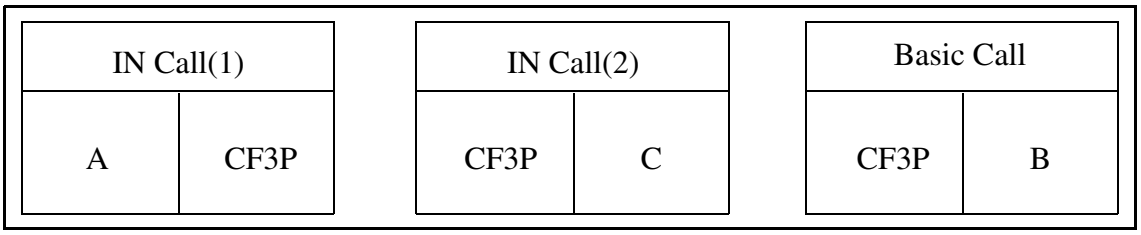
State 1



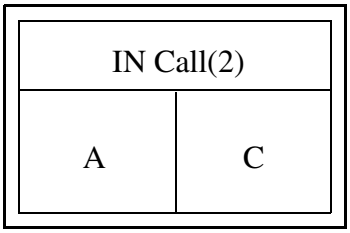
State 2



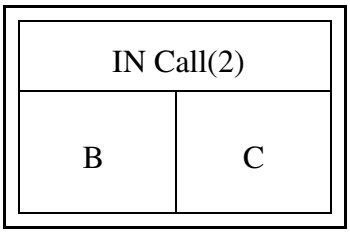
State 3



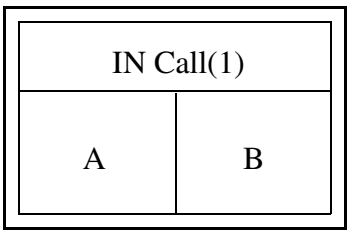
IN Call(1) -> EDP(9), EDP(17) for port 1: B on-hooked. Call was at State 2 or State 3.



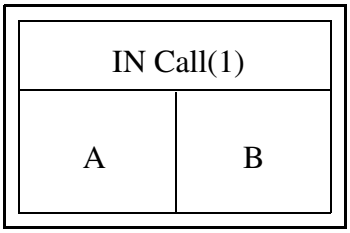
IN Call(1) -> EDP(9), EDP(17): A on-hooked. Call was at State 2 or State 3.



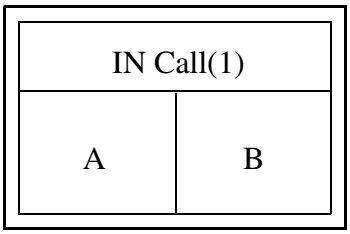
IN Call(2) -> EDP(4), EDP(5), EDP(6), EDP(13), EDP(14): Second call failed. Call was at State 2.



IN Call(2) -> EDP(9), EDP(17): C on-hooked. Call was at State 2 or State 3.

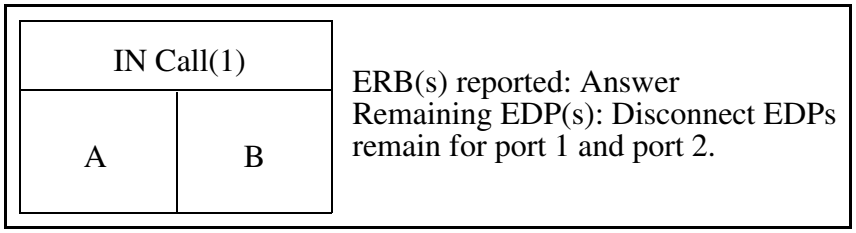


IN Call(2) -> EDP(9), EDP(17) for port 1: B flashed a second time during conference. Call was at State 3.

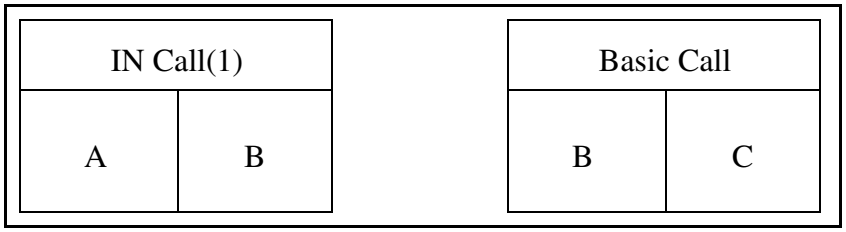


(e) The first call is an IN call, the second call is a basic call and the called party activates CXR.

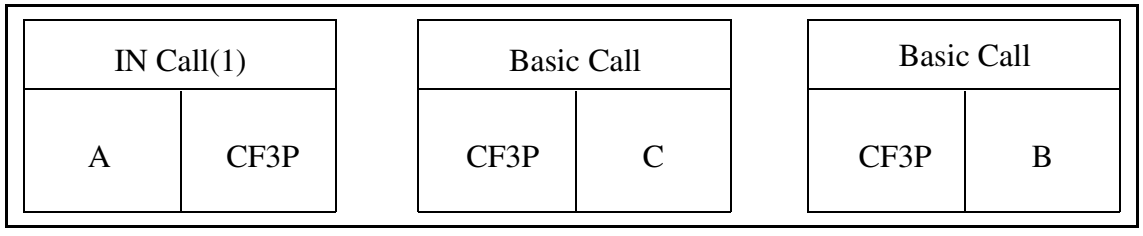
State 1



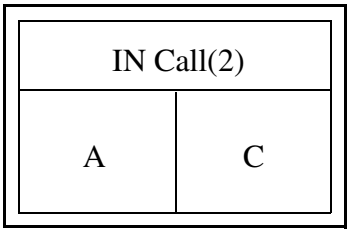
State 2



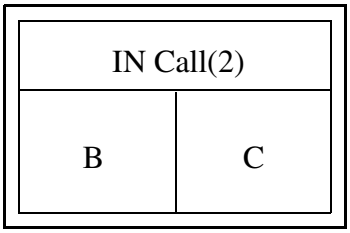
State 3



IN Call(1) -> EDP(9), EDP(17) for port 1: B on-hooked. Call was at State 2 or State 3.

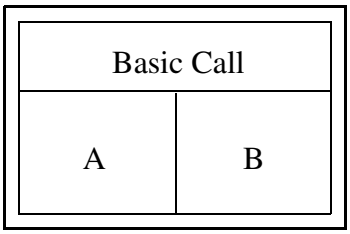


IN Call(1) -> EDP(9), EDP(17): A on-hooked. Call was at State 2 or State 3.

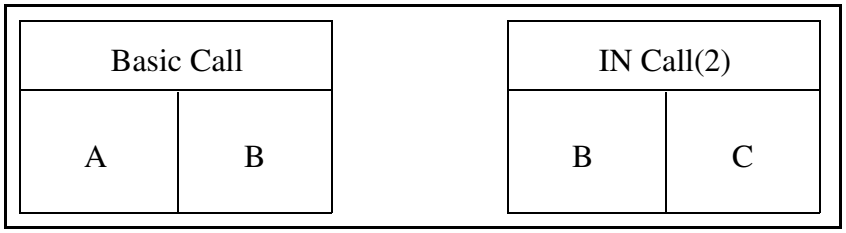


(f) The first call is a basic call, the second call is an IN call and the called party activates CXR.

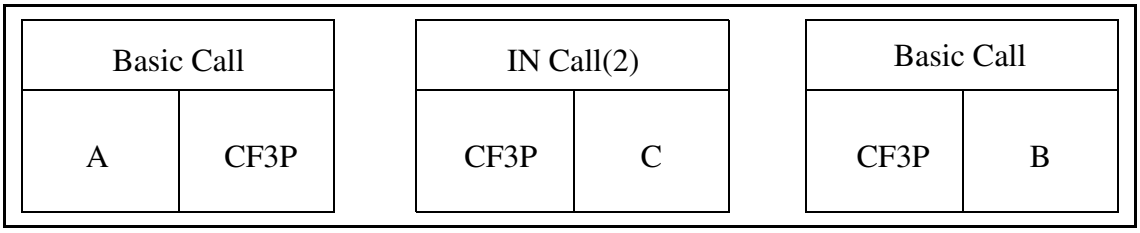
State 1



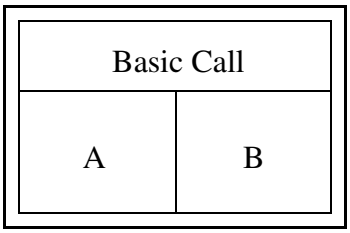
State 2



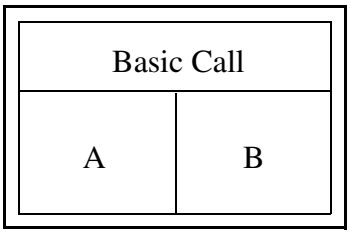
State 3



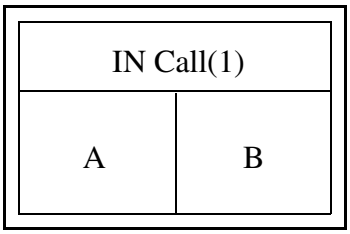
IN Call(2) -> EDP(4), EDP(5), EDP(6), EDP(13), EDP(14): Second call failed. Call was at State 2.



IN Call(2) -> EDP(9), EDP(17): C on-hooked. Call was at State 2 or State 3.



IN Call(2) -> EDP(9), EDP(17) for port 1: B flashed a second time during conference. Call was at State 3.



Limitation / Restriction:

In scenarios where there is only one IN dialog parties can not be tracked correctly.

1.1.4 Optionality

A new SERVINFO option CONV_DESK is defined which can be datafilled on a per-service basis. In order for the IN triggers to behave as described above this option should be datafilled.

1.2 Hardware Requirements or Dependencies

Not applicable.

1.3 Software Requirements or Dependencies

Not applicable.

1.4 Limitations and restrictions

Limitations and restrictions are specified for each feature.

As a general limitation / restriction:

- In scenarios where IN dialog is aborted multimedia session ends.
- Only Connect, Continue, EDP-4(N), EDP-5(N), EDP-6(N), EDP-7(N), EDP-9(N), EDP-10(N), EDP-13(R, N), EDP-14(R, N), EDP-15(N), EDP-17(N), EDP-18(N) should be used.
- IN specific billing (i.e. FCI operation, SERVINFO options) is not supported.

1.5 Interactions

This is already the subject of this document.

1.6 References/Recommended Reading

A00008464 - Terminating EDPs support.

1.7 Glossary

Term	Description
EDP	Event Detection Point
IN	Intelligent Networks
MSAC	Meridian Services Attendant Console

1.8 Appendix for A00008484

1.8.1 Call Forward Enhancements

The IBN Call Forward Enhancements allows for the addition of multiple Call Forwarding and personal call screening options to a customer group. These enhancements are for customer groups only. The system cannot assign these enhancements to separate lines.

This option can allow multiple Call Forwarding for other Call Forwarding features like CFU, CFI, CFB, CFD.

The personal call screening option allows the system to transfer forwarded calls back to a base station. The system forwards the calls even if Call Forwarding is active. This option can allow personal call screening for Call Forwarding features like CFU, CFI, CFB, and CFD.

Other options in this package also include customer group transparency, ring splash for CFI and denied call forwarding.

1.8.2 Direct (ICM)

The MBS Intercom allows an end user to press the Intercom (ICM) key to terminate on a selected Meridian business set (MBS).

If directory numbers (DN) are not active on the terminating MBS, audible ringing occurs and the ICM key of the terminator flashes. The terminator can press the ICM key to answer or wait 2 s. When the terminator waits 2 s, an automatic connection occurs.

If busy DNs are on the terminating MBS, a buzzing tone occurs. The system does not make an automatic connection. Press the ICM key to answer the call. The system places the active calls on automatic hold.

You can answer the intercom call on the loudspeaker or through the handset. The entry of both sets can occur to originate or answer an intercom call on the ICM key.

1.8.3 Direct Station Select/Busy Lamp Field (BLF)

Direct Station Select/Busy Lamp Field for MBS provides the following capabilities:

- Busy lamp field (BLF) enables a Meridian business set (MBS) end user to determine if a directory number (DN) is idle or busy by monitoring the state of the lamp next to the assigned feature key. This lamp is on when the DN is busy or off when the DN is idle.
- Direct station select (DSS) enables the end user of the monitoring set to press the specified feature key to dial the monitored DN directly.

Direct Station Selection/Busy Lamp Field for MBS can be used for direct calling or transferring calls, as described in the following paragraphs.

Direct calling by an MBS end user:

While calling a monitored DN, an MBS end user notes that the lamp light associated with the DN is not lit. He or she presses a DN key and then the BLF key associated with the DN.

Transferring calls:

The procedure to transfer a call or establish a three-way call using the BLF key is the same procedure as if the monitored DN was dialed directly.

1.8.4 Intercom Group (GIC)

The MBS Group Intercom (GIC) allows an end user to terminate on a member of a selected group using abbreviated dialing. An intercom group can have a maximum size of 10 members, 1000 members, or 10 000 members. End users in a 10 member group dial a single digit, 0 to 9, to reach others members in

their group. End users in a 100 member group dial a two digit number, 00 to 99. In a 1000 member group, end users dial a three digit code, 100 to 999. In a 10 000 member group, end users dial a four digit code, 0000 to 9999. A Meridian business set (MBS) can have members of several different GIC groups. A separate feature key must represent each group.

The DMS-100 switch accommodates a maximum of 4095 GIC groups. You can assign each GIC group to one large customer group. You can assign each GIC group to many customer groups.

1.8.5 Key Short Hunt (KSH)

This feature provides the capability for incoming calls to search a set of DN appearances on a business set for an idle DN to terminate.

KSH is a subset feature and must be assigned to key 1 if feature KSH is required. Either all DNs of the business set or a subset of DNs can be specified in the hunt list.

Hunting of an idle DN starts from the dialed DN, then goes up the keys of the business set as defined in the keylist. This hunt is not circular and stops once an idle DN is found or the hunt list following the dialed DN is exhausted. If the hunt list is exhausted without finding an idle DN, then an optional overflow DN or route is terminated.

The keylist can only contain standard DNs or multiple appearance DNs (MADN), but not intercom (ICM), group intercom (GIC), or private business line (PBL) DNs. A given DN cannot appear in more than one short hunt group or any other type of hunt group: multiline hunt (MLH), distributed line hunt (DLH), or directory number hunt (DNH). Any MADN member in the hunt keylist must be the primary member of that MADN group.

2: Configuration for A00008484

2.1 Hardware and Software Requirements

2.2 Initial Configuration

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

2.4 Upgrade Considerations

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
SERVINFO	CHANGED	UNCHANGED

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name: SERVINFO

Service Information Table

2.5.2.1.1 Functional description

It is not a new table.

2.5.2.1.2 Usage sequence and implications (CM Only)

Current datafill order unchanged.

2.5.2.1.3 Size

Unchanged.

2.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVINFO.

Table 2 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
FI	Changed		CONV_DESK option is added to the possible values.	When CONV_DESK is added to a tuple under FI then the corresponding IN triggers show converged desktop behavior as follows: IN can co-exist with line based DMS services as described in the FN along with some limitations and restrictions to the existing IN functionality.

2.5.2.1.5 Datafill example

The following example shows sample datafill for table SERVINFO.

Table 3 SERVINFO Sample Datafill

```
SERVIDX                                                    OPTION
-------------------------------------------------------------------------------
    19   (INITDP_PARMS ( SERVKEY) (CDPA) (CLI) (EVENT_TYPE) (OCN) (RDN)
         (RD_INFO) $)
         (FI (RETRIG_OPTION ALLOW GTE 1) (CONV_DESK ) $)$
```

2.5.2.1.6 Table release history update

IN can co-exist with line based DMS services as described in the FN along with some limitations and restrictions to the existing IN functionality.

2.5.2.1.7 Supplementary information

None.

2.5.2.1.8 Translation verification and other tools

The new option does not change the way SERVINFO and translation verification tools interact.

2.6 Service Orders (SO) (CM & SESM)

2.7 Software optionality control (SOC)

2.8 Element Management

2.9 User interface changes

2.10 OSSGate Interface Changes

2.11 Security

2.12 Configuration Walkthrough

Product = World Trade

A00008556--SIP Lines Core OAMP Support

Functional Description

1: Applicable Solution(s)

Int'l CHS

1.1 Description

The provisioning of DPL agents affects three major network components, the CS2K core, GWC, and CS2K Session Server(CS2KSS). Each of these components have their own specific provisioning requirements and each are provisioned via the appropriate application within SESM. The relationships between these components and SESM are shown in Figure 1 DPL Provisioning Component Overview below.

As part of this overview, the basic steps required to provision DPLs across the different components is included below. These steps are included here for context and intended only as a guide.

- Install the CS2KSS and activate DPL lines application CS2KSS.
- Configure commissioning data on CS2KSS using CS2KSS EM.
- Use SESM Provisioning GUI to “ADD GWC NODE” with the following details.
  - — Select the GWC profile ‘DPL’ signifying the GWC supporting DPL agents.
  - — Select Term type of DPL_TERM.
  - — Select Exec Data of DPLEX.
  - — The CM interface will subsequently add the GWC to table SERVRINV with DPLEX exec lineup and DPL_TERM term_type.
  - — Table SERVRINV ADD tuple will subsequently cause a static data download of DPLEX execs to the GWC.
  - — The GWC Configuration Manager will configure the GWC as a ‘DPL’ type GWC with DPLSupported GCM parameter set to TRUE.
- Use SESM Provisioning GUI to “ASSOCIATE Media Gateway”, the CS2KSS GW.
  - — Enter GW name, GW IP, and GWC to host GW.
  - — Select Gateway Profile Name of CS2KSS.
  - — Enter number of Reserved Terminations in multiples of 1023 up to a maximum value of 6138.
  - — Select the Gateway SITE name as previously provisioned in table SITE in the CS2K Core, and which must be unique for each CS2KSS GW added.
  - — Signalling protocol type will default to GCP.
  - — Enter protocol port and version.
  - — The CS2KSS EM proxy in SESM proxies this GW data to the CS2KSS which uses this data to identify new CS2KSS instances and provisions DPL agent data as required.

— The CM interface in SESM will cause provisioning to occur in the CS2K core table LGRPINV and table LNINV. An LGRP will be created for each increment of 1023 reserved terminations. 1023 tuples will be added to table LNINV for each LGRP added in LGRPINV.

— When the DPL line tuples are added to LNINV, static data is downloaded to the GWC for each terminal including the term type of DPL per TID.

— The GWC EM in SESM will cause the CS2KSS gateway to be registered as a 'D' type GW in the GWC with an CS2KSS lines profile name and a protocol of GCP.

— The GWC EM in SESM will cause the addition of endpoint groups for each 1023 endpoints on the CS2KSS GW in the GWC.

— The GWNAME will consist of up to 32 chars.

— The EPids added will have the format of SITE_Name/<0-511></0-9>/<0000-1022> E.g SIPVMG1.tampa.vz.com TMP1/000/2/0478

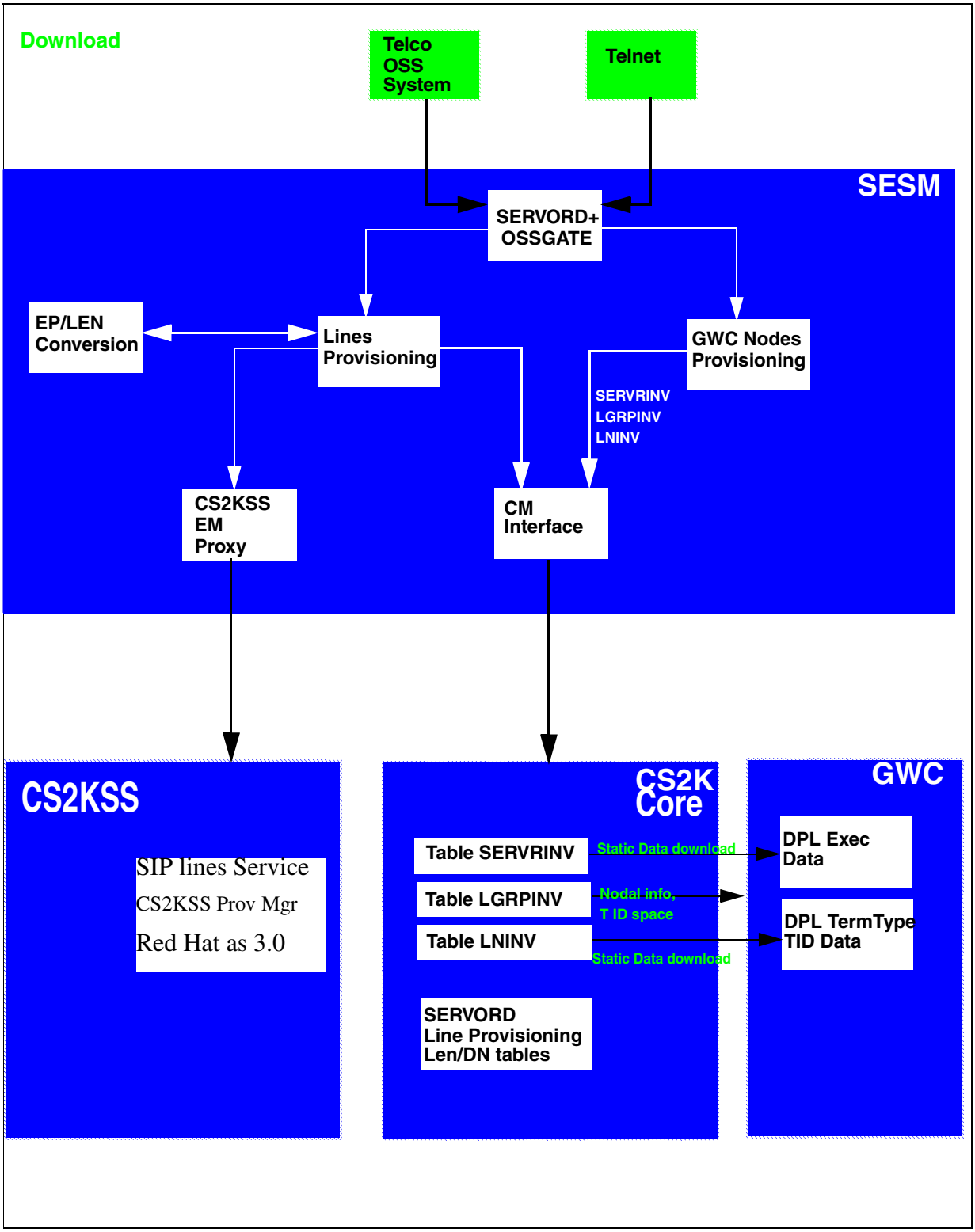
- Use Telco OSS or Telnet to perform SERVORD+ line provisioning via SESM.

— CS2KSS EM within SESM will proxy CS2KSS to provision user data in CS2KSS system.

— CM Interface within SESM will proxy the CS2K core to perform Servord line provisioning.

— Either LEN format or Gateway name and EPid combination will be accepted.

Figure 1 DPL Provisioning Component Overview



This activity focuses on the CORE OAMP (Operation, Administration, Maintenance & Provisioning) portion of the overall SIP feature. The components in this activity are as follows:

- GWC Provisioning.
- CS2KSS-GWC Association.
- DPL Lines Provisioning.
- Journal File.
- NCAS Link Provisioning.
- Core Maintenance support.
- Tool support
- SOC support (Refer the CN section).
- NCAS Link Logs (Refer the FM section).

1.1.1 GWC provisioning:

The GWC is commissioned through the SESM. The core stores information about this commissioned GWC in the table SERVRINV. The SIP feature deals with supporting new type of agent called dynamic packet line on the GWC.

- A new term_type DPL_TERM and a new exec_lineup called DPLEX are defined for supporting the DPL agents on the GWC. The new definitions DPL_TERM and DPLEX are passed onto the core along with the GWC information when the GWC is commissioned.
- On the core side, the table SERVRINV is enhanced so that it can accept these new definitions. When the GWC is commissioned, a tuple similar to the below one is expected to be datafilled in the table SERVRINV automatically:

Table SERVRINV:

SRVRNAME SRVRADDR **SRVREXEC** SRVRTONE BEARNETS SRVROPTS
GWC 0 IP 45 46 47 48 **(DPL_TERM DPLEX)**$ NORTHAA (NET_IP Y)$ $

This table is supposed to be provisioned via SESM and not manually. The field in bold is updated to support a new entry DPL_TERM DPLEX.

1.1.2 CS2KSS-GWC Association:

Currently, a gateway controller can be associated with a maximum of 6 gateways (LGRP nodes) in CS2KSS. After the GWC is commissioned, a logical association is created in the core between the GWC and the gateways in the CS2KSS.

- The table LGRPINV stores the information about the LGRP node and the GWC which it is associated with. After the GWC information is provisioned in the table SERVRINV, the LGRP node information for corresponding LGRP nodes are datafilled in the table LGRPINV. The table LGRPINV is enhanced so that a new lgrp_type 'SSDPL' is supported. This new lgrp_type signifies that this LGRP node is associated with DPL lines.

- Currently, each LGRP node can support 1023 lines and this size will not change as a part of this feature. The information on these lines for each of the LGRP node is stored in the table LNINV. Table LNINV does not require any enhancements to support this functionality.

- A tuple with following structure is expected after the table LGRPINV is provisioned:

Table LGRPINV:

LGRP_NO SRVR_NAME **GRPTYPE** LGRPOPTS
LG 1 1 GWC 5 **SSDPL** $

This table will be provisioned via SESM and is not supposed to be datafilled manually. As shown above, a new lgrp_type 'SSDPL' is supported now for table LGRPINV.

When 1 LGRP is provisioned, corresponding 1023 lines subtending from that lgrp will be datafilled in table LNINV. As a part of this feature, the table LNINV is enhanced so that it can support only RDTLSG (North American market) and GWLPOT (International Market) cardcode for SSDPL lgrp_type. Also, the restriction has been applied to the cardcodes valid for the other lgrp_types. A sample tuple:

Table LNINV:
LEN CARDCODE PADGRP STATUS GND BNV MNO CARDINFO CS2KSS 1 1 10 13 RDTLSG PKLNL HASU N NL Y NIL

As a part of this feature the following valid cardcodes apply for different lgrp_types:

LGRP_TYPE	List of Valid Cardcodes
SSDPL	RDTLSG, GWLPOT
S	RDTLSG, RDTCON, GWLPOT, RDTEBS,GWLEBS

LGRP_TYPE	List of Valid Cardcodes
M	RDTEBS, GWLEBS
C	RDTLSG, RDTCON, GWLPOT
LL_3RDPTY	RDTLSG, RDTCON, GWLPOT, RDTEBS, GWLEBS
CALIX_C7	RDTLSG, RDTCON, GWLPOT, RDTEBS, GWLEBS

The table LNINV will be provisioned via SESM and is not supposed to be datafilled manually.

1.1.3 DPL Lines Provisioning:

The DPL line is differentiated from other lines by adding DPL option on that line. The table IBNFEAT is enhanced to support a new data_feature DPL. The DPL option can be added only to IBN/RES lines. Also, SERVORD+ is enhanced for accepting new DPL related options and should be used for datafilling the DPL option.

1.1.3.1 The new DPL option

As a part of supporting new DPL option, table IBNFEAT, LCCOPT and OPTOPT are enhanced.

- The table IBNFEAT have been enhanced to support the DPL data_feature. The DPL line option will have a SIP sub option. The SIP sub option of DPL will itself have a sub option of MAX_NUM_CALLS(10).
- The table control editor commands, ADD,DEL and CHA are disabled for the DPL option in table IBNFEAT much in the same manner of the PDO option.

Table IBNFEAT:

LEN DNNO DF FEATURE DATA
LG 01 1 00 14 0 **DPL DPL Y 10**

This table will be provisioned via SESM.

- DPL option can only be added via Servord and not Table Control.
- The options incompatible with the DPL option can be datafilled in the table OPTOPT. A sample tuple:

Table OPTOPT:

DPL (BC) (CSDO) (EOF) (FIG) (FTS) (LDTPSAP) (LNPTST) (MAN) (MPB) (NDC) (NOH) (VOWDN) $

You can add options in this tuple which you want to make incompatible with option DPL. This is just a sample tuple. To see the list of supported options with DPL, please refer the interactions section of FN.

- The LCC's supporting the DPL option can be modified through the table LCCOPT. Currently, only IBN and RES lines support the DPL option. Sample tuples are as below for IBN and RES LCC's.

Table LCCOPT:

RES (ACB) (ACRJ) (ADSI) (ADSL) (AIN) (AINDENY) (AINDN) (AMATEST) (AMSG) **(DPL)**

IBN (ACB) (ACD) (ACDNR) (ACRJ) (ADSI) (AIN) (AINDN) (ALI) (AMATEST) (AMSG) **(DPL)**

1.1.3.2 SERVORD+ Enhancements:

SERVORD+ Enhancements have been made so that it will now accept three new options related to SIP lines provisioning: DPL, SIP_PASSWORD and SIP_DATA. DPL will be seen in the core whereas the options SIP_PASSWORD and SIP_DATA will be send to the CS2KSS.

- When provisioning a SIP line all three of the options described above must be present in the SERVORD+ NEW command.
- The above options can not be added later via ADO.
- ADO and DEO of options that are compatible with DPL will be permitted. But ADO/DEO can not be used with the DPL line option.
- Only NEW, OUT and CHF will support the DPL line option. It is possible to add a DPL compatible option that does not require the DPL option in the command (such as ADO PIC). CHF can be used to manipulate the MAX_NUM_CALLS value subfield of the DPL option. The line must not be in the CPB or call processing busy state or the change will be rejected. CHG can be used to change all but the LCC (line class code).
- DGT option is required. It will be automatically added if not present.
- Long SERVORD+ commands are supported by allowing commands to be continued on a second line by using a + sign.
- The SIP URI change will be reflected in the CS2KSS and not in the core.
- E.g. of the SERVORD+ command:

Servord+ NEW Command:

NEW $ 6212500 IBN BNR 0 0 613 NILLATA 0 LG 000 0 10 13 DPL Y 3 SIP_PASSWORD xx SIP_DATA bobby mb1

1.1.3.3 Journal File:

The Journal File (JF) subarea provides a facility for preserving Data Modification Orders (DMO) on tape so that data tables can be restored if the switch should fail. The Journal File is an optional feature of the DMS switch which preserves DMO on magnetic tape. If a switch failure occurs that requires a reload, this magnetic tape is loaded back into the machine and switch data is restored to its condition at the time of switch failure.

1.1.4 NCAS Link Provisioning:

The core communicates directly with the CS2KSS Provisioning Server through NCAS links. The CS2KSS Provisioning Server can return both static and dynamic call data stored in CS2KSS back to the core via the NCAS link

The NCAS link is going to be an instance of SCTP. The table IPAPPL provides SCTP instance for various connections in DMS. This table is enhanced to support a new application called SIPMTC (just like AIN, SMDI etc). The core can now communicate with CS2KSSs using this SCTP instance.

Table IPAPPL:

InstKey InstName Transport IPDevice IPaddrs port optlist
1 a sctp hiop 198 202 188 221 4982 (application **sipmtc**)
(setprime 1)

The NCAS link association is going to be used for the new QSIP command.

The SIPMTC application is supported over HIOP only.

The multihoming functionality is not supported in SIPMTC application.

The port number allocated for SIPMTC application is 4982.

Multiple instances for SIPMTC are not allowed i.e. in table IPAPPL, there can be only one instance datafilled for SIPMTC.

1.1.5 Core Maintenance Activities:

On the core side, maintenance actions can be performed on the DPL lines. The maintenance operations will keep the core, gwc and cs2kss informed about each other's activities.

1.1.5.1 MAP Commands and Line State Propagation:

The DPL line can be posted on mapci; lns; ltp level.

- The line states for DPL lines on the Core include: IDL, LMB, MB, INB, CPB, CPD, SB. After the line is posted, operations like BSY, RTS, FRLS, HOLD, NEXT can be performed on the posted line. When these operations are performed, the state change of the lines is propagated to the GWC which in turn notifies CS2KSS.
- There are plans to support DIAG in the second phase of this feature, but they will not be supported in the current release. When DIAG is run on the core side, a message will be displayed: “This command is not valid for posted line.”.
- At the map level, the base DPL tid will be posted. If there is any call active, then the information posted for base DPL tid will depend upon the number of call appearances active. If there is only call appearance active, then the linking information for that call appearance will be posted. However, for more than one call appearance, the linking information will not be displayed for all the call appearances. The maintenance operations on specific call appearances will be supported in later release.
- The DPL line can be posted at all the sub-levels of the LTP level: LTPLTA, IBNCON, LTPMAN, LTPDATA, LTPISDN, DCTLTP, DTPLTP. But no maintenance operations can be performed on posted DPL lines at any of these sub-levels.
- For the BSY command, the CS2KSS will be notified that this DPL client is not available for call processing. If there are no call appearances active, then the base TID will be put into MB state and no calls can be associated with this DPL agent. If there are any call appearances active, then the base TID will be put into CPD state. When all the calls are taken down, the base dpl TID will move from CPD to MB state. New calls cannot be originated/terminated on the DPL line that has been busied. The line has to be RTSed back for new calls to be originated/terminated.
- A FRLS on a DPL agent will clear all active calls for the line. If there are no active calls then the base TID, then the tid will be put to MB state. If there are active calls, a FRLS will terminate all the sessions. However, FRLS on a particular session will be supported in a later release.
- On RTS operation, the line will be put into IDL state. This operation cannot be performed when the calls are active on a DPL line.
- The maintenance operations BSY/RTS/FRLS at the MAP level are applicable for all the multiple call appearances. The Mtc operations are applied to all the VIDs.
- The HOLD command puts the posted DPL line in the hold position.
- The NEXT command moves the line in a specified HOLD position to the control position, or replaces the line in the control position with the line in a

specified hold position. The NEXT command does not list the next provisioned DPL VID.

- The LGRP node can be posted at the PM level but maintenance operations cannot be performed on the entire LGRP. Thus, the state changes because of maintenance operations are propagated upwards to the core through the GWC.

Note: The maintenance operations are not supported for the SSDPL lgrp.

- When the BSY LGRP command is given for the SSDPL lgrp, the following error message is displayed:

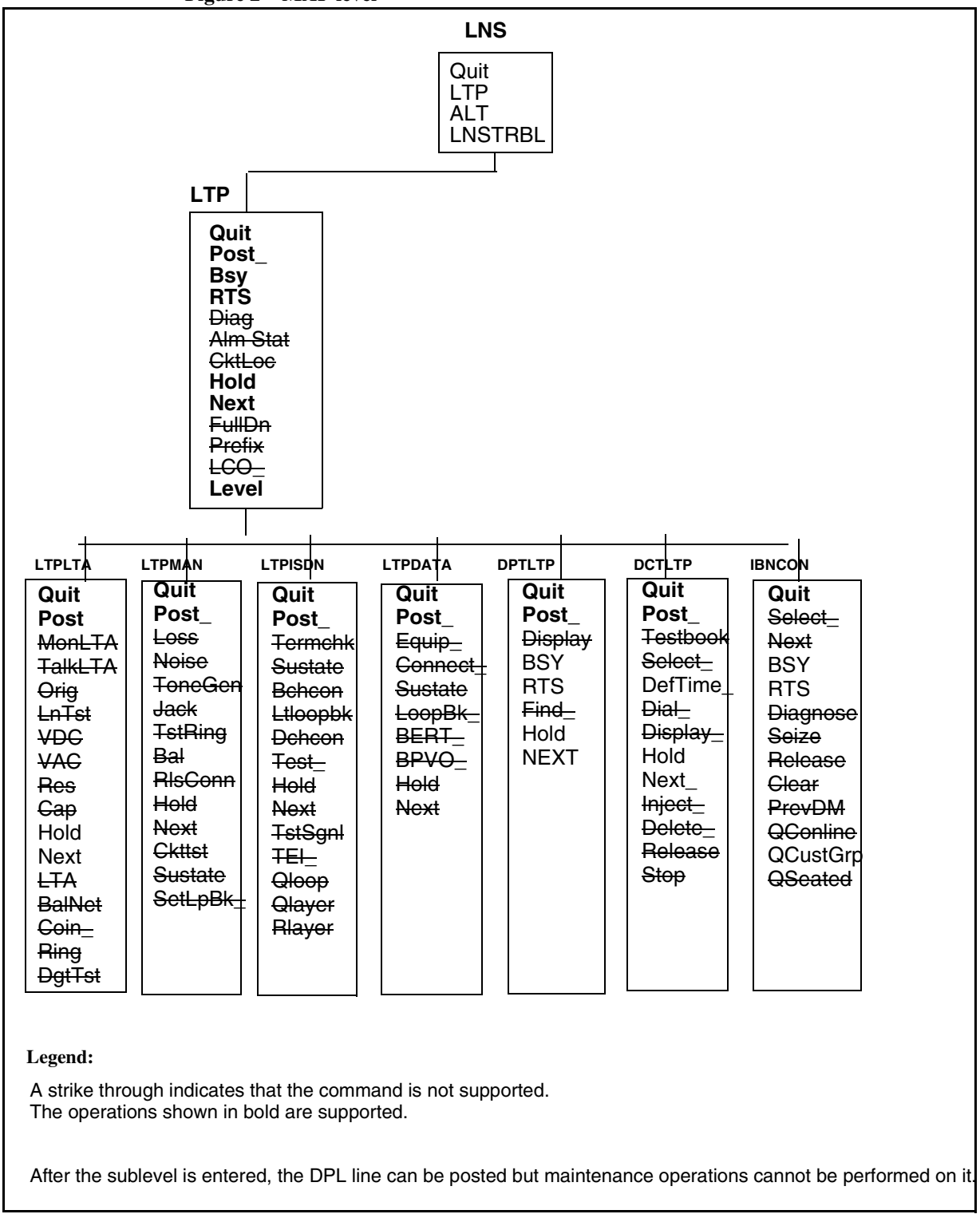
BSY COMMAND IS NOT SUPPORTED FOR THIS TYPE OF LGRP NODE.

- When the RTS command is given for the SSDPL lgrp, the following error message is given:

RTS CAN ONLY GO FROM MANB STATE.

Figure 2 Map Level below shows the MAP levels and operations which are supported and blocked for DPL lines.

Figure 2 MAP level



Legend:

A strike through indicates that the command is not supported.
The operations shown in bold are supported.

After the sublevel is entered, the DPL line can be posted but maintenance operations cannot be performed on it.

At the **LTPLTA** level, the error messages that will be seen for the unsupported maintenance commands are:

MonLTA, TalkLTA, Orig, LnTst, VDC, VAC: **This command is not valid for posted line.**
BalNet: **This command is not valid for Call Server LGRP lines.**
Coin, Ring, DgtTst: **No talk connection to posted line**

At the **LTPMAN** level, the error messages that will be seen for the unsupported maintenance commands are:

Loss, Noise, Tonegen, Jack, RlsConn: **This command is not valid for the posted line.**
Tstring: **To test the ringing function for Call Server LGRP lines, please run the DIAG command.**
Bal: **This command is not valid for Call Server LGRP lines.**
Ckttst: **CKTTST command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
SetLpBk_: **SETLPBK command is not valid on POTS/COIN lines.**

At the **LTPISDN** level, the error messages that will be seen for the unsupported maintenance commands are:

TERMCHK: **TERMCHK command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
BchCon: **BCHCON command is not valid on POTS/COIN lines.**
LTLOOPBK: **LTLOOPBK command is not valid on POTS/COIN lines.**
DCHCON: **DCHCON command is not valid on POTS/COIN lines.**
TEST: **TEST command is not valid on POTS/COIN lines.**
TSTSGNL: **TSTSGNL command is not valid on POTS/COIN lines.**
TEI: **TEI command is not valid on POTS/COIN lines.**
QLOOP: **QLOOP command is not valid on POTS/COIN lines.**
QLAYER: **QLAYER command is not valid on POTS/COIN lines.**
RLAYER: **RLAYER command is not valid on POTS/COIN lines.**

At the **LTPDATA** level,

Equip, Loopbk_, BERT_, : **This command is not valid for Call Server LGRP lines.**
Connect: **CONNECT command is not valid on POTS/COIN lines.**
Sustate: **SUSTATE command is not valid on POTS/COIN lines.**
BPVO: **BPVO command is not valid on POTS/COIN lines.**

At the **DPTLTP** level,

Find_ : **CLLI entered is not of a DPT trunk**
Display: **DN not involved in a call**

At the **DCTLTP** level,

Testbook: **No testbook is active.**
Select: **SELECT command not executed. No testbook is active.**
Dial: **DIAL command not executed. No testbook is active.**
Display: **DISPLAY command not executed. No testbook is active.**
Inject: **INJECT command not executed. No testbook is active.**
Delete: **DELETE command not executed. No testbook is active.**
Release: **RELEASE command not executed. No testbook is active.**
Stop: **STOP command not executed. No testbook is active.**

At the **IBNCON** level,

Select: **That line is not associated with a console.**
Next, Diagnose, Seize, Release, Clear, PrevDm, Qconline, Qseated: **Console not selected.**

1.1.5.2 Restart and Swact Recovery:

It is desired that when Core, GWC and CS2KSS undergo restart/swact, each of the component's view of line states are in sync.

When the core undergoes restart/swact it notifies the GWC about the type of restart/swact. The GWC performs the necessary operations and also notifies the CS2KSS regarding this. The heartbeat mechanism is used to notify each other of their availability.

When the core undergoes restarts/swacts, a message is sent to GWC about the type of restart/swact. The GWC has to take action upon the type of restart/swact that occurred.

Core Recovery:
The stable calls are the ones in the talking state. The unstable calls imply the ones not in the talking state.

- For core warm restart, GWC clears all unstable calls.
- For core cold restart, GWC clear all stable and unstable calls.
- For core warm SWACT, GWC clear unstable calls.
- For core cold SWACT, GWC clears all stable and unstable calls.
- For core reload restart, BSY GWC Node. When core recovers, RTS the GWC node.
- After the core restart is completed, a message is sent to the GWC that the core is in 'Running' state. If the GWC was BSYed, it will be RTSed. The core sends a SST320 message to RTS all the lines of an LGRP.

- If the CS2KSS is OOS before the restart, lines are put into LMB state. The availability of CS2KSS is tracked by the GWC by the heartbeat mechanism.
- Even if the line was manually BSYed before restart, the line is RTSed to IDL state after restart is over.
- When the core recovers, the endpoints appear as SB until the recovery process is complete, then they transition to IDL. However, the transition state SB cannot be tracked because by the time core recovers completely and we can post the line at the mapci level, the line would have been RTSed to IDL state.

GWC Recovery:

- When the GWC is busy, the state of the GWC in the core side will be ManB. If the GWC is OOS, the state of the GWC in the core would be SysB. When the GWC is not InSv, the LGRP will be in SysB state.
- When GWC goes down, a message is sent to the core to put the line in LMB state.
- When GWC recovers, message is sent to the core to put the line into IDL state. But since the connection between the GWC and CS2KSS is lost, the lines will be put into LMB state. When the discovery message from CS2KSS to GWC is sent, the lines of the corresponding lgrp are out into IDL state.

CS2KSS Recovery:

The maintenance operations are not supported on CS2KSS in this release. The line states are dependent upon whether CS2KSS is up or not.

- CS2KSS gateway is not provisioned on the GWC side.
  If the gateway is not provisioned on the GWC side, the lgrp state is SYSB the lines will be in INB state.

- CS2KSS gateway is provisioned but the gateway is OOS
  When the gateway is OOS, the lgrp is in SYSB state and the lines are in the LMB state. Only when the DISCOVERY message is sent to the GWC from the CS2KSS, the lines are put to IDL state.

1.1.6 Tools:

1.1.6.1 QSIP:

QSIP is a new query command at the CI level. It has been introduced as a part of this activity. QSIP would query the SIP Line data for a particular SIP Line.

The QSIP command will display the following information:

- SIP URI

- Registration State
- Allow Post Busy Termination
- Number of Contacts
- Contacts
- Service Package
- Services
- Endpt ID
- Virtual Media Gateway
- Middle Box ID List
- Client Type
- Static Client
- Node number and Terminal number of the VIDs of all the Active Call Appearances
- Number of Active Sessions in CS2000 Session Server

The QSIP command will launch a Query message to the CS2000 Session Server over the NCAS link. The CS2000 Session Server will launch a Response to the Core over the NCAS link. Upon receiving the Response from the CS2000 Session Server, the Core QSIP command will display the above SIP Lines information.

The response for the QSIP query sent is expected to arrive within a specific time interval. The default QSIP response time interval is 15 seconds. However, the timeout can be set from 1 to 30 seconds. If any value greater than 30 or lesser than 1 is given as the timeout value, the timeout value will be set to the default timeout value of 15. Timeout is an optional parameter in the QSIP command.

The QSIP command will only display the CS2000 Session Server services that are ENABLED. There could be services provisioned on the SIP line which are DISABLED which would not be shown. However, the QSIP will display the Service Package Name which would help if it is known which services are in a particular Service Package.

If a SIP line has contacts, only the URIs of the first three contacts will be shown.

If a SIP line has more than 3 middle box ids, only 3 middle box ids will be displayed.

If QSIP cannot display the SIP data from the CS2000 Session Server a message will be printed as follows:

SIP DATA CANNOT BE DISPLAYED DUE TO <REASON>

Where <REASON> could be one of the following

- RESPONSE TIMEOUT FROM CS2000 SESSION SERVER
- BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER
- QSIP SEND REQUEST FAILURE
- The QSIP Application Error String from the QSIPReportError message received from CS2000 Session Serve

If the response from the CS2000 Session Server does not have any data for any of the parameters then the following message is displayed:

- SIP DATA CANNOT BE DISPLAYED BECAUSE NO DATA RECEIVED FROM CS2000 SESSON

If the CS2000 Session Server responds with partial data, before the SIP data portion of the QSIP display begins there will be a message:
"PARTIAL DATA RECEIVED FROM THE CS2000 SESSION SERVER."
Then, the QSIP will display whatever data it can and leave the other fields blank.

If the total number of parameters, including main parameters and their sub-parameters, received in the response message from CS2000 Session Server is greater then 19 then it would be considered as an error scenario and the following message would be displayed:

SIP DATA CANNOT BE DISPLAYED DUE TO BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER

The Allow Post Busy Termination and Node numbers and Terminal numbers of the VIDs active on the call are displayed only if some data is received in the response message from the CS2000 Session Server.

QSIP will work for all the LENs that work fine with QLEN. However, to get data the LEN should correspond to a SIP Line.

If QSIP is used with a non-SIP DN then the following message will be displayed:
QSIP SHOULD BE GIVEN FOR SIP LINES ONLY

If a non-existent DN is specified for QSIP then the following message will be displayed:
INVALID DN SPECIFIED FOR THE QSIP COMMAND

If a non-existent LEN is specified for QSIP then the following message will be displayed:
INVALID LEN SPECIFIED FOR THE QSIP COMMAND

The QSIP command's CI format is shown below:

>q qsip

DISPLAY SIP LINE INFORMATION
Command Format: QSIP <DR_LEN_TYPE>
Parms: [<TIMEOUT> {1 TO 30}]

- Example for QSIP (DN as a parameter)

> qsip 6138675309
SIP USER DATA
==========
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12
CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061
6138675309@1.2.3.4:5062
SERVICE PACKAGE: DEFAULT_PKG
SERVICES: ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
==========
ENDPT ID: PHX/003/0/1000
VMG: VMG.1
MIDDLE BOX ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
==========
ACTIVE CALL APPEARANCES:
NODENO TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12

- Example #2 for QSIP (LEN as a parameter)

> qsip 6138675309
SIP USER DATA
==========
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12

CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061
6138675309@1.2.3.4:5062
SERVICE PACKAGE: DEFAULT_PKG
SERVICES: ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
==========
ENDPT ID: PHX/003/0/1000
VMG: vmg
MIDDLE BOX ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
==========
ACTIVE CALL APPEARANCES:
NODENO TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12

1.1.6.2 QDN/QLEN/DISPCALL/PMIST/CALLTRAK:

The QDN, QLEN, DISPCALL, PMIST, and CALLTRAK tools will be supported for DPL Lines, and they will retain their same functionality and same command interfaces. There will be no impact to these tools by this activity. However, tools like CALLTRAK are tid-based, and thus when tracing on a DPL line with multiple active calls, trace data for ALL of the active calls with be captured.

1.1.6.3 DISPCALL:

DISPCALL is a tool which is used to capture the call data associated with the agent.The agent can be selected to capture the call information using following commands.They are SAVETID and SAVELEN.

The parameter for SAVETID is node number and terminal number.And parameter for SAVELEN is LEN of the agent. For DPL lines a new optional parameter KEY has been added along with the existing parameter for both SAVETID and SAVELEN.The KEY parameter holds the key value of the call appearance.The key values can be obtained form the tool DPLTEST.

IF the agent is selected with out key value for DPL lines, the tool checks for number of call appearance associated with the selected TID or LEN. IF there is only one call appearance associated with the TID/LEN then it gives the information associated with that call. IF there are multiple call appearances, then it displays the message saying multiple calls associated with this call, please enter the key value.

1.1.6.4 CALLTRAK:

CALLTRAK tool is used to capture the IO messages and procedure traces for the agent selected. For DPL lines, Since all the VIDS are allocated dynamically, and deallocated by the time the call complete, there would not be any vids associated with the agent by the time logs are displayed using the display command. So the log may not show the exact agent information.

For DPL lines, the hook has been added in the calltrak, so that it will store only the base TID in the call data and also capture all the information associated with that TID. Since only the base TID is stored in the call data, the calltrak log will not show the KEY information in the IO message for DPL lines.

Ex:

INCOMING 14:48:20.116 NODE TYPE= LGRP_NODE SCP_X_ALERTING_MSG

NN= 00B5 TN= 002F MSGTAG= 00 ROUTE= 0080 ERROR= 00 LENGTH= 0C

AGENT= SS 00 0 00 46 DN 6136215046

6D 02 00 00

1.1.7 Information regarding the Network Services / Signalling Interworking:

The following tables illustrate the network services/signalling interworking information.

Client Services
Call Forward (local)
Call Return (local)
Call Waiting
Call Waiting Disable
Caller ID
Do Not Disturb (local)
Hold
3-Way Call
Call Transfer

Country Specific services

Austria - Carrier Pre-Selection (via TNS parameter)
Belgium LNP (OR, ACQ)
Belgium TOPS
Belgium Lawful Intercept
Belgium 8 / 9 Digit Dialplan
France ETSI V.23 CLASS
France Backward Charging via Tax Message
Germany Network AOC
Germany Carrier Pre-Selection
Germany Carrier Pre-Selection
Germany TNS Routing
Germany Lawful Intercept
Germany Call Compl Busy Sub
Germany QSIG
Germany LNP
Germany Variable Dial Plan
Israel Backward Charging for Intnl Calls
Israel Voice Mail
Netherlands LNP (OR, ACQ)
UK LNP (OR and ACQ)
UK Carrier Pre Selection
UK Bellcore CLASS
UK Automatic Recall
UK MSAC
UK CDR Billing
UK ACD / Compucall
UK Network ACD
UK DPNSS Feature Transparency

Mexico TOPS
Mexico CLASS
Mexico Trunk Offer
Australia Lawful Intercept
Australia ACD / Compucall
Australia Network ACD
Australia CLASS
Australia TOPS
Australia TR533 (IN variant)
Australia LNP (ACQ)
Australia E800
Australia Carrier Pre-selection
Australia Centrex IP

Agent Interworking

Agent Interworking Test - French BRI
Agent Interworking Test - Israel Res Lines (MMP15 only)
Agent Interworking Test - UK DASS 2
Agent Interworking Test - Mexico Fixed Wireless Access
Agent Interworking Test - Australia MFT
Agent Interworking Test - Australia TS13

Signalling Interworking

Signalling Interworking test - ETSI ISUP V1
Signalling Interworking test - ETSI ISUP V2
Signalling Interworking test - IBN7
Signalling Interworking test - H.323
Signalling Interworking test - QSIG
Signalling Interworking test - ETSI PRI
Signalling Interworking test - V5.2
Signalling Interworking Test - Austria ISUP

Signalling Interworking Test -Belgium ISUP (migrating to ETSI V2)
Signalling Interworking Test - France, SSUTR2
Signalling Interworking Test - France, SPIROU
Signalling Interworking Test - France, SSURN
Signalling Interworking Test - German ISUP
Signalling Interworking Test - Israel ISUP
Signalling Interworking Test - Israel PRI
Signalling Interworking Test - Israel FDCP R2
Signalling Interworking Test - Netherlands ETSI ISUP V2
Signalling Interworking Test - Netherlands Dutch PRI
Signalling Interworking Test - Norway ISUP
Signalling Interworking Test - Spain ISUP V1
Signalling Interworking Test - Spain PRI
Signalling Interworking Test - Swiss ETSI ISUP V2
Signalling Interworking Test - Swiss PRI
Signalling Interworking Test - UK IUP
Signalling Interworking Test - UK ISUP
Signalling Interworking Test - UK IBN7 Backbone
Signalling Interworking Test - Mexico ISUP
Signalling Interworking Test - Mexico Telmex ISUP
Signalling Interworking Test - Mexican R2
Signalling Interworking Test - Australia IE ISUP
Signalling Interworking Test - Australia I-ISUP
Signalling Interworking Test - Australia ATUP
Signalling Interworking Test - Australia AISUP
Signalling Interworking Test - Australia IBN7 Backbone
Signalling Interworking Test - Australia RLT
Signalling Interworking Test - Australia TS14
Signalling Interworking Test - NZ ISUP
Signalling Interworking Test - Newzealnd R2

PMA Based

Last Number Redial
Anonymous Call Rejection
IBN CFU/CFB/CFD intragroup / intergroup screening
IBN Do Not Disturb
Subscriber Activated Call Blocking - International Line Restriction for international deployment
IBN Call Forward Programming - No call forward interrogation option may be desired in some markets.
Call screening override
Speed Dial programming

Network based

Message Waiting
Station Message Detail Recording
Special Billing - CDR
Suspended Service
Terminating DN Billing
Tollfree Services
Multi-Switch Business Group (MBG) i/w
Interop with other Succession endpoints (PVG, MG9K, legacy lines via IW SPM IP, etc.)
Direct Inward Dial
Direct Outward Dial
E911 termination
IN - no digit collection
Lawful Intercept
Free Number Terminating
Customer groups with mix of Unistim, SIP, IBN lines
Subscriber Line Usage
Operator Number Identification

PIC
Dial Plan Management
Virtual Private Network (VPN)
INWATS / OUTWATS - Freephone number Intl.
VFG
Local Number Portability
Carrier Pre-Selection (provisioned and prefix dialing)
Simple MEETME and PRESET Conference
Carrier Toll Denial - International calls - Inter-Lata - Intra-Lata
NCOS restrictions
NCOS Time of Day routing
Denied Termination
Denied Origination

1.2 Hardware Requirements or Dependencies

None.

1.3 Software Requirements or Dependencies

The CORE OAMP functionality has dependencies associated with some of the other components in the overall SIP lines feature:

- SESM
- CS2KSS
- GWC
- OSSGATE
- NCAS Link

1.3.1 SESM:

SESM EM needs the enhancements in table LGRPINV for bulk provisioning and line provisioning.

1.3.2 CS2KSS:

- QSIP core client is dependent on the CS2KSS API for QSIP query.
- SCPLITE APIs should be present to support the QSIP messaging.
- The CS2KSS profile team has to provide an API to get the Registration status and the SIP URI information

- The CS2KSS callp should provide an API to give the Active sessions for a SIP Line
- The CS2KSS will need to know the syntax of the QSIP messages it will receive from and send to the Core.

1.3.3 GWC

- GWC EM requires table SERVRINV enhancements to support the new term type DPL and a new exec lineup DPLEX.
- The state changes due to the operations BSY, RTS, FRLS, HOLD, NEXT performed on SIP lines in core should be propagated to the GWC.
- When the CS2KSS or GWC are taken down, the same should be notified to the core.
- Audit messages will be sent between the CORE & GWC and the message protocol from both the parties should be understood by each other.
- Carcodes for the DPL lines are restricted to RDTLSG for the North American market whereas it is restricted to GWLPOT for the International market.

1.3.4 OSSGATE:

- It needs the IBNFEAT and servord enhancements for line provisioning and other servord+ line commands like DEO, ADO etc.

1.3.5 NCAS Link:

- It should be available for the QSIP query to take place.

1.4 Limitations and restrictions

- Since the CLTG command is applicable only to POTS and RES lines, the CLTG Servord command applies to only RES DPL lines. CHG NCOS will have to be used for providing the functionality to IBN DPL lines. The CLTG and CHG will be done via SESM.

1.5 Interactions

None.

1.6 Glossary

Term	Description
CS2K	Communication Server 2000
CPD	Call Processing Deloaded
CB	Connection Broker
DEL	Deloaded
GWC	Gateway Controller
INB	Installation Busy
LMB	Line Module Busy
LCC	Line Class Code
NCAS	Non Call Associated Signalling
NEQ	Not Unequipped
OSSGATE	Operation Support System Gate
OAMP	Operation, Administration, Maintenance & Provisioning
CS2KSS	Communication Server 2000 Session Server
SESM	Succession Element and Sub-Element Manager
SB	System Busy
SERVORD	Service Order
SOC	Software Optionality Control
SCTP	Stream Control Transmission Protocol

2: Configuration for A00008556

2.1 Hardware and Software Requirements

No new hardware or software requirements are created by this activity.

2.2 Initial Configuration

At initial configurations, it is assumed that standard datafill exists in the DMS/CS2K, GWC and CS2KSS. Since a usage SOC is used for this feature, the SOC limit decides whether any service will be provided initially by the design components applicable after the DPL line is provisioned.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

N/A

2.4 Upgrade Considerations

None.

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 below shows a list of new/modified tables.

Table 1 New or modified tables

Table/MIB name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
SERVRINV	CHANGED	UNCHANGED
LGRPINV	CHANGED	UNCHANGED
IPAPPL	CHANGED	UNCHANGED
IBNFEAT	CHANGED	UNCHANGED
LCCOPT	CHANGED	UNCHANGED
OPTOPT	CHANGED	UNCHANGED

2.5.2 Table/MIB/Remote Database Schema information

2.5.2.1 Name: SERVRINV

SERVER INVENTORY

2.5.2.1.1 Functional description

Server Inventory table stores the information on GWC. Each entry in this table provides information about a specific GWC which includes the following:

- Server type and numeric ID, e.g. GWC 7.
- Packet network type (IP or ATM).
- GWC IP address.
  Note: The last element of this address must be a multiple of four, because four IP addresses are used by each GWC; the three IP addresses next in sequence are assigned automatically.
- The server exec(s) to be used, which determines the type of call processing to be performed by the GWC. A new entry is specified for this field by this feature.
- Toneset to be used.
- Bearer Networks.
- Optional attributes to be associated with this GWC.

2.5.2.1.2 Usage sequence and implications (CM Only)

The table SERVRINV can be datafilled independently through SESM. There is no change in the current table datafill order.

2.5.2.1.3 Size

Table 2 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
SERVRINV	0	256	Memory is dynamically allocated at 16 tuples per allocation.

2.5.2.1.4 Fields/OIDs

The following table lists fields/OIDs for SERVRINV.

Table 3 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
SRVREXEC	Changed	TERM_TYPE EXEC_LINEUP	DPL_TERM DPLEX	This field now supports a new term_type DPL_TERM and a new exec_lineup DPLEX.

2.5.2.1.5 Datafill example

The following example shows sample datafill for table SERVRINV.

Table SERVRINV:

SRVRNAME SRVRADDR ***SRVREXEC*** *SRVRTONE BEARNETS SRVROPTS*
GWC 0 IP 45 46 47 48 ***(DPL_TERM DPLEX)*** *$ NORTHAA (NET_IP Y) $ $*

2.5.2.1.6 Table release history update

The table SERVRINV is enhanced to support new SRVREXEC entry DPL DPLEX. This entry for a new terminal_type and new exec_lineup is specifically going to be used to support the DPL agents on the GWC.

2.5.2.1.7 Supplementary information

None.

2.5.2.1.8 Translation verification and other tools

None.

2.5.2.2 Name: LGRPINV

LOGICAL GROUP INVENTORY

2.5.2.2.1 Functional description

Logical group inventory table defines the gateways or nodes supported under the gateway controller. The gateway or node entries are:

- Logical group number (site name, frame no, shelf no) e.g. LG 2 3
- Server name (GWC datafilled in table SERVRINV)e.g GWC 7
- Logical group type: This field is to specify the group type.
  Existing logical group types are
  S MG9K large lines gateways
  M CICM large lines gateways
  C Small lines gateways
  LL_3RDPTY Large Line Third Party gateways
  SSDPL DPL lines.
- When the LGRPINV is provisioned with a LGRP ‘SSDPL’, then a termtype ‘DPL’ is specified in LNINV table. When lines are provisioned in table LNINV, then an exec_lineup DPLEX corresponding to termtype ‘DPL’ will be downloaded to the GWC. Also, the cardcode of the DPL lines is restricted to RDTLSG for North American market and GWLPOT for International market.
- Logical group options
  Existing options are: (MTSTAPT, LGRPLOC, GTWYKEY)

2.5.2.2.2 Usage sequence and implications (CM Only)

The table LGRPINV depends upon the table SERVRINV. It references the server name from the table SERVRINV.

2.5.2.2.3 Size

The following table lists the size of LGRPINV table.

Table 4 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
LGRPINV	0	1000	Memory is dynamically allocated at 10 tuples per allocation.

2.5.2.2.4 Fields/OIDs

The following table lists fields/OIDs for LGRPINV

Table 5 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
GRPTYPE	Changed	N/A	SSDPL	A new LGRP SSDPL has been introduced to support DPL lines.

2.5.2.2.5 Datafill example

The following example shows sample datafill for table LGRPINV

Table LGRPINV:

LGRP_NO SRVR_NAME ***GRPTYPE*** *LGRPOPTS*
LG 1 1 GWC 5 ***SSDPL*** *$*

2.5.2.2.6 Table release history update

The table LGRPINV is enhanced to support DPL agents. As part of this enhancement new lgrp_type 'SSDPL' is introduced.

2.5.2.2.7 Supplementary information

None.

2.5.2.2.8 Translation verification and other tools

None.

2.5.2.3

2.5.2.4 Name: IPAPPL

Internet Protocol Application

2.5.2.4.1 Functional description

Table IPAPPL datafill provides instance of various connections to the DMS. The use of SCTP transport requires that the application store the specific remote IP addresses and local Port number. Therefore table IPAPPL is datafilled in order to provide these details. Table IPAPPL includes following fields.

TABLE IPAPPL Fields and description are as follows:

- InstKey is datafilled in order to map this instance with an internally assigned instance number. This field is the unique key to the tuple.
- InstanceName is datafilled in order for the telco personnel to be able to distinguish one connection from the other.

- Transport is datafilled in order to classify the instance to which transport protocol be used. Currently the table will support SCTP functionality ONLY.
- IPDevice is datafilled to indicate which IP interface hardware will be used. This table currently supports EIU and HIOP.
- IP addresses (up to 4 addresses) are allowed in one instance tuple. This may be used to support multihoming. The first IP address in the list will be used as the primary address. IPV4 type IP addresses are supported.Only one IP address will be used for DPL, the IP address of the CS2KSS Provisioning Manager.
- Port Number is the local port number at which the DMS-Core will expect to receive messages from this instance. (Note that the remote port is received during the INIT message from the far-end). Valid range of Source port allowed to be configured on the CORE is from 4900 to 4982
- OptList field may be datafilled with “SETPRIME” to set any of the IP address in an instance to be used as to set the primary destination address.
- Optlist sub-field “APPLICATION” can be datafilled to specify the application e.g.: DPL. Here the SIPMTC (Application) option is incorporated along with AIN option.
- Optlist sub-field “mode” is to specify the mode SERVER/CLIENT.
- Optlist sub-field “multihoming” is used to specify if the remote node supports multihoming. This option is currently only supported on the HIOP ipdevice.

2.5.2.4.2 Usage sequence and implications (CM Only)

The table IPAPPL is an independent table.

2.5.2.4.3 Size

Table 6 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IPAPPL	0	64	Memory is automatically allocated for 64 Intelligent Network SCTP instances

2.5.2.4.4 Fields/OIDs

The following table lists fields/OIDs for IPAPPL.

Table 7 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
OPTS	Changed	Application	SIPMTC	A new application 'SIPMTC' is added to option list.

2.5.2.4.5 Datafill example

The following example shows sample datafill for table IPAPPL:

Table IPAPPL:

InstKey InstName Transport IPDevice IPaddrs port optlist
1 a sctp hiop 198.202.188.121 4982 (application ***sipmtc****)*
(setprime 1)

2.5.2.4.6 Table release history update

The table IPAPPL is enhanced to create an instance for SIPMTC service.

2.5.2.4.7 Supplementary information

- The NCAS link association is going to be used for the new QSIP command.
- The SIPMTC application is supported over HIOP only.
- The multihoming functionality is not supported in SIPMTC application.
- The port number allocated for SIPMTC application is 4982.
- Multiple instances for SIPMTC are not allowed; i.e. in table IPAPPL, there can be only one instance datafilled for SIPMTC.

2.5.2.4.8 Translation verification and other tools

None.

2.5.2.5 Name: IBNFEAT

IBN Feature

2.5.2.5.1 Functional description

IBNFEAT (IBN Line Feature) lists line features that are assigned to the IBN lines listed in table IBNLINES.

Table IBNFEAT fields and description are as follows:

LEN: Line equipment number. This field consists of the subfields SITE, FRAME, UNIT, DRAWER, LSG and CIRCUIT.

DNNO_RANGE: Directory number. This field specifies the DN of the LEN being referenced. Enter a value from 0 to 6 for the DN.

DF : Data feature. This field specifies the data feature assigned to the line.

FEATURE: Data feature. This field specifies the data feature assigned to the line.

DATA: SIP: Bool. Enter Y if a SIP line

MAX_NUM_CALLS: Enter a value between 1-10.

ALLOW_BSY_TERM: Bool. It determines whether or not a busy SIP line can take an additional call termination.

Only Servord can be used to datafill the DPL option. It cannot be done via table control.

2.5.2.5.2 Usage sequence and implications (CM Only)

- In table LCCOPT, DPL option should be made compatible with IBN LCC.
- The table IBNLINES should have the LEN datafilled before the DPL option can be added on it.

2.5.2.5.3 Size

2.5.2.5.4 Fields/OIDs

Table 8 Table size

Abbreviated table name	Minimum tuples	Maximum tuples	Information on memory
IBNFEAT	0	TBD	TBD

The following table lists fields/OIDs for IBNFEAT.

Table 9 Table field descriptions

Field	New or Changed	Subfield or refinement	Entry	Explanation and action
DF	Changed	N/A	DPL	A new feature DPL to be assigned to an IBN line.
Feature	Changed	N/A	DPL	A new feature DPL to be assigned to an IBN line.
DATA	Changed	SIP MAX_NUM_CALLS Allow_Bsy_Term	Y/N 1-10 Y/N	Enter Y if a SIP line Max Simultaneous Call Appearances. It determines whether or not a busy SIP line can take an additional call termination.

2.5.2.5.5 Datafill example

The following example shows sample datafill for table IBNFEAT.

Table IBNFEAT:

LEN DNNO DF FEATURE DATA
LG 01 1 00 14 0 DPL DPL Y 10 Y

2.5.2.5.6 Table release history update

Table IBNFEAT has been enhanced to support a new feature DPL which will convert the IBN line into a DPL line.

2.5.2.5.7 Supplementary information
None.

2.5.2.5.8 Translation verification and other tools
None.

2.6 Service Orders (SO) (CM & SESM)
SERVORD+ will accept three new options related to DPL lines provisioning: DPL, SIP_PASSWORD and SIP_DATA. When provisioning a SIP line all three of the options described above must be present in the SERVORD+ NEW command. They can not be added later via ADO.

2.6.0.1 LCC and options
New line option DPL is introduced by this feature. It is compatible with RES and IBN line class codes only. DPL is not compatible with huntgrps, scmp, MADN, FTRG.

Table 10 Meridian digital centrex feature assignment requirements

Feature	500 2500	MDC SET	ISDN SET	MDC Set ISDN Set Relationship							
				SET	SUBSET	KEY	DN	DEDKEY	LAMP	CODE	DISPLAY
DPL	Y	N	N	N							

The feature in the table above requires a handsfree Business Set. This feature must be assigned to key 1.

2.6.1 New commands
No new commands are introduced with this feature.

2.6.1.1 How service order commands are presented

2.6.1.1.1 Description
The NEW command is used to associate a DN with a LEN due to which the line state changes from HASU (hardware assigned-software unassigned) to IDL, i.e. puts the line into service.

2.6.1.1.2 Applicability

The DPL line option can only be added with the NEW command. Other commands that prompt for options such as EST, ADD, DE0, ADO and NEWACD will be rejected if the DPL option is present with these commands. A warning message will be output. The CDN and CLN commands will be blocked if the DPL option is present on the line. The line must be OUTed and NEWed to effect a change of LEN or endpoint or DN. CHG of line class code will be blocked if DPL is present on the line.
The DPL option should only be added via SESM. It cannot be added via table control.

2.6.1.1.3 Example

The examples below show how SERVORD+ command NEW can be used to provision the DPL line. Servord+ should be used to add the DPL option. Th e prompt mode is shown as an example of the fields only. Note that SIP_PASSWORD and SIP_DATA are not valid options on the core and are shown here for example only.

Figure 1 Example of the NEW command in prompt mode (SERVORD only)

```
>NEW
SONUMBER:     NOW   4 10 20 PM
>$
DN:
>6212500
LCC_ACC:
>IBN
GROUP:
>BNR
SUBGRP:
>0
NCOS:
>0
SNPA:
>613
LATA:
>NILLATA
LTG:
>0
LEN_OR_LTID:
>LG 000 0 10 13
Option:
>DPL
SIP:
>Y
MAX_NUM_CALLS:
```

```
>3
ALLOW_BSY_TERM:
>Y
SIP_PASSWORD:
>xxx
SIP_DATA:
>bobby mb1
```

Figure 2 Example of the NEW command in no-prompt mode

In the no-prompt mode, the command as entered through SESM will be:

```
NEW $ 6212500 IBN BNR 0 0 613 NILLATA 0 LG 000 0 10 13 DPL Y 3  Y
xx bobby mb1
```

Figure 3 Example of the CHF command in no-prompt mode

```
CHF $ 6212500 DPL Y 7 N $
```

2.6.1.2 How service order options are presented

2.6.1.2.1 Description

A new option DPL is introduced as a part of this activity. This option DPL converts an IBN line into DPL line. The following sections lists how the DPL option and the sub-options associated with the DPL option are assigned through SERVORD.

2.6.1.2.2 Example

The following examples show how a new option DPL and its sub-options are added to a line to convert it into a DPL line.

Figure 4 Example of the DPL option in prompt mode (SERVORD only)

```
Option:
>DPL
SIP:
>Y
MAX_NUM_CALLS:
>3
ALLOW_BSY_TERM:
>Y
```

Figure 5 Example of the DPL option in no-prompt mode

```
DPL Y 3  Y xx bobby mb1
```

2.6.1.2.3 Option prompts

Table 11 System prompts for DPL option

Prompt	Valid input	Description	Areas affected by prompt
SIP	Y	Bool	
MAX_NUM_CALLS	1-10	Integer	
ALLOW_BSY_TERM	Y/N	Bool	

2.6.1.2.4 Line class code compatibility

The new DPL option is applicable only for the IBN and RES lines.

Table 12 DPL compatibility to LCC

Line class code	Compatible?
IBN	Yes
RES	Yes

2.6.1.2.5 Assignability

DPL is not a valid keyset option.
The following functionalities apply to this option:

- set functionality: <yes or no>
- subset functionality: <yes or no>
- DN functionality: <yes or no>
- key functionality: <yes or no>

2.6.1.2.6 Option prerequisites

None.

2.6.1.2.7 Notes

The subfields SIP and MAX_NUM_CALLS which will be prompted for will have the default values of Y and 1 shown respectively. For SN08 and SN09, these are the only valid values and cannot be changed.

2.6.1.2.8 SERVORD+ Exceptions

None.

2.6.2 Line equipment format changes

2.6.2.1 LEN

There are no changes made in the LEN format.

2.6.2.2 Media gateway endpoint format

The MG endpoint format is similar to the LEN format to make the mapping between them easier.

The suggested endpoint format is:
<GW NAME> <SITE>/NNN/G/TTtt where
GW_NAME = up to 32 chars
<SITE> = a site name datafilled in Table SITE and used as the first part of the LGRPINV key.
NNN = logical frame number from core table LGRPINV
G = group number 0-9 from core table LGRPINV
TT = 00 to 10
tt = 00 to 99 except when TT = 10 then tt = 00 to 22
Example:
SIPVMG1.tampa.vz.com TMP1/000/2/0478 maps to LEN: TMP1 000 2 04 78

2.7 Software optionality control (SOC)

This feature will be controlled by standard usage-based SOC. The limit will define the maximum number of DPL lines that can be provisioned in the switch.

- The default usage limit will be zero, indicating that the DPL option can not be provisioned. New limits can be purchased via SOC in increments of 1 subscriber at a time if desired.
- There will not be a maximum limit. Hence, any limit can be assigned to the SOC CS2C0005.
- When a new DPL line is provisioned, the current DPL count (SOC usage count) will be compared to the purchased limit (SOC usage limit). If the limit has already been reached, the new line can not be provisioned. If the limit has not been reached, the new line is allowed, and the SOC usage count is incremented.
- When an existing DPL line is removed, the current SOC usage count will be decremented, but the SOC limit will not change.
- If the SOC limit is ever decreased to a value below the current usage count, existing DPL line agents will continue to function properly. However, new DPL lines can not be added. Further, if existing DPL lines are removed, they can not be re-added until the current count is below the limit.
- The SOC audit will generate a warning log on each pass if the usage count is above the usage limit.
- The SOC code is functional whenever a line is provisioned with the DPL option whether through table control / servord.
- The usage control of the SOC utility allows the activation/deactivation for provisioning of DPL lines.
- A new module will be created to contain the new SOC code. The new module will belong to a new user group called DPLOAMP.

- It is strongly recommended that the SOC code be sourced in SN09 if possible. This is due to the fact that patching of a usage-based SOC can introduce certain obstacles regarding usage limits and usage counts being updated during ONP. To minimize these obstacles, the SOC code can be sourced in SN09.
- Table 13 below shows the SOC details.

Table 13 SOC

SOC option name:	CS2C0005
SOC option title:	Number of SIP CLient
SOC option control type:	USAGE
New SOC option?	Yes
SOC option order code	CS2C0005
Option defined in DRU:	CCM
Affected products:	CS2K

2.8 Element Management

Not Applicable.

2.9 User interface changes

2.9.1 Directory:

N/A

2.9.2 Command: QSIP

2.9.2.1 Command type: NON-MENU

2.9.2.2 Command target: BRISC, POWERPC

2.9.2.3 Command availability: NONRES

2.9.2.4 Command description

The QSIP command at the CI level will query the CS2KSS to get the SIP information. QSIP command will query the following for the DPL agent:

SIP URI

Registration State

Allow Post Busy Termination

Number of Contacts

Contacts

Service Package

Services

Endpt ID

Virtual Media Gateway

Middle Box ID List

Client Type

Static Client

Node number and Terminal number of the VIDs of all the Active Call Appearances

Number of Active Sessions in CS2000 Session ServerSIP URI

- The CS2KSS will handle the query from the CS2K via the NCAS link for the QSIP command and respond back to the CS2K with the requested data.

- The default time interval for getting a response to the QSIP query is 15 seconds. Time can be set from 1 to 30 seconds. If any value lesser than 1 and greater than 30 is given then the time value will be set to the default value of 15. It is an optional parameter in the QSIP command.

- The QSIP command's format is listed below

CI:
>q qsip
DISPLAY SIP LINE INFORMATION
Command Format: QSIP <DR_LEN_TYPE>
Parms: [<TIMEOUT> {1 TO 30}]

- If the NCAS Link is unavailable or the CS2KSS did not respond, the QSIP command's timer will expire with the following message:

>qsip 8675309
SIP DATA CANNOT BE DISPLAYED DUE TO RESPONSE TIMEOUT FROM CS2000 SESSION

2.9.2.5 Command syntax

Table 14 QSIP command parameters and variables

Command	Parameters and variables
QSIP	<DR_LEN_TYPE> [<Timeout> {1 to 30}]
Parameters and variables	Description
DR_LEN_TYPE	The DN/LEN of a SIP line agent is specified
TIMEOUT	Maximum time for which QSIP waits for a response from CS2KSS. Min value:1 seconds Max value:30 seconds Default value:15 seconds

2.9.2.6 Qualifications and warnings

QSIP query takes place through the NCAS link. Hence, the command response depends upon the availability of the NCAS link.

When the response is not received in a specified time interval, a message is displayed at the console:

“NO RESPONSE FROM CS2KSS WITHIN TIMEOUT OF 15 SECONDS”.

2.9.2.7 Responses

Table 15 MAP outputs with associated meanings and actions

Command
Example 1: >qsip 8675309 --- SIP USER DATA ========== SIP URI: 6138675309@NORTELNETWORKS.COM ACCOUNT STATUS: ACTIVE REGISTERED: Y ALLOW POST BSY TERMINATIONS: N NUMBER OF CONTACTS: 12 CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061 6138675309@1.2.3.4:5062 SERVICE PACKAGE: DEFAULT_PKG SERVICES: ADHOC 4 ADDRBK 50 VMAIL SIP LINE DATA ========== ENDPT ID: PHX/003/0/1000 VMG: vmg MIDDLE BOX ID(s): 1234 1234 3456 CLIENT TYPE: ONT STATIC CLIENT: N SIP CALL DATA ========== ACTIVE CALL APPEARANCES: NODENO TERMNO NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12 ---
Meaning: The querying was successful. All the data obtained is displayed. **System or user actions:** None.

Table 15 MAP outputs with associated meanings and actions

Command
Unsuccessful Query: **Example 2:** >qsip 8675309 SIP DATA CANNOT BE DISPLAYED DUE TO RESPONSE TIMEOUT FROM CS2000 SESSION SERVER **Meaning:** The response was not received before the QSIP timer expired either because the NCAS link is either busy/not available or the CS2KSS did not respond before the timeout occurred. **System or user actions:** The user is expected to run QSIP again. **Example 3:** >qsip 122456783 QSIP SHOULD BE GIVEN FOR SIP LINES ONLY **Meaning:** The DN supplied is not a SIP line. **System or user actions:** The user is expected to give a valid SIP Line DN for QSIP. Example 4: >qsip 122456783 INVALID DN SPECIFIED FOR THE QSIP COMMAND Meaning: The DN supplied is not a valid DN. System or user actions: The user is expected to give a valid SIP Line DN for QSIP. Example 5: >qsip LG 0 2 3 4 INVALID LEN SPECIFIED FOR THE QSIP COMMAND Meaning: The LEN supplied is not a valid LEN. System or user actions: The user is expected to give a valid SIP Line LEN for QSIP. Example 6: >qsip 8675309 SIP DATA CANNOT BE DISPLAYED DUE TO BAD MESSAGE RECEIVED FROM CS2000 SESSION SERVER Meaning: The response received from CS2KSS in not valid. System or user actions: The user is expected to run QSIP again. Example 7: >qsip 8675309 SIP DATA CANNOT BE DISPLAYED BECAUSE NO DATA RECEIVED FROM CS2000 SESSON SERVER Meaning: The response received from CS2KSS does not have any data to display System or user actions: The user is expected to run QSIP again.

Example 8:

```
>qsip 8675309
SIP DATA CANNOT BE DISPLAYED DUE TO QSIP SEND REQUEST
FAILURE
```

Meaning: An error occurred while the QSIP sent the query to the CS2KSS.

System or user actions: The user is expected to run QSIP again.

Example 8:

```
>qsip 8675309
PARTIAL DATA RECEIVED FROM THE CS2000 SESSION SERVER.
--------------------------------------------------------------------------------
SIP USER DATA
=============
SIP URI: 6138675309@NORTELNETWORKS.COM
ACCOUNT STATUS: ACTIVE
REGISTERED: Y
ALLOW POST BSY TERMINATIONS: N
NUMBER OF CONTACTS: 12
CONTACTS:
SERVICE PACKAGE: DEFAULT_PKG
SERVICES: ADHOC 4 ADDRBK 50 VMAIL

SIP LINE DATA
=============
ENDPT ID: PHX/003/0/1000
VMG: vmg
MIDDLE BOX ID(s): 1234 1234 3456
CLIENT TYPE: ONT
STATIC CLIENT: N

SIP CALL DATA
=============
ACTIVE CALL APPEARANCES:
  NODENO   TERMNO
NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12
--------------------------------------------------------------------------------
```

Meaning: the response from CS2KSS did not have data for all the parameters..

System or user actions: None.

2.9.2.8 Example

Table 16 Usage examples for QSIP command

Description of task	The QSIP command at the CI level will query the CS2KSS to get the SIP information.
Command: MAP response:	Example: QSIP 8731932 >qsip 8675309 ---------- SIP USER DATA ========== SIP URI: 6138675309@NORTELNETWORKS.COM ACCOUNT STATUS: ACTIVE REGISTERED: Y ALLOW POST BSY TERMINATIONS: N NUMBER OF CONTACTS: 12 CONTACTS: 6138675309@4.3.2.1:5060 6138675309@4.3.2.1:5061 6138675309@1.2.3.4:5062 SERVICE PACKAGE: DEFAULT_PKG SERVICES: ADHOC 4 ADDRBK 50 VMAIL SIP LINE DATA ========== ENDPT ID: PHX/003/0/1000 VMG: vmg MIDDLE BOX ID(s): 1234 1234 3456 CLIENT TYPE: ONT STATIC CLIENT: N SIP CALL DATA ========== ACTIVE CALL APPEARANCES: NODENO TERMNO NUMBER OF ACTIVE SESSIONS IN SIP LINE SERVER: 12 ----------

2.10 OSSGate Interface Changes

Not Applicable.

2.11 Security

None.

2.12 Configuration Walkthrough

The following shows a sequence in which the tables are datafilled:

Table SERVRINV (Provisioned through SESM):

*SRVRNAME SRVRADDR **SRVREXEC** SRVRTONE BEARNETS SRVROPTS*
*GWC 0 IP 45 46 47 48 **(DPL_TERM DPLEX)** $ NORTHAA (NET_IP Y)$ $*

Table LGRPINV (Provisioned through SESM)

*LGRP_NO SRVR_NAME **GRPTYPE** LGRPOPT*
*LG 1 1 GWC 5 **SSDPL** $*

Table LNINV (Provisioned through SESM):

LEN CARDCODE PADGRP STATUS GND BNV MNO CARDINFO
LG 1 1 10 13 RDTLSG PKLNL HASU N NL Y NIL

Servord+ Command (Provisioned through SESM):

NEW $ 6212500 IBN BNR 0 0 613 LG 000 0 10 13 DPL 3 SIP_PASSWORD xx SIP_DATA bobby mb1

Table IPAPPL (Provisioned by Crafts person):

InstKey InstName Transport IPDevice IPaddrs port optlist
*1 a sctp eiu 12 12 12 12 4901 (application **sipmtc**)*
(setprime 1)

Product = World Trade

A00009145 -- Record Feature Usage

1: Applicable solution(s)

Int'l DMS

1.1 Description

The purpose of this activity is to provide detailed information about the subscriber action of a service usage at the billing records.

With this activity, developed in ISN09 (MMP22) release, DMS - MMP is capable to give detailed information about the subscriber feature actions as a billing record. By using these billing records, Telcos can charge their customers for their feature usage, if desired.

Feature usage indication is provided for ***Call Lock (ILR), Call Waiting (ICWT), Abbreviated Dialing (SCL), CLIR (SUPPRESS + CNDB), AUL, Do not Disturb (CDND), Directory Number Hunting (DNH)***, and ***Call Wake Up (IWUC)*** upon subscriber actions which are ***activation, deactivation, interrogation,*** and ***customer usage***, where applicable. Crafts person operations via SERVORD are not supported.

This activity is implemented only for IBN lines and provides recording of the feature usage depending on the state of a new AMAOPTS option, which is created by this activity. When this option is ON, a new AMA record is generated and MC611 is appended to this AMA record to indicate the subscriber actions.

When the AMAOPTS option is set to ON and one of the requested features (*) is activated, deactivated, interrogated, or used by the end user, a separate billing record is generated immediately to indicate that user action. This billing record provides the following information within the described fields as below:

- **Feature Subscriber DN:** Stored in the Originating Open Digits 1 field of the Structure Code.
- **Date:** Stored in the Date field of the Structure Code
- **Time:** Stored in the Connect Time field of the Structure Code.
- **Feature Code:** Stored in the Service Identifier field of the module code MC611 context ID 80024
- **Action Type:** Stored in the Service Event field of the module code MC611 context ID 80024.

Note: * stands for the requested set of features which consists of Call Lock (ILR), Call Waiting (ICWT), Abbreviated Dialing (SCL), CLIR (SUPPRESS + CNDB), AUL, Do not Disturb (CDND), Directory Number Hunting (DNH), and Call Wake Up (IWUC).

Feature Subscriber DN represents the IBN line agent which uses the feature actions.

Date is the date at which the feature action is initiated.

Time is the time when the feature action is initiated.

Feature Code is used to represent each feature in the requested set by a feature ID uniquely.

Action Type is used to represent the feature action types which are usage, interrogation, subscriber activation, and subscriber deactivation.

The feature actions; activation, deactivation, interrogation, and usage are not applicable for all of the features in the requested set. A detailed description about which action applies to which feature is given in Table 1 - Feature Requirement List.

Table 5: Feature Requirement List

Feature Name	Feature Option	Act/Deact Billing	Interr. Billing	Feature Usage Billing	For Release
1) Abbreviated Dialing	IBN SCL	Y	Not requested	Y	ISN09
2) Call Waiting	CEPT ICWT	Not requested	Not requested	Y	ISN09
3) Hot Line	IBN AUL	Not requested	Not requested	Y	ISN09
4) Three Way Calling	CEPT I3WC	Not requested	Not requested	Y	Further Releases
5) Call Forwarding Immediately	CEPT CFU	Y	Not requested	Y	Further Releases
6) Call Forwarding on Busy	CEPT CFB	Y	Not requested	Y	Further Releases
7) Call Forwarding on No Answer	CEPT CFD	Y	Not requested	Y	Further Releases
8) Do Not Disturb	CEPT CDND	Y	Not requested	Y	ISN09
9) Call Wake Up	CEPT IWUC	Y	Not requested	Not requested	ISN09
10) Multiple Line Hunting	IBN DNH	Not requested	Not requested	Y	ISN09
11) Call Lock	CEPT ILR	Y	Not requested	Y	ISN09
12)CLIR/CNDBO	IBN SUPPRESS + CNDBO+CND	Not requested	Not requested	Y	Further Releases
Centrex Features					
CLIR	IBN SUPPRESS + CNDB	Not requested	Not requested	Y	ISN09
Call Transfer (CXR)	IBN CXR	Not requested	Not requested	Y	Further Releases
Call Hold Send the Music	IBN CHD	Not requested	Not requested	Y	Further Releases

1.1.1 Background

1.1.1.1 Existing AMA Record and MC611 Components Used in This Feature

In the existing billing framework, an AMA record consists of a base Structure Code and optional Module Codes containing specific information relevant to the call. If any information is necessary in addition to that contained in a base structure, this information is appended to the base structure in the form of module codes. (For detailed information about Structure Codes and Module Codes please refer to the NTP documents 297-1001-830 and 297-9051-800.) In this implementation, feature actions are recorded in the form of AMA billing records. The Feature Subscriber DN, Date, and Time info related to the feature action are stored in the base structure of the record. Whereas, Feature Code and Action Type are stored in MC611 with CCI_80024 and this module code is appended to the structure code. The fields of MC611 with CCI_80024 and an example structure code can be seen in Table 2 and Table 3.

Table 6: Structure Code 00514

Information	Number of BCD Characters
Record Descriptor Word	8
Hexadecimal Identifier	2
Structure Code	6
Call Type Code	4
Sensor Type	4
Sensor Identification	8
Recording Office Type	4
Recording Office Identification	8
Date	6
Timing Indicator	6
Study Indicator	8
Called Party Off-Hook	2
Service Observed, traffic sampled	2
Operator Action	2
Service Feature	4
Connect Time	8
Elapsed Time	10

Table 6: Structure Code 00514

Information	Number of BCD Characters
Significant Digits in Next Field	4
Originating Open Digits 1	12
Originating Open Digits 2	10
Originating Charge Information	4
Domestic/International Indicator	4
Significant Digits in Next Field	4
Ext terminating open digits 1	12
Ext terminating open digits 2	10
Completion Indicator	4
Module Code	

Table 7: MC611 with CCI_80024

BCD character	Meaning
1 - 12	Service Identifier Up to 6 EBCDIC characters
13 - 14	Service Event 00 = Unidentified 01 = Provisioning of service to line 02 = Removal of service from line 03 = Administration Programming 04 = Subscriber Programming 05 = Interrogation of Service 06 = Usage of service 07 = Subscriber Activation of Service 08 = Administration Activation of Service 09 = Subscriber Deactivation of Service 10 = Administration Deactivation of Service
15	Not used

Table 7: MC611 with CCI_80024

BCD character	Meaning
16	Sign (hex C)

MC611 with context identifier 80024 is the SUSB context and it is already used in MMP to provide Subscriber Usage Sensitive Billing. For instance, when the SOC option RBIL0005 and the SUSP option in Table AMAOPTS are ON, a billing record with MC611 is generated upon end user's activation of the SACB feature. SOC RBIL0005 must be ON to be able to use SUSB billing.

In this activity, a new AMAOPTS option named MC611_FOR_RFU (where RFU stands for **R**ecord **F**eature **U**sage) is created to control the recording of feature actions. Subscribers' feature actions are recorded only if the MC611_FOR_RFU option is set to ON. A brand new billing record is generated after the feature action is initiated. The Feature Subscriber DN, Date, and Time info are put in the Originating Open Digits 1, Date, and Connect Time fields of this record, respectively. After that, module code MC611 with CCI_80024 is generated. Feature Code and Action Type are put in the Service Identifier and Service Event fields of the MC611 and it is appended to the just created Structure Code.

In Figure 1, an example billing record with MC611 can be seen, which is created for the usage of the AUL.

Figure 1 Example view of the record taken with the CALLDUMP FULL command

```
>calldump ama full

*
HEX ID:                    AA
STRUCTURE CODE:                40514C
CALL CODE:                   006C      STATION PAID
SENSOR TYPE:                  036C      DMS 100F
SENSOR ID:                  0000000C
REC OFFICE TYPE:               036C      DMS 100F
REC OFFICE ID:               0000000C
DATE:                      50317C    MARCH 17, 2005
TIMING IND:
   TIMING GUARD FLAG            0        UNUSED
   SHORT CLD PARTY OFF-HOOK IND    0        UNUSED
   LONG DUR/SERV PTY CAPABILITY IND 0        UNUSED
   UNUSED                   0
   UNUSED                   0C
STUDY IND:
   STUDY TYPE A              0        UNUSED
   STUDY TYPE B              2        NETWORK COMPLETION
   STUDY TYPE C              0        UNUSED
   TEST CALL IND             0        UNUSED
   UNUSED                   0
   ORIG/TERM NANP NUM IND         0        UNUSED
   OPERATOR SERV IND            0C        UNUSED
CLD PTY OFF-HK:                0C        CLD OFF-HOOK DETECTED
SERVICE OBSERVED:              0C        NONE
OPER ACTION:                  0C        ANI, CUSTOMER DIALED CALL
SERVICE FEATURE:               000C      OTHER
SIG DIGITS NEXT FIELD:          010C
ORIG OPEN DIGITS 1:            01027835406C
ORIG OPEN DIGITS 2:           FFFFFFFFFF
ORIGINATING CHARGE INFO:         FFFF
DOMESTIC/INTL INDICATOR:         9C        UNKNOWN
SIG DIGITS NEXT FIELD:          000C
EXT TERM OPEN DIGITS 1:          000000000000000C
EXT TERM OPEN DIGITS 2:          FFFFFFFFFFFFFFFF
CONNECT TIME:                 1105378C   11:05:37.8
ELAPSED TIME:                000000000C 000000:00.0
COMPLETION INDICATOR:            001C      COMPLETED: ANSWERED
MODULE CODE:                  611C      GENERIC MOD: ONE DGT STR FMT
GENERIC CONTEXT ID:
   PARSE RULES               80024     UNKNOWN
   SIGNIFICANT DIGITS          00C       NIL
GENERIC DIGIT STRING ONE:        81A493000000060C
MODULE CODE:                  000C      FINAL MODULE
```

In this figure, Generic Digit String One is interpreted as below:

81A493000000060C

- First twelve characters serve as the Service Identifier
  "81" = a, "A4" = u, "93" = l ---> AUL
- The remaining six characters of the first twelve are represented with zeroes, since there are only three letters in the feature acronym.
- The next two characters, "06", represent the service event, which is usage here.

Generic Digit Strings for the features included in the requested set can be seen in Table 4.

Table 8: Generic Digit Strings

Feature	Service Identifier
AUL	81A493000000**XX**C
CDND	838495840000**XX**C
CNDB	839584820000**XX**C
DNH	849588000000**XX**C
ICWT	8983A6A30000**XX**C
ILR	899399000000**XX**C
IWUC	89A6A4830000**XX**C
SCL	A28393000000**XX**C
SUPPRESS	A2A497979985**XX**C

Note: The XX in the Digit String can be 1- 04 for Subscriber Programming, 2- 05 for interrogation, 3- 06 for usage, 4- 07 for Subscriber Activation, 5- 09 for Subscriber Deactivation as shown in Table 3.

1.1.2 Provisioning for Feature Recording

1.1.2.1 Office Wide Parameters:

1. To enable feature recording, the AMAOPTS option MC611_FOR_RFU, created by this activity to make feature recording optional, is set to ON.
2. To disable feature recording, MC611_FOR_RFU is set to OFF.

Figure 2 Provisioning of the new AMAOPTS option MC611_FOR_RFU

```
> Table AMAOPTS

OPTION SCHEDULE
---------------
MC611_FOR_RFU ON
>
```

1.1.2.2 Software Optionality Control

No new Software Optionality Control is created by this activity.

This activity implements a SUSB like recording of feature actions. SUSB can be summarized as DMS's ability to create a billing record per use of a feature action. The features can be billed based on activation, programming, deactivation, or usage. Module code 611 is appended to some of the structure codes during pay per use billing. It uses the context identifier 80024 which has been approved by Bellcore. The existing SOC option RBIL0005 - Subscriber Usage Sensitive Billing must be ON to generate SUSB records.

1.2 Hardware Requirements or Dependencies

No new customer hardware requirements or dependencies are introduced in this feature.

1.3 Software Requirements or Dependencies

This feature uses the existing AMA/Billing framework and the existing components of this framework.

1.4 Limitations and Restrictions

- This activity is implemented for the requested set of features described in Section 2.2 only. Subscriber actions that are not compatible with these features are not supported.
- The functionality provided by this activity applies to IBN lines only.
- Crafts person actions via SERVORD are not recorded. A feature action is recorded only if it is initiated by the subscriber.
- A feature action is recorded only if it is applicable to the related feature. Applicability of actions to features can be seen in Table 1.
- In order to record a feature action in a billing record:
  - — all the datafill described in Section 2.2.2 must be performed
  - — the feature must be contained in the required set of features
- All limitations which apply to features in the existing implementation (e.g. feature compatibility, precedence, etc.) apply to this activity, as well.

- All features are activated/deactivated/programmed according to CEPT rules (for non CEPT features CEPTONCENTREX is datafilled in Table ISERVOPT).
- Subscriber feature actions are not recorded if the related feature is not assigned to the line or if it is not a default feature (i.e. trying to activate/deactivate/use a feature even if it does not exist on the line)
- A subscriber feature action is recorded only if it results in success:
  - If a feature subscriber wants to activate a feature which is not compatible with one or more features already assigned to the line and that is why the activation action is not successfully ended, this action is not recorded.
  - If a feature subscriber tries to activate an already active feature or deactivate an already inactive feature, this action is not recorded.
- ICWT usage is recorded only if the ICWT subscriber puts in hold or disconnects the active agent and accepts the new calling agent after he gets the ICWT tone.
- The pilot DN is written into the Originating Open Digits1 for DNH usage.
- SUPPRESS usage is recorded only if the SUPPRESS_DN field is 'Y' (SUPPRESS_DN is given through SERVORD action during feature assignment and can be checked via QDN command).
  - If the state of SUPPRESS is toggled using CNDB (i.e. SUPPRESS_DN becomes 'N') for a specific call, CNDB usage is recorded as feature action. SUPPRESS usage is not recorded for that case.
  - If SUPPRESS is not assigned to the line or SUPPRESS_DN field is set to 'N' and CNDB is used for a specific call, CNDB usage is recorded as feature action.

1.5 Interactions

- If a user originated feature action is perceived, this action is recorded in a billing record.
- AMA in MMP is based on Bellcore AMA Format. This feature uses the existing AMA/Billing framework components with no change in their existing structures to realize customer's requirements. So, there is no effect on the existing AMA subsystem in the MMP load.

1.6 Applicable customer facing sections

Fault Management

Logs	N/A

Alarms	N/A
Configuration	
Data Schema	N/A
User Interface	N/A
Element Management	N/A
Security	N/A
Service Order	N/A
Office Parameters	Y
Accounting (includes AMA billing)	Y
Performance (includes operational measurements)	N/A

1.7 Glossary

Term	Description
AMA	Automatic Message Accounting
AUL	Automatic Line
CCI	Call Code Index
CDND	CEPT Do not Disturb
CEPT	Conference of European Posts and Telecommunications Administration
CLIR	Calling Line Identification Restriction
CNDB	Calling Number Delivery Blocking
DIRP	Device Independent Recording Package
DMS	Digital Multiplex System
DNH	Directory Number Hunting
FPE	Feature Processing Environment
ICWT	International Call Waiting
ILR	International Line Restriction
IWUC	International Wake Up Call
MCI	Module Code Index
MMP	Multi Market Product
SCI	Structure Code Index

Term	Description
SCL	Speed Calling Long
SOC	Software Optionality Control
Telco	Telecom Company

1.8 Recommended Reading/References

a. NTP 297-9051-800 ‘DMS100 MMP AMA Reference Guide’

b. NTP 297-1001-830 ‘Bellcore Format Automatic Message Accounting Message Guide’

c. NTP 297-9051-855 Office Parameters Volume 1 0f 3 (OFCENG)

d. 297-9051-351 Data Schema Reference Manual Volume 8 0f 12

2: Configuration for A00009145

2.1 Hardware and Software Requirements

No new software and hardware requirements.

2.2 Initial Configuration

To generate a billing record for subscriber’s feature usage, the option MC611_FOR_RFU in Table AMAOPTS must be set to ON.

2.3 Office/Subnet parameters (OP/SP) (CM & SESM)

Not applicable.

2.4 Upgrade Considerations

None.

2.5 Data schema (DS) (CM, MIBS, RDB)

2.5.1 New/modified tables, MIBs, or Database Schema

Table 1 New or modified tables

Table name	NEW/CHANGED/ or DELETED/	Table Control (NEW/OLD/UNCHANGED)
AMAOPTS	CHANGED (A new option is defined)	UNCHANGED

2.5.2 Table/MIB/Remote Database Schema information

A new option named MC611_FOR_RFU is created in Table AMAOPTS. This option is set to ON to activate the feature. The default value is OFF for this option.

While activating and deactivatingMC611_FOR_RFU , a warning is printed as given below to indicate the change in the functionality:

For activation (ON state):

```
"This change results feature action recording

upon subscriber feature actions."
```

For deactivation (OFF state):

```
"This change prevents feature action recording

upon subscriber feature actions."
```

2.5.2.1 Datafill example

Figure 1 New AMA option MC611_FOR_RFU in Table AMAOPTS

```
TABLE: AMAOPTS
OPTION SCHEDULE
---------------
...
MC611_FOR_RFU ON
...
```

Figure 2 Activating/deactivating the new option MC611_FOR_RFU

```
>table amaopts
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: AMAOPTS
>pos mc611_for_rfu
MC611_FOR_RFU ON
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: ON
>off
TUPLE TO BE CHANGED:
MC611_FOR_RFU OFF
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
This change prevents feature action recording
upon subscriber feature actions.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
>
>dis
MC611_FOR_RFU OFF
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: OFF
>on
TUPLE TO BE CHANGED:
MC611_FOR_RFU ON
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
This change results feature action recording
upon subscriber feature actions.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
```

2.5.2.2 Functional description

This ISN09 activity is targeted to provide recording of the subscriber initiated feature actions in the form of AMA billing records.

It is required that this capability is able to be turned off and on. Therefore, a new AMAOPTS option, MC611_FOR_RFU, is created. When this option is set to ON, a billing record is created for the feature actions (Please refer to the FN document for the list of supported features and actions) initiated by subscribers. Otherwise, the billing flow is not impacted.

2.6 Service Orders (SO) (CM & SESM)

Not applicable.

2.7 Software optionality control (SOC)

Not applicable.

2.8 Element Management

Not applicable.

2.9 Security

Not applicable.

3: Accounting for A00009145

3.1 Accounting strategy

This activity provides detailed information about the subscribers' feature actions at the billing records.

In the existing billing framework, an AMA record consists of a base Structure Code and optional Module Codes containing specific information relevant to the call. If any information is necessary in addition to that contained in a base structure, this information is appended to the base structure in the form of module codes. (For detailed information about Structure Codes and Module Codes please refer to the NTP documents 297-1001-830 and 297-9051-800.)

This feature uses the existing AMA/Billing framework based on the Bellcore AMA Format. Feature actions are recorded in the form of AMA billing records. The Feature Subscriber DN, Date, and Time info related to the feature action are stored in the base structure of the record. Whereas, Feature Code and Action Type are stored in MC611 with CCI_80024 and this module code is appended to the structure code.

MC611 with context identifier 80024 is the SUSB context and it is already used in MMP to provide Subscriber Usage Sensitive Billing. For instance, when the SOC option RBIL0005 and the SUSP option in Table AMAOPTS are ON, a billing record with MC611 is generated upon end user's activation of the SACB feature. SOC RBIL0005 must be ON to be able to use SUSB billing.

In this activity, a new AMAOPTS option named MC611_FOR_RFU (where RFU stands for **R**ecord **F**eature **U**sage) is created to control the recording of feature actions. Subscribers' feature actions are recorded only if the MC611_FOR_RFU option is set to ON. A brand new billing record is generated after the feature action is initiated. The Feature Subscriber DN, Date, and Time info are put in the Originating Open Digits 1, Date, and Connect Time fields of this record, respectively. After that, module code MC611 with CCI_80024 is generated. Feature Code and Action Type are put

in the Service Identifier and Service Event fields of the MC611 and it is appended to the just created Structure Code.

Figure 1 Example view of the record taken with the CALLDUMP FULL command

```
>calldump ama full

*
HEX ID:                        AA
STRUCTURE CODE:                   40514C
CALL CODE:                     006C      STATION PAID
SENSOR TYPE:                   036C      DMS 100F
SENSOR ID:                    0000000C
REC OFFICE TYPE:               036C      DMS 100F
REC OFFICE ID:                0000000C
DATE:                         50317C    MARCH 17, 2005
TIMING IND:
   TIMING GUARD FLAG             0       UNUSED
   SHORT CLD PARTY OFF-HOOK IND  0       UNUSED
   LONG DUR/SERV PTY CAPABILITY IND 0    UNUSED
   UNUSED                     0
   UNUSED                     0C
STUDY IND:
   STUDY TYPE A                  0       UNUSED
   STUDY TYPE B                  2       NETWORK COMPLETION
   STUDY TYPE C                  0       UNUSED
   TEST CALL IND                 0       UNUSED
   UNUSED                     0
   ORIG/TERM NANP NUM IND        0       UNUSED
   OPERATOR SERV IND             0C      UNUSED
CLD PTY OFF-HK:                  0C      CLD OFF-HOOK DETECTED
SERVICE OBSERVED:                0C      NONE
OPER ACTION:                    0C       ANI, CUSTOMER DIALED CALL
SERVICE FEATURE:                000C     OTHER
SIG DIGITS NEXT FIELD:           010C
ORIG OPEN DIGITS 1:              01027835406C
ORIG OPEN DIGITS 2:             FFFFFFFFFF
ORIGINATING CHARGE INFO:         FFFF
DOMESTIC/INTL INDICATOR:         9C      UNKNOWN
SIG DIGITS NEXT FIELD:           000C
EXT TERM OPEN DIGITS 1:          000000000000000C
EXT TERM OPEN DIGITS 2:          FFFFFFFFFFFFFFFF
CONNECT TIME:                   1105378C  11:05:37.8
ELAPSED TIME:                 000000000C 000000:00.0
COMPLETION INDICATOR:            001C     COMPLETED: ANSWERED
MODULE CODE:                    611C     GENERIC MOD: ONE DGT STR FMT
GENERIC CONTEXT ID:
   PARSE RULES                 80024     UNKNOWN
   SIGNIFICANT DIGITS           00C      NIL
GENERIC DIGIT STRING ONE:       81A493000000060C
MODULE CODE:                    000C     FINAL MODULE
```

In this figure, Generic Digit String One is interpreted as below:

81A493000000060C

- First twelve characters serve as the Service Identifier
  "81" = a, "A4" = u, "93" = l ---> AUL
- The remaining six characters of the first twelve are represented with zeroes, since there are only three letters in the feature acronym.
- The next two characters, "06", represent the service event, which is usage here.

Figure 2 New AMA option MC611_FOR_RFU in Table AMAOPTS

```
TABLE: AMAOPTS
OPTION SCHEDULE
---------------
...
MC611_FOR_RFU ON
...
```

Figure 3 Activating/deactivating the new option MC611_FOR_RFU

```
>table amaopts
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
TABLE: AMAOPTS
>pos mc611_for_rfu
MC611_FOR_RFU ON
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: ON
>off
TUPLE TO BE CHANGED:
MC611_FOR_RFU OFF
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
This change prevents feature action recording
upon subscriber feature actions.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
>
>dis
MC611_FOR_RFU OFF
>cha
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
AMASEL: OFF
>on
TUPLE TO BE CHANGED:
MC611_FOR_RFU ON
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
This change results feature action recording
upon subscriber feature actions.
TUPLE CHANGED
JOURNAL FILE INACTIVE
>
```

3.2 CM billing changes

3.2.1 Structure codes

No new structure code is created by this feature. No changes are made to the existing structure codes.

3.2.2 Module code

No new module code or context identifier is created by this feature. No changes are made to the existing module codes.

3.2.3 Tables (fields)

No fields are created/changed.

3.3 Other changes

None.

Product = World Trade

A00009216 -- JI-ISUP to Base ETSI ISUP V2 Mapping Enhancement

1: Applicable solution(s)

Int'l DMS

1.1 Description

This activity provides an optionality to pass some ISUP parameters unchanged for the JI-ISUP to Base ETSI ISUP V2 interworking. Followings are the parameters to be mapped unchanged:

- Nature of Address (NOA) in Calling Party Number
- ISUP Preference Indicator in Forward Call Indicator
- Calling Party Category value 'calling subscriber with priority'

This feature is optional with a new controlled SOC option. When the state of this SOC option is ON, feature becomes active, otherwise system behaves as it was before this functionality.

This feature will be available in TDM offices in ISN09 and later releases on DMS100 MMP.

1.2 Current Behavior

1.2.1 NOA of Calling Party Number

In current behavior, Nature of Address of the Calling Party Number is always set to NATL without checking the received value for JI-ISUP to Base ETSI V2 ISUP interworking. Refer to the following table for current mapping of the NOA.

Table 1 Current NOA Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Param-eter	**Field**	**Field Value**		**Field Value**	**Field**	**Param-eter**
Calling Party Number	Nature of Address Indicator	0000000 - spare	?	0000011 - All values are mapped to National	Nature of Address Indicator	Calling Party Number
		0000001 - Subscriber number				
		0000010 - Reserved for national use				
		0000011 - National number				
		0000100 - International number				
		0000101 - 1101111 spare				
		1110000 - 1111101 reserved for national use				
		1111110 - peculiar number of network				
		1111111				

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

1.2.2 ISUP Preference Indicator in Forward Call Indicator

The current behavior of mapping ISUP Preference Indicator for JI-ISUP to Base ETSI V2 ISUP interworking is as follows:

1. If there are any supplementary services in the received IAM (ATP, UUI, CLIP) then set the outgoing ISUP Preference Indicator to 'ISUP Preferred All The Way'.
2. If the condition in item 1 is not met, and the BC received in the TMR/USI combination is set to Speech or 3_1_kHz_Audio, then set the outgoing ISUP Preference Indicator to 'ISUP Not Required All The Way'.
3. If the conditions in item 1 and item 2 are not met, then set the outgoing ISUP Preference Indicator to 'ISUP Preferred All The Way'.

If the received ISUP Preference Indicator value is 'Spare', the Protocol_Error treatment is set and call goes to treatment.

Refer to the following table for current mapping of the PI.

Table 2 Current ISUP PI Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Param-eter	**Field**	**Field Value**		**Field Value**	**Field**	**Param-eter**
Forward Call Indicator	ISDN User Part Preferenc e Indicator	00 - ISDN user part preferred all the way	?	Refer to the table immediately below.	ISDN User Part Preferenc e Indicator	Forward Call Indicator
		01 - ISDN user part not required all the way				
		10 - ISDN user part required all the way				
		11 - Spare				

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

Table 3 ISUP Preference Indicator Parameter Coding

Information Field	**JI-ISUP V.2-->**	**--> ETSI v2**	**JI-ISUP V.2-->**	**--> ETSI v2**
Supplementary Service	**None (No UUI, ATP or CLIP present in the IAM)**		**Any (UUI, ATP and/or CLIP present in the IAM)**	
(Applies to messages: IAM)	**Bits**	**Bits**	**Bits**	**Bits**
ISUP Preferred	HG	HG	HG	HG
For Bearer Service = Speech	00	01	00	00
For Bearer Service = 3.1kHz Aud.	00	01	00	00
For Bearer Service = 64k Unres.	00	00	00	00
For Bearer Service = Other	00	00	00	00
ISUP Not Required All The Way	HG	HG	HG	HG
For Bearer Service = Speech	01	01	01	00
For Bearer Service = 3.1kHz Aud.	01	01	01	00
For Bearer Service = 64k Unres.	01	00	01	00
For Bearer Service = Other	01	00	01	00

Information Field	JI-ISUP V.2-->	--> ETSI v2	JI-ISUP V.2-->	--> ETSI v2
Supplementary Service	None (No UUI, ATP or CLIP present in the IAM)		Any (UUI, ATP and/or CLIP present in the IAM)	
(Applies to messages: IAM)	Bits	Bits	Bits	Bits
ISUP Required All The Way	HG	HG	HG	HG
For Bearer Service = Speech	10	01	10	00
For Bearer Service = 3.1kHz Aud.	10	01	10	00
For Bearer Service = 64k Unres.	10	00	10	00
For Bearer Service = Other	10	00	10	00
Spare	HG	HG	HG	HG
For Bearer Service = Speech	11	01	11	00
For Bearer Service = 3.1kHz Aud.	11	01	11	00
For Bearer Service = 64k Unres.	11	00	11	00
For Bearer Service = Other	11	00	11	00

1.2.3 ISUP Calling Party Category

In existing behavior, Calling Party Category value ‘calling subscriber with priority’ is mapped as CPC Unknown for JI-ISUP to Base ETSI ISUP V2 interworking. Refer to the following table for current mapping of Calling Party Category.

Table 4 Current CPC Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Parameter	**Field**	**Field Value**		**Field Value**	**Field**	**Parameter**
Calling Party Category		00000000 - calling party's category unknown 00000001 - spare 00000010 - spare 00000011- spare 00000100 - spare 00000101 - spare 00000110 - By mutual agreement 00000111 - By mutual agreement 00001000 - By mutual agreement	?	00000000 - CPC Unknown	Calling Party Category	
		00001001 - national operator desk		00000000 - CPC Unknown		
		00001010 - ordinary calling subscriber		00001010 - ordinary calling subscriber		
		00001011 - calling subscriber with priority		00000000 - CPC Unknown		
		00001100 - data call		00000000 - CPC Unknown		
		00001101 - test call		00001101 - test call		
		00001111 - payphone		00001111 - payphone		
		00010000 - 11110000 spare		00000000 - CPC Unknown		
		11110001 - 11111110 reserved for national use		00000000 - CPC Unknown		
		11111111 - spare		00000000 - CPC Unknown		

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

1.3 Desired Behavior

1.3.1 Activation of the feature

Activation of the functionality is controlled by the new SOC option NETK00XX-"NETK Jpn I ISUP Parm Enh".

NETK Jpn I ISUP Parm Enh is a controlled SOC and it has two states, ON and IDLE. Default state of *NETK Jpn I ISUP Parm Enh* is IDLE. When its state is ON, this feature becomes functional.

Table 5 SOC for Activation of Feature

SOC group:	NETK

SOC option name:	NETK Jpn I ISUP Parm Enh
SOC option title:	NETK Jpn I ISUP Parm Enh
SOC option control type:	state
New SOC option?	Yes
SOC option order code	NETK0087
Option defined in DRU:	WT22
Affected products:	ISN09

1.3.2 NOA of Calling Party Number

This activity provides an optionality to pass the value of NOA in calling party number as unchanged to the Base ETSI ISUP V2 for the JI-ISUP to Base ETSI ISUP V2 interworking. In order to achieve this, the implementation will be made optional by new created SOC option.

The NOA values used in JI-ISUP are

- NATL (0000011)
- INTL (0000100)
- Peculiar Number (1111110)

Peculiar Number is a national use value and it is not supported in ETSI ISUP.

After the state of the new SOC option is changed to ON, and if the received NOA value is NATL or INTL, then received value is transparently passed to the Base ETSI ISUP V2. If the received value is Peculiar Number or any other value, then outgoing NOA of Calling Party Number is set to NATL.

If the state of the new SOC option is IDLE, then by default, the current behavior will be kept as described in “NOA of Calling Party Number” under Current Behavior.

Table 6 Desired NOA Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Param-eter	Field	Field Value		Field Value	Field	Param-eter
Calling Party Number	Nature of Address Indicator	0000000 - spare	?	0000011 - National number	Nature of Address Indicator	Calling Party Number
		0000001 - Subscriber number		0000011 - National number		
		0000010 - Reserved for national use		0000011 - National number		
		0000011 - National number		0000011 - National number		
		0000100 - International number		0000100 - International number		
		0000101 - 1101111 spare		0000011 - National number		
		1110000 - 1111101 reserved for national use		0000011 - National number		
		1111110 - peculiar number of network		0000011 - National number		
		1111111		0000011 - National number		

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

1.3.3 ISUP Preference Indicator of Forward Call Indicator

The existing behavior is modified not to send the call to the treatment when the received ISUP preference indicator value is 11-Spare. If received ISUP preference indicator value is ‘11-spare’, it is mapped as in “Table 3 ISUP Preference Indicator Parameter Coding” on page 2341 for JI-ISUP to Base ETSI V2 ISUP interworking:

1. If there are any supplementary services in the received IAM (ATP, UUI, CLIP) then set the outgoing ISUP Preference Indicator to ’ISUP Preferred All The Way’.
2. If the condition in item 1 is not met, and the BC received in the TMR/USI combination is set to Speech or 3_1_kHz_Audio, then set the outgoing ISUP Preference Indicator to ’ISUP Not Required All The Way’.
3. If the conditions in item 1 and item 2 are not met, then set the outgoing ISUP Preference Indicator to ’ISUP Preferred All The Way’.

This changing on the current behavior is in effect when the new created SOC option state is IDLE.

Also with this activity, the received ISUP Preference Indicator is tranparently passed to the Base ETSI ISUP V2 for the JI-ISUP to Base ETSI ISUP V2

interworking. This behavior is optional. In order to achieve this, the implementation will be made via new created SOC option.

The ISUP Preference Indicator values used in JI-ISUP are

- ISUP Preferred All The Way (00)
- ISUP Not Required All The Way (01)
- ISUP Required All The Way (10)

If the received ISUP Preference Indicator value is one of the above, and the state of the new SOC option is ON, then received value is passed unchanged for JI-ISUP to Base ETSI ISUP V2 interworking. If the received value is 'spare (11)', then it is mapped as '00-ISUP Preferred All The Way' when the new SOC option state is ON.

Table 7 Desired ISUP PI Mapping - JI-ISUP to Base ETSI ISUP V2 i/w

JI-ISUP IAM			dir	Base ETSI ISUP V2 IAM		
Param-eter	Field	Field Value		Field Value	Field	Param-eter
Forward Call Indicator	ISDN User Part Preference Indicator	00 - ISDN user part preferred all the way	?	00 - ISDN user part preferred all the way	ISDN User Part Preference Indicator	Forward Call Indicator
		01 - ISDN user part not required all the way		01 - ISDN user part not required all the way		
		10 - ISDN user part required all the way		10 - ISDN user part required all the way		
		11 - Spare		00 - ISDN user part preferred all the way		

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

If the state of this SOC option is IDLE, then by default, the current behavior will be kept as described in Please refer to Section "1.2.2 ISUP Preference Indicator in Forward Call Indicator" on page 2340. except the received ISUP Preference Indicator value is '11-spare'.

1.3.4 ISUP Calling Party Category

This activity also provides an optionality to transparently pass the calling party category value 'Calling subscriber with priority' to the Base ETSI ISUP V2 for the JI-ISUP to Base ETSI ISUP V2 interworking. In order to achieve this, the implementation will be made optional via new created SOC option.

If the state of this SOC option is not ON, then by default the current behavior will be kept as described in "ISUP Calling Party Category."

After the state of the SOC option is changed to ON, CPC value 'Calling subscriber with priority (00001011)' will be passed as received from the JI-ISUP side for the JI-ISUP to Base ETSI ISUP V2 interworking.

Table 8 Desired CPC Mapping - JI-ISUP to ETSI ISUP V2 i/w

JI-ISUP IAM			dir	ETSI ISUP V2 IAM		
Parameter	**Field**	**Field Value**		**Field Value**	**Field**	**Parameter**
Calling Party Category		00000000 - calling party's category unknown 00000001 - spare 00000010 - spare 00000011- spare 00000100 - spare 00000101 - spare 00000110 - By mutual agreement 00000111 - By mutual agreement 00001000 - By mutual agreement	?	00000000 - CPC Unknown	Calling Party Category	
		00001001 - national operator desk		00000000 - CPC Unknown		
		00001010 - ordinary calling subscriber		00001010 - ordinary calling subscriber		
		00001011 - calling subscriber with priority		00001011 - calling subscriber with priority		
		00001100 - data call		00000000 - CPC Unknown		
		00001101 - test call		00001101 - test call		
		00001111 - payphone		00001111 - payphone		
		00010000 - 11110000 spare		00000000 - CPC Unknown		
		11110001 - 11111110 reserved for national use		00000000 - CPC Unknown		
		11111111 - spare		00000000 - CPC Unknown		

Note : The values in shaded cells are the values that are not supported by the JI-ISUP protocol.

1.4 Hardware Requirements or Dependencies

None

1.5 Software Requirements or Dependencies

To make this new feature functional, new controlled SOC option NETK0087 is used. Since the SOC state will be IDLE after ONP completed, it must be changed to ON manually to make the feature functional.

1.6 Limitations and restrictions

None

1.7 Interactions

This feature is effective in the scenarios below:

1. call forwarding (when the received call over JI-ISUP is forwarded to another agent over Base ETSI ISUP V2)
2. Carrier Name Notification (CNN) feature

automatically without making any extra implementation.

The NOA value of the outgoing IAM message can be changed with the datafills and features below:

3. EDITCLI option in table TRKSGRP
4. Serving Country Code (SCC) feature

With this activity, those are still be active on the outgoing Base ETSI ISUP V2 trunk without making any new implementation.

1.8 Glossary

Term	Description
ATP	Access Transport Parameter
BC	Bearer Capability
CLIP	Calling Line Identification Presentation
CPC	Calling Party Category
DMS	Digital Multiplex System
IAM	Initial Address Message
MMP	Multi Market Product
NOA	Nature Of Address
ONP	One Night Process
PI	Preference Indicator
SOC	Software Optionality Control
TMR	Transmission Medium Requirement
USI	User Service Information
UUI	User to User Information

1.9 Recommended Reading/References

a. SIM Specification: Japan Interconnect ISUP DMS/CS2000 Implementation: Interworking Specification

b. ITU-T Recommendation Q763 : Signalling System No.7 - ISDN User Part Formats and Codes

c. A59034248 - Japon Interconnect ISUP Carrier Name Notification for Carrier Designation

d. A59023331 - Serving Country Code

Product = World Trade

A00009321 -- NMC Code Blocking

1: Applicable solution(s)

Int'l IAW

1.1 Description

1.1.1 Introduction

This feature is to enhance the Mass Call function on the CS2Kc system.

GAP is a existing hidden CBK option which is the time interval between completed calls. In Code Blocking feature, another CBK option PCT is provided. Within the implementation of this activity, following will be covered:

- *Percentage* (PCT) is a CBK option which allows calls to be blocked from proceeding based upon the destination code (digits). Calls can be blocked by a specified percentage, ranging from 1 to 100. Blocked calls can have one of three possible treatments applied: NCA, EA1, or EA2.

Whether a CBK control should be applied only depends on the destination digits. It does not care if the call agent is line or any kind of trunk.

1.1.2 Block calls with the percentage

The Code Blocking control provides a means to block calls from progressing further into the Network. Because the route taken by a call is determined by the destination code, the control provides a means to limit traffic over particular routes.

A certain percentage(between 1 and 100 percent) can be defined in PCT option and the specified percentage of calls should be blocked based on the preset destination code.

Calls which are blocked from proceeding further into the Network can be sent to one of three possible treatments:

- No Circuit Announcement (NCA);
- Emergency Announcement 1 (EA1); or
- Emergency Announcement 2 (EA2).

1.1.3 PCT option is available in MASSCALL command

MASSCALL command is implemented to List/Apply/Remove mass call control. PCT is available in MASSCALL command as a CBK option.

Following are some examples:

Example 1

```
MASSCALL APPLY CBK PCT PX CSXLA '8308001' '8308004'
60 NCA
```

In this example, only 40 percent of calls which enters:

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with called party digits starting in range from ’8308001’ to ’8308004’

will be allowed to complete, all other calls will be sent to NCA treatment.

Example 2

```
MASSCALL APPLY CBK GAP PX CSXLA '8308001' '8308004'
'60.0' NCA
```

In this example, only one call per 60 seconds which enters:

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be allowed to complete, all other calls will be sent to NCA treatment.

Example 3

```
MASSCALL LIST CBK PCT PX CSXLA ALL
```

In this example, all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be listed.

Example 4

```
MASSCALL LIST CBK GAP PX CSXLA ALL
```

In this example, all the gap code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be listed.

Example 5

```
MASSCALL REMOVE CBK PCT PX CSXLA '8308001' '8308004'
```

In this example, the percentage code blocking control which enters

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be removed.

Example 6

```
MASSCALL REMOVE CBK GAP PX CSXLA '8308001' '8308004'
```

In this example, the gap code blocking control which enters

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’

will be removed.

1.1.4 PCT option is available in MAPCI commands

PCT is available in MAPCI commands as a CBK option. Direct access to the CodeCtrl menu level is from the Command Interpreter (CI) level by entering the commands “MAPCI;NWM;CODECTRL”. This level can also be entered indirectly by selecting the appropriate menu item until the desired level is reached.

CodeCtrl commands are to List, Apply and Remove code controls.The PCT option is available in these code control commands.

Followings are some examples:

Example 1

```
APPLY CBK PCT PX CSXLA '8308001' '8308004' 60 NCA
```

In this example, only 40 percent of calls which enters:

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with called party digits starting in range from ’8308001’ to ’8308004’

will be allowed to complete, all other calls will be sent to NCA treatment.

Example 2

```
APPLY CBK GAP PX CSXLA '8308001' '8308004' '60.0' NCA
```

In this example, only one call per 60 seconds which enters:

1. UXLA with an XLASYS of PX

2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’ will be allowed to complete, all other calls will be sent to NCA treatment.

Example 3

```
LIST CBK PCT PX CSXLA ALL
```

In this example, all the percentage code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be listed.

Example 4

```
LIST CBK GAP PX CSXLA ALL
```

In this example, all the gap code blocking controls that applied which enters UXLA with an XLASYS of PX and an XLANAME of CSXLA will be listed.

Example 5

```
REMOVE CBK PCT PX CSXLA '8308001' '8308004'
```

In this example, the percentage code blocking control which enters

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’ will be removed.

Example 6

```
REMOVE CBK GAP PX CSXLA '8308001' '8308004'
```

In this example, the gap code blocking control which enters

1. UXLA with an XLASYS of PX
2. XLANAME of CSXLA with digits starting in range from ’8308001’ to ’8308004’ will be removed.

1.1.5 TRAVER routines

A new message is created to be displayed if PCT option is activated while doing TRAVER which is as following:

- ‘A Mass Call Code Block Control with percentage may affect this call.’

The message which is displayed if GAP option is activated while doing TRAVER is also modified to indicate that this condition is encountered. Following is the message:

- ‘A Mass Call Code Block Control with gapping may affect this call.’

A TRAVER example of a call encountering a PCT Code Blocking Control is shown in Figure 1.

Figure 1 TRAVER example displaying Mass Call warning message

```
>traver l 8306007 8306008 b
TABLE IBNLINES
LG 00 1 00 06 0 DT STN IBN 8306007 CSGRPA 0 0 131 $
.....

TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE IBNXLA: XLANAME CSXLA
CSXLA 830 NET N N 0 N CSDIG Y Y DOD N CSIDXA CSGRPA CS_NIL NONE $
TABLE DIGCOL
TUPLE NOT FOUND
Default is RPT
TABLE LINEATTR
CSIDXA IBN DAT1 NT 0 0 NILSFC 0 PX CSXLA TESTTONE 00 CSGRPA CS_NIL $
LCABILL OFF - BILLING DONE ON BASIS OF CALLTYPE
TABLE XLAPLAN
CSGRPA NSCR 131 NPRT NONE N $ $
TABLE RATEAREA
CS_NIL NLCA NIL NILLATA $
NOTE: A Mass Call Code Block Control with percentage may affect this call.
TABLE PXHEAD
CSXLA SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          8306008
TABLE PXCODE
CSXLA 83060 83060 CONT ( MM 7 7) ( XLT PX CSTERM)$
TABLE PXHEAD
CSTERM SDFLT NODFOP NOCON F
THE DIGITS USED TO INDEX THE NEXT TABLE ARE:                          8306008
TABLE PXCODE
CSTERM 830 830 DNRTE ( CLASS NATL) ( DN 131 830)$

.....
```

1.2 Hardware Requirements or Dependencies

No hardware dependency.

1.3 Software Requirements or Dependencies

None.

1.4 Limitations and restrictions

Please refer to the activity AU3395-Mass Call Control FN document for limitations and restrictions as there are no new restrictions are added by this feature to the functionality.

The ‘MM’ option in translation allows the possibility of creating an “unreachable” Mass Call Control tuple. (i.e. A Mass Call tuple with more digits than the Min value of the associated call's translations.) This attempt at setting a Mass Call Control is unreachable and could never be exercised. To avoid this issue, the minimum value in ‘MM’ should be datafilled not less than the digits in the masscall control code.

The Pass and Block counters are reset to 0 when they reach the maximum value 65536.

1.5 Interactions

This feature is a enhancement of Mass Call Control feature. A new CBK option PCT is implemented to provide the function to block calls with percentage based upon destination digits. This feature does not extend the capacity of the Code block control. The sum of CBK, PRP and HTRF entries still can not exceed 256.

1.6 Glossary

Term	Description
CBK	Code Blocking
PCT	Code Blocking with percentage
GAP	Code Blocking with gapping
TRAVER	Translation verification

1.7 References

1. AU3395 - Mass Call Control
2. 2990 - RFF - CHT NMC Code Blocking RFF v2

Product = World Trade

A00009322 -- Call Lock and Do Not Disturb Enhancements

Functional Description

1: Applicable solution(s)

Int'l IAW

1.1 Call Lock

1.1.1 Introduction

CEPT ILR feature gives the administrator the capability to restrict outgoing calls for the subscriber according to the predefined restriction classes. The administrator can assign, de_assign, activate or deactivate this feature on a line via Service Order or assign and de_assign the feature by using the default

option functionality. Subscribers are able to activate, deactivate or interrogate ILR feature by dialing access codes.

The following enhancements are provided by this activity over existing Call Lock Feature:

- To support dial tone during the deactivation procedure.The user can originate a new call directly after the successful deactivation without going on hook.
- To allow class of restriction to be overwritten by new entry without doing a feature deactivation.
- To allow the user to change the password according to the required dialing sequence LH DT*SC*PWO*PWN#CT. The password is 4 digits.
- To generate report and disallow any feature modification (activation, deactivation, change) until the following day upon 3 times of wrong password entry in succession, or until the administration by operator. The following day is the time after the next 00:00 midnight. The 3 times is the value of field MAX_PIN_RETRY which is datafilled in CEPTPW tuple of table ISERVOPT. The password is 4 digits.

1.1.2 General Considerations

These enhancements are provided for IBN lines. There are some prerequisites to implement these enhancements which are:

- For the first two enhancements the subscriber should assigned ILR option.
- For the last two enhancements the subscriber should assigned CEPTPW option.

For the assignment of ILR and CEPTPW option, please refer to References 1,2,3.

1.1.3 To support dial tone during the deactivation procedure

The subscriber will hear dial tone instead of confirm tone when deactivating the ILR successfully, and the subscriber can originate a new call directly after the successful deactivation without going on hook.

Dial tone is optional and determined according to the field ALLOW_ORIG_AFTER_DEACT of ILRCLS tuple in table ISERVOPT.

- ALLOW_ORIG_AFTER_DEACT {BOOLEAN}: indicates that the dial tone will be generated or confirm tone will be generated. If it is set as ‘Y’, dial tone is generated and the user can originate a new call directly after the successful deactivation without going on hook. Otherwise, confirm tone is generated. The default value for the field is ‘N’.

Figure 1 :The View of CEPT_FTR_DIALTONE tuple in ISERVOPT table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ilrcls
OPTION:
>ilrcls
ILR_PROG:
>n
SDT:
>n
CR_PSWD:
>y
SHOW_CHG_PSWD:
>y
ALLOW_ORIG_AFTER_DEACT:
>y
OVERRIDE_ILR_CLASS:
>y
TUPLE TO BE ADDED:
            ILRCLS ILRCLS N N Y Y Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

1.1.4 To allow class of restriction to be overwritten by new entry without doing a feature deactivation

The subscriber can overwrite the class of restriction when activating the ILR option without doing a ILR deactivation first by using the following dialing sequence:

LH DT*SC*PW*CR#CT

This enhancement is optional and determined according to the field OVERRIDE_ILR_CLASS of ILRCLS tuple in table ISERVOPT.

- OVERRIDE_ILR_CLASS{BOOLEAN}: indicates whether the user can overwrite the class of restriction when activating the ILR option without doing a ILR deactivation first or not. If it is set as ‘Y’, the user can overwrite the class of restriction, otherwise can’t. The default value for the field is ‘N’.

Figure 2 The view of ILRCLS Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ilrcls
OPTION:
>ilrcls
ILR_PROG:
>n
SDT:
>n
CR_PSWD:
>y
SHOW_CHG_PSWD:
>y
ALLOW_ORIG_AFTER_DEACT:
>y
OVERRIDE_ILR_CLASS:
>y
TUPLE TO BE ADDED:
            ILRCLS ILRCLS N N Y Y Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

Please refer to References 1,2.

1.1.5 To allow the user to change the password according to the required dialing sequence LH DT*SC*PWO*PWN#CT

The user can change the password according to the required dialing sequence LH DT*SC*PWO*PWN#CT when CEPTPW line option is assigned to the subscriber.

This enhancement is optional and determined according to the field NEW_PWD_ONCE of tuple CEPTPW in table ISERVOPT.

- NEW_PWD_ONCE{BOOLEAN}: indicates whether the user can change the password by the dialing sequence LH DT*SC*PWO*PWN#CT or not. If it is set as ‘Y’, the user can change the password by this dialing sequence. Otherwise the subscriber can change the password by the dialing sequence LH DT*SC*PWO*PWN*PWN#CT. The default value for the field is ‘N’.

Figure 3 The view of CEPTPW Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT_PIN:
>1111
PIN_VALID:
>n
COLLECT_DNPIN_IN_DIFF_STAGES:
>n
ANNOUNCE:
>n
NEW_PWD_ONCE:
>y
AUTO_UNLOCK:
>y
TUPLE TO BE ADDED:
            CEPTPW CEPTPW 3 1111 N N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

Please refer to References 3.

1.1.6 Password Unlock

When CEPTPW and ILR line option is assigned to the subscriber, upon 3 times of wrong password entry in succession the subscriber will be disallowed any feature modification (activation, deactivation, change) until the following day, or until the administration by operator.The following day is the time after the next 00:00 midnight. The 3 times is the value of field MAX_PIN_RETRY which is datafilled in CEPTPW tuple of table ISERVOPT. The password is 4 digits.

CEPT102 log is generate when subscriber is locked. This log has four fields which are:

- Date and time
- feature

- action of the third wrong password
- calling DN

This enhancement is optional and determined according to the field AUTO_UNLOCK of tuple CEPTPW in table ISERVOPT.

- AUTO_UNLOCK{BOOLEAN}: indicates whether the information of locked user will be recorded and the locked user will be unlocked in the following day automatically. If it is set as 'Y', the locked user will be unlocked automatically in the following day. The default value for the field is 'N'.

Figure 4 The view of CEPTPW Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>ceptpw
OPTION:
>ceptpw
MAX_PIN_RETRY:
>3
DEFAULT_PIN:
>1111
PIN_VALID:
>n
COLLECT_DNPIN_IN_DIFF_STAGES:
>n
ANNOUNCE:
>n
NEW_PWD_ONCE:
>y
AUTO_UNLOCK:
>y
TUPLE TO BE ADDED:
            CEPTPW CEPTPW 3 1111 N N N Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

1.2 Do Not Disturb

1.2.1 Introduction

When a called subscriber has CEPT Do Not Disturb feature active, then the calling subscriber receives a busy tone or an announcement.

The following enhancements are provided by this activity over existing CDND Feature:

- To support Special Dial Tone if the feature is activated.
- To disable the ring splash.
- To support dial tone upon feature deactivation dialing sequence, the user is able to originate new call without hanging up.

1.2.2 General Considerations

These enhancements are developed for IBN lines.

1.2.3 To support special dial tone if the feature is activated

This function has been implemented by feature AT.59019083 and updated by feature AT.59022097. In table ISERVOPT, if the SPECIAL_DIAL_TONE field of CEPT_CFX tuple set to Y and CFD_CFB_INDICATION field of CEPT_CFX set to Y and CDND is active, the special dial tone will be given. A verify will be done in PV stage.

1.2.4 Disable the ring splash

CEPT CDND has no ring splash.

1.2.5 To support dial tone instead of confirmation tone during the deactivation procedure

The subscriber will hear dial tone instead of confirm tone when deactivating the CDND successfully, and the subscriber can originate a new call directly without hanging up.

Dial tone is optional and determined according to a datafill at table ISERVOPT. There is a new tuple CDND defined in table ISERVOPT, and a new field ALLOW_ORIG_AFTER_DEACT is added in this tuple.

- ALLOW_ORIG_AFTER_DEACT {BOOLEAN}: indicates that the dial tone will be generated or confirm tone will be generated. If it is set as ‘Y’, dial tone is generated. Otherwise, confirm tone is generated. The default value for the field is ‘N’.

Figure 5 :Example of ISERVOPT table datafill

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>CDND
OPTION:
>CDND
ALLOW_ORIG_AFTER_DEACT:
>y
TUPLE TO BE ADDED:
CDND CDND Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

1.3 Hardware Requirements or Dependencies

Please refer to the hardware requirements or dependencies part of References 1,2,3,4,5.

1.4 Software Requirements or Dependencies

This feature does not affect the provision method of CEPT ILR, CEPTPW and CDND. It takes effect when the subscriber is using CEPT ILR, CEPTPW and CDND and it is controlled by following datafill:

- in table ISERVOPT, tuple ILRCLS, the ‘Allow_orig_after_deact’ field

- in table ISERVOPT, tuple ILRCLS, the ‘Override_ilr_class’ field

- in table ISERVOPT, tuple CEPTPW, the ‘New_pwd_once’ field

- in table ISERVOPT, tuple CDND, the ‘Allow_orig_after_deact’ field

Please refer to the software requirements or dependencies part of References 1,2,3,4,5 for more details.

1.5 Limitations and restrictions

- The user will not be locked when user input wrong password three times in succession in the period of ONP Swact.
- The max locked users who can be unlocked automatically simultaneously in the following day is limited to 10000. When the number of locked users exceed 10000, the new locked user can't be unlocked automatically in the following day, but CEPT 102 log will still be generated.

For the other details of limitations and restrictions, please refer to References 1,2,3,4,5.

1.6 Interactions

Please refer to the interaction part of References 1,2,3,4,5.

1.7 Glossary

Term	Description
LH	Lift Handset
SC	Service Code
CR	Class Restrict
PW	Password
DT	Dial Tone
DN	Dial Number
CT	Confirm Tone
PWO	Old Password
PWN	New Password
CM	Core Machine
CEPT	European Conference of Postal and Telecommunications Administrations
ILR	International Line Restriction
CDND	CEPT Do not Disturb

1.8 References

1. A59019295 - CEPT International Line Restriction

2. A00001914 - CEPT International Line Restriction Enhancements

3. A00001919 - CEPT Services Password Enhancement

4. A59019083 - CEPT Call Diversion and CEPT Do Not Disturb

5. A00002755 - China PSTN Line Service Compliance

6. SFR2992 - CHT Call Lock

7. SFR2993 - CHT Do Not Disturb

Product = World Trade

A00009489 -- CHT: Call Waiting Enhancement

Functional Description

1: Applicable solution(s)

Int'l IAW

1.1 Description

This ISN09 activity ACT.A00009489 enhances the CEPT Call Waiting for CS2Kc IP platform. Only IBN lines and TW ISUP, TW PRI are supported.

The feature is to enhance the existing CEPT Call Waiting in the aspects as below:

- To support generating the second Call Waiting Tone B for both parties during Call Waiting scenario.
- To support answer the call and toggle between held parties by hook-flash only, no need to enter any digit right after hook-flash.

1.1.1 Call Waiting Scenario

The feature supports the following scenario.

Assume that subscriber A with ICWT option is talking with subscriber B, when a new call to subscriber A comes from subscriber C. The call waiting operation with the implementation of the feature shall be as follows:

a) Subscriber C shall receive a ring back tone.

b) Subscriber A shall receive Call Waiting Tone A.

After 2 seconds (which can be datafilled in CWT_TONE_CYCLE_TIME tuple of table OFCVAR), Call Waiting Tone B shall then be sent periodically to both talking subscribers A and B until A answers the new call.

c) Subscriber A may answer the new call by flashing the cradle hook of his telephone set; the previous talking path connection is still held.

d) Subscriber B shall receive a SILENCE Tone if he continues to hold his telephone off hook.

e) Flashing action by turns shall cause the change over of talking path to subscriber B or subscriber C as desired.

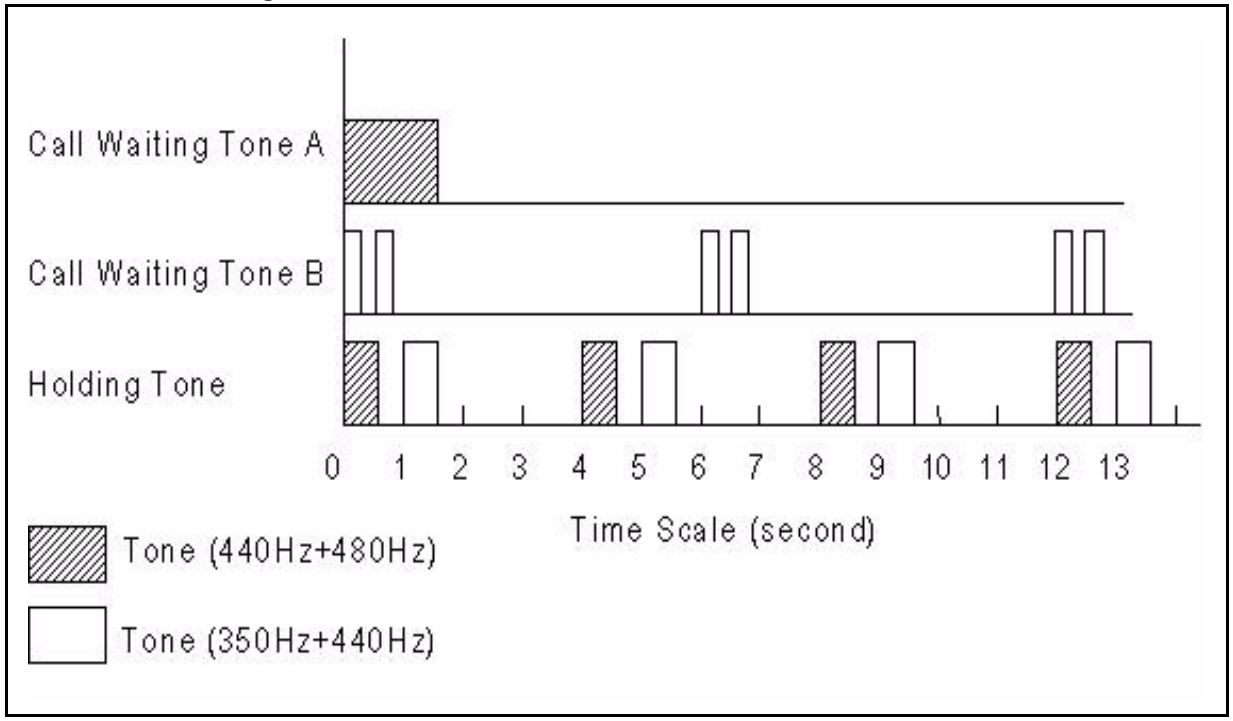
f) When subscriber B or C hangs up, another terminating call shall be able to reach subscriber A, and the call waiting action proceeds as before.

1.1.2 TONES CHARACTERISTICS

Table 1: Tones Characteristics

Tones	Frequency	Level (dBm0)	Cadence ON-1	Cadence OFF-1	Cadence ON-2	Cadence OFF-2	Duration
Call Waiting Tone A	440+480	-13	One pulse ON				1.5 sec
Call Waiting Tone B	350+440	-13	0.25 sec	0.25 sec	0.25 sec	5.25 sec	INFINITE

Figure 1 Tones Characteristics



1.1.3 Example of ISERVOPT table datafill

When ICWT_2PTY_TONE_B is changed from ‘N’ to ‘Y’, a warning message will be displayed: ‘* WARNNING * - If icwt_2pty_tone_b is datafilled YES, field icwt_ignore_waiting_tmo will be disabled.’.

When ICWT_DFLT_RCODE is changed from ‘N’ to ‘Y’, a warning message will be displayed: ‘ If icwt_dflt_rcode is datafilled YES, only TOGGLE ACTION is supported, and Rcode tuple with toggle action in table ISERVOPT should be datafilled.’

Figure 2 The view of ICWT Tuple in ISERVOPT Table

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>icwt
OPTION:
>icwt
ICWT_IGNORE_WAITING_TMO:
>11
ICWT_ANN_ACTIVE:
>y
ICWT_TMO_ANN_ACTIVE:
>y
ICWT_TIMEOUT_TREATMENT:
>BUSY
ICWT_2PTY_TONE_B:
>y
ICWT_DFLT_RCODE:
>y
* WARNNING * -
If icwt_2pty_tone_b is datafilled YES,
field icwt_ignore_waiting_tmo will be disabled.
* WARNNING * -
If icwt_dflt_rcode is datafilled YES,
only TOGGLE ACTION is supported, and Rcode tuple with
toggle action in table ISERVOPT should be datafilled.
TUPLE TO BE ADDED:
                ICWT
                                                ICWT 11 Y Y BUSY Y Y
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
...
```

1.2 Hardware Requirements or Dependencies

Table 2: Signals should be supported in Media Gateways

	Call Waiting Tone A	Call Waiting Tone B
MGCP	L/wt1	L/wt2
Megaco/H.248	alert/cw{pattern=1}	alert/cw{pattern=2}

VG201, MG1K and PVG should support Taiwan Tonesets including the signal above. While Call Waiting Tone B is OFF, speech path should NOT be killed by VG201, MG1K and PVG.

1.3 Software Requirements or Dependencies

This feature does not affect the provision method of CEPT ICWT. It takes effect when the subscriber is using CEPT ICWT and it is controlled by following datafill:

- In table OFCVAR, tuple CWT_TONE_CYCLE_TIME should be set to 2, which is the interval between the beginning of CWT tone A and CWT tone B.

- In table ISERVOPT, tuple ICWT, the ICWT_2PTY_TONE_B field. If datafilled ‘Y’, Call Waiting Tone B will be applied to both talking side infinitely after applying Call Waiting Tone A to the controller and field icwt_ignore_waiting_tmo will be disabled.

- In table ISERVOPT, tuple ICWT, the ICWT_DFLT_RCODE field. If datafilled ‘Y’, R-code is not needed while toggling between held parties. The RCODE tuple in table ISERVOPT must exist and ACTION “TOGGLE” must be datafilled. If not, a nack tone will be given when flash and after the tone is over, the call will revert to the former state before flash.

Please refer to the software requirements or dependencies part of References b, c for more details.

1.4 Limitations and restrictions

Please refer to References b, c.

1.5 Interactions

Please refer to References b, c.

1.6 Glossary

Term	Description
CEPT	European Conference of Postal and Telecommunications Administrations
ICWT	Line Option on CEPT Call Waiting
Megaco/H.248	ITU-T and IETF Media Gateway Control Protocol
MGCP	Media Gateway Control Protocol
VG201	4 Port Integrated Access Device
MG1K	Media Gateway MG1000
PVG	Packet Voice Gateway
I3WC	International Three Wall Calling

1.7 Reference

a. SFR 2991 - CHT Call Waiting Tone

b. A59019288 - CEPT Call Waiting

c. A59019281 - CEPT I3WC and ICT

1.8 Appendix for A00009489: Q01097743 FN (I3WC Default Rcode)

CR.Q01097743: ISN09, ICWT&I3WC Enhancement, I3WC default RCODE.

The CR is to enhance the existing CEPT International Three Way Calling in the aspects as below:

- To support using hook-flash only without dialing RCODE in I3WC scenario.

1.8.1 I3WC Scenario

This feature supports following scenario:

Assume that line A has the I3WC feature. A is talking with B, and then A flashes to calls C to make a three way call. The scenario with the implementation of this feature will be described as follows:

a) If C is busy, A will hear a busy tone. Then A can flash and resume the two parties connect with B.

b) If C is not busy and answers the call from A, the active parties are A and C and B is the holding party. If A flashes, **without dialing RCODE**, a three way conference is established. A is the controller.

c) In 3-way conference state, if A flashes, **without dialing RCODE**, party C is disconnected, A and B are still in talking mode.

d) In 3-way conference state, if B or C goes on hook, then A will be connected to the remaining 3wc party. That means if B disconnect, A will be connected to C and A can make another conference call by hook-flash.

e) In 3-way conference state, if the controller A goes on hook, then the conference call is over, i.e. all calls drop.

To implement the above requirement needs supporting I3WC without dialing RCODE.

1.8.2 Support I3WC Without Dialing RCODE

A new tuple I3WC with field I3WC_DFLT_RCODE(Y/N) will be defined in table ISERVOPT. When the I3WC_DFLT_RCODE is ‘N’, the existing behavior will be used. When the I3WC_DFLT_RCODE is set to ‘Y’, the scenario described above will be used. The default value for the field is ‘N’.

When I3WC_DFLT_RCODE is changed from ‘N’ to ‘Y’, two warning messages will be displayed: ‘RCODE tuple in table ISERVOPT must exist and ACTION CON_3WC and DISC_ACT must be datafilled.’ and ‘Default RCODE only supports CON_3WC and DISC_ACT actions.’

Figure 3 :Example of ISERVOPT table datafill

```
TABLE: ISERVOPT
>add
MACHINES NOT IN SYNC - DMOS NOT ALLOWED
JOURNAL FILE UNAVAILABLE - DMOS NOT ALLOWED
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
>y
SOPTSKEY:
>I3WC
OPTION:
>I3WC
I3WC_DFLT_RCODE:
>y
TUPLE TO BE ADDED:
I3WC I3WC Y

ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
>y
* WARNNING * - RCODE tuple in table ISERVOPT must exist and
ACTION CON_3WC and DISC_ACT must be datafilled.
* WARNNING * - Default RCODE only supports CON_3WC and
DISC_ACT actions.
TUPLE ADDED
```

Notes: the interaction between I3WC, ICWT, I6WC and ICT features will change accordingly.

- Assume that subscriber A with ICWT option is talking with subscriber B, when a new call to subscriber A comes from subscriber C. In this case, the ICWT feature has the highest priority. That means when A flashes, the default flash action is toggle if icwt_dflt_rcode datafill Y even the I3WC or I6WC or ICT feature exist on the line A.
- If not in the ICWT case described above, the I6WC feature has the highest priority. Suppose ICWT, I6WC, I3WC and ICT exist on the line at the same time but not in ICWT scenario, due to we don't disable the Rcode for I6WC, after flashing, we need dialing rcode to select the action we want. Everything seems like before, but if we select establish 3-way call, and after we enter the 3-way call scenario, whether we need rcode in 3-way call is decided by i3wc_dflt_rcode datafill.
- If not in the ICWT case and line A has not I6WC feature, the I3WC feature will take the highest priority. Suppose ICWT, I3WC and ICT exist on the line at the same time but not in ICWT scenario, after flashing, if i3wc_dflt_rcode datafilled Y, we don't need Rcode to setup the 3-way call and don't need Rcode to disconnect party C as well.

- If not in the ICWT case and line A has not I6WC and I3WC feature, the ICT feature will take effect. In this case, Rcode is needed.

1.8.3 Software Requirements or Dependencies

This feature does not affect the provision method of CEPT I3WC. It takes effect when the subscriber is using CEPT I3WC and it is controlled by following datafill:

- In table ISERVOPT, tuple I3WC, the I3WC_DFLT_RCODE field. If datafilled 'Y', R-code is not needed in I3WC scenario. The RCODE tuple in table ISERVOPT must exist and ACTION "CON_3WC" and "DISC_ACT" must be datafilled. If not, a nack tone will be given when flash and after the tone is over, the call will revert to the former state before flash.

Product = World Trade

A00011363 -- International H.323 2 CLI (Calling Line Identity) Support

Functional Description

1: Applicable solution(s)

Int'l CHS

1.1 Description

The activity provides support for 2 CLI delivery to a H.323 terminating Gateway/terminal[1] in the International CS2000 ISN load, for public calls.

This feature provides support for 2 CLI delivery for the following originating agent scenarios in a French market configuration, with functional equivalency to a terminating PRI trunk:

- ETSI ISUP v2 Base Variant -> International H.323 in Section 1.1.2.1.
- SPIROU -> International H.323 in Section 1.1.2.2.
- ETSI PRI -> International H.323 in Section 1.1.2.3.
- International H.323 -> International H.323 in Section 1.1.2.3.
- International H.323 -> ETSI PRI in Section 2.2.2.3
- International H.323 -> ETSI ISUP V2 Base Variant in Section 2.2.2.4

1. A H.323 terminating Gateway/terminal is referred to as the "International H.323 terminator" through out this document.

- International H.323 -> SPIROU in Section 2.2.2.5

Other originators and market configurations may also work but are not formally verified by this feature.

Support for 2 CLI delivery on outgoing ISUP/PRI trunks for a call originating from H323 is already supported and not changed by this feature.

The 2 CLI functionality is associated with ISDN supplementary service provisioning option Calling Line Identification Presentation (CLIP) and Calling Line Identification Restriction (CLIR). With 2 CLI the calling line has two identities namely the Network Number (NN) and Presentation Number (PN).

The standard 2 CLI handling mode described as “special arrangement” in H.246 and Q.699 is supported by this feature. In this mode of operation a User Provided CLI is passed on without verification and a 2nd Network Provided CLI is added to the call signalling by the 1st public network exchange.

- A Network Number is a CLI provided by the public network, which identifies the actual network termination point from which a call originates.
- A Presentation Number (PN) is a dialable number that the calling user wishes to display to the called user. It is normally User provided and not verified by the network (Q699/H.246 “special arrangement” case).

The NN and PN may or may not be the same. The PN can be used to return a call to the originator or an associated number. For example, a calling salesperson may want to display a free phone number, in order to provide the incentive of a free call, when a purchase is made.

For the International H.323 terminator, if 2 CLIs are available they are delivered in the SETUP message by sending the Presentation Number in the CGN IE (Calling Party Number Information Element) field and the Network number in the additionalSourceAddresses field. If only 1 CLI is available then it is delivered in the CGN IE whether it is a Network Number or Presentation Number.

This complies with ITU-T H.246.0 Annex C(07/2003)[2] as amended by the ITU-T H.323 System Implementors’ Guide(30th January 2004), for the case of interworking to a Gateway/terminal in “special arrangement” mode.

For this feature to work functionally a Gateway that also supports this capability per these versions of the specifications is required eg.OneAccess.

2. Older versions of the H.323 and H246 specifications had different unrobust schemas.

This feature extends the existing functionality implemented by French market 2 CLI feature A59027509 to provide equivalent behavior for International H323 terminators. A59027509 is a refinement and extension of MMP14 feature A59016672 that developed 2CLI delivery for an ETSI PRI terminator. A59016672 in turn works only in conjunction with feature AJ5284 "Presentation CLI Support" and enhanced it to support Special Arrangement on selected agents. The "Special Arrangement" feature introduced by AJ5284 was developed to give selected customers the possibility to deliver Calling Party Numbers to the terminator which are not screened.

If Special Arrangement applies to a customer, the CGN digits delivered by him are not screened, however the NPI (Number Plan Indicator) and TON (Type of Number) information elements are screened to check public E.164 numbers are provided.

1.1.1 Datafill control

This feature will reuse the same datafill options that control 2 CLI delivery and behavior for PRI trunks. Reference A59016672 & A59027509.

1.1.1.1 2 CLI delivery control options on the Terminating H323

1.1.1.1.1 2CLI Delivery Control option for International H.323 Terminator

Delivery of 2 CLIs vs. only 1 CLI for an International H.323 terminator is enabled on a trunk group basis by datafilling the 2CLI option on the H.323 QSIG trunk. When the "2CLI" option is not data filled the QSIG interface will not generate 2CLI's in the outgoing SETUP message. A sample datafill in table LTDATA is as follows:

Table 1 Table LTDATA - Datafill 2CLI Option (New Datafill)

LTDKEY	LTDRSLT	LTCLI_OPTION	LTCLI_OPTION
H323TST CLI	CLI	2CLI	$

The 2CLI option is an existing option in table LTDATA previously only functional for PRI trunks.

1.1.1.1.2 CLIP option Table LTDATA

The CLIP option is applicable to ETSI PRI and International H.323 terminator. Sample datafill for International H.323 terminator is as follows:

Table 2 Table LTDATA CLIP option

LTDKEY	LTDRSLT	AUDTRMT	CGNREQD	CGNDELV	CDNDELV
H323TST 1 SERV	SERV	N	Y	SCREENED	ALWAYS

1.1.1.2 Related CLI options on the Originating H323

The availability of 2 CLIs for delivery is dependent on several factors. For PRI/H323 to H323 the following options on the originating trunk are relevant (all are existing options and unchanged by this feature):

- CLIR option provisioned for the originator
- Screening for originator (Table LTDATA)
- CUSTGROUP public call (relation between originator and terminator)
- PN_SUPPORTED = Y

1.1.1.2.1 CLIR option Table LTDATA

The CLIR option is applicable for ETSI PRI and International H.323 originators. Sample datafill allowing presentation of the CLI unless overridden by per call CLIR activation code.

Table 3 Table LTDATA CLIR option

LTDKEY	LTDRSLT	LTCLI_OPTION	PI	MODE
H323TST 1 CLI	CLI	DFLTPI	ALLOW	TEMP

1.1.1.2.2 Screening in Table LTDATA

For “special arrangement” behavior as required in France no screening is performed on the received CLI from the user. This is configured by using the NOSCRN option in a LTDATA CLI tuple.

Table 4 Table LTDATA

LTDKEY	DATATYPE	OPTION
H323TST 1 CLI	CLI	**NOSCRN**

In this NOSCRN case the Network Number is taken from the DFLTCGN option in LTDATA

Table 5 Table LTDATA

LTDKEY	DATATYPE	DFTLTCGN
H323TST 1 DN	DN	017 230 3680 $

Note: For other markets other CLI options are used to configure different screening behavior. e.g.: SCRNPN (screen the received CLI but use it as a PN) or SCRNLTID and SCRNDFLT (“no special arrangement scenarios to screen the received CLI and use after editing as a single User provided Verified and Passed CLI)

1.1.1.2.3 CUSTGROUP Table CUSTNTWK

This option is applicable for ETSI ISUP V2, SPIROU, ETSI PRI and International H.323. It is a prerequisite for the 2CLI feature that the call must be a public call.

1.1.1.2.4 PN_SUPPORTED Table OFCENG

This option is applicable for ETSI ISUP V2, SPIROU, ETSI PRI and International H.323. The office parameter has two fields. They are ACTIVE and BTUP_SIM_HANDLING. For this feature, the field ACTIVE must be set to Y to enable 2 CLI behavior for PRI/H323 to H323. It should not affect the ISUP interworkings. Datafill for PN_SUPPORTED option is illustrated below:

Table 6 Table OFCENG

PARMNAME	PARMVAL
PN_SUPPORTED	**Y** N

1.1.1.3 Example datafill for French 2 CLI configuration

```
>
2004/09/23 06:11 SWC00007.PPC3 V:12
TABLE: TRKGRP

>pos oa_4
OA_4
PRA 0 NPDGP NCRT MIDL 0172303690 (QSIG 9) $ $
>pos oa_2
OA_2
PRA 0 NPDGP NCRT MIDL 0172303688 (QSIG 10) $ $
>

TABLE: LTDATA
>lis all
TOP
LTDKEY LTDRSLT
--------------
QSIG 9 DN DN 017 230 3690 $
QSIG 9 SERV SERV Y N SCREENED ALWAYS (DAS PRIOVLP)
(NET_RINGBACK_ON )
(PRI_IP_PROT H323) $
QSIG 9 CLI CLI (DFLTPI ALLOW TEMP) (NOSCRN ) $
QSIG 10 DN DN 017 230 3680 $
QSIG 10 SERV SERV Y N SCREENED ALWAYS (DAS PRIOVLP)
(NET_RINGBACK_ON )
(PRI_IP_PROT H323) $
QSIG 10 CLI CLI (DFLTPI ALLOW TEMP) (NOSCRN ) $
```

1.1.2 CLI Mapping for Interworking Scenarios Supported:

1.1.2.1 ETSI ISUP v2 Base Variant to International H.323

There are three possible cases:

1.1.2.1.1 "Calling party Number" parameter in IAM complete

If a CGPN is present and complete in the IAM then one or two "calling party number" IE may be created according to the presentation indicator and the category of the served subscriber,i.e.

- If the presentation indicator of the CGPN is set to 0 (Presentation allowed), one or two "calling party number" IE may be created.
- If the presentation indicator of the CGPN is set to 1 (Presentation restricted) and called subscriber has the CLIR override category one or two "calling party number" IE may be created.

If the above condition is met and if the served subscriber is subscribed to the CLIP[3] supplementary service, then:

GNP presentation - If a "Generic Number" qualified to "additional calling party number" is present, it shall be sent in a first "calling party number" IE. This IE contains the address signal received in the IAM and is coded as follows:

Table 7 Generic Number mapped to CGN IE in International H.323SETUP

Bits	Value
Octet 3 bits 765	Type of Number is mapped transparently according to bits BA of identity of the calling line.
Octet 3 bits 4321	Numbering Plan Identification is mapped transparently.
Octet 3a bits 76	Presentation Indicator is mapped transparently
Octet 3a bits 21	Screening Indicator is mapped transparently
Octet 4 and above	Address signals

3. Data filled in table LTDATA for the International H.323 terminator
Sample Datafill:
LTDKEY LTDRSTL CGNDELV CDNDELV

QSIG 1 CLI SERV SCREENED ALWAYS

A second CLI (the Network Number) is sent to the terminating International H.323 agent in the additionalSourceAddresses parameter. The Calling party number parameter from the IAM is used to encode the additionalSourceAddresses Information element as follows:

Table 8 Coding of the additionalSourceAddresses Information Element According to the Calling party number parameter

IAM Calling Party Number parameter	SETUP additionalSourceAddresses
Nature of Address National number International number	Type of number National number International number
Numbering Plan Indicator	"Numbering plan identification"
ISDN/Telephony Numbering Plan	ISDN/Telephony Numbering Plan
Address Presentation Restricted Indicator Presentation allowed Presentation Restricted	Presentation Indicator Presentation Allowed Presentation restricted
Screening Indicator User provided, verified and passed Network Provided	Screening Indicator User provided, verified and passed Network Provided
Address signals	Number digits

1.1.2.1.2 Calling Party Number absent or incomplete

If the "calling party number" parameter received in the IAM is absent or incomplete then only one "calling party number" IE shall be created. The IE contains no address signal and is coded as follows:

Table 9 Calling Party Number in the SETUP (International H.323)

Bits	Value
Octet 3 bits 765	The "type of number" is set to unknown (000).
Octet 3 bits 4321	"Numbering plan identification" is set to unknown (0000)
Octet 3a bits 76	"presentation indicator" is set to number not available due to interworking (10).
Octet 3a bits 21	"Screening indicator" is set to network provided (11)

1.1.2.1.3 Identity complete, presentation restricted (without CLIR override)

If the "calling party number" received in the IAM is complete and available, and the presentation indicator is set to restricted, and the served subscriber does not have the CLIR override category, then only one "calling party number" IE shall be created. The IE contains no address signal. It shall be coded as follows:

Table 10 “Calling Party Number” in SETUP

Octet 3 bits 765	The “type of number” is set to unknown (000).
Octet 3 bits 4321	“Numbering plan identification” is set to unknown (0000).
Octet 3a bits 76	“presentation indicator” is set restricted (01).
Octet 3a bits 21	“Screening indicator” is set to network provided (11)

1.1.2.2 SPIROU to International H.323

The CLI handling is the same as Figure 1.1.2.1, "ETSI ISUP v2 Base Variant to International H.323".

1.1.2.3 International H.323/ ETSI PRI to International H.323/ ETSI PRI

The mapping of parameters for International H.323/ETSI PRI to International H.323 according to ETSI/ITU Q.699for the following configurations is supported:

Configuration	Calling user provisioned to:	Called user provisioned to:
I as described 1.1.2.3.1	CLIR option provisioned; PI = **allowed**	**CLIP** option provisioned 2CLI option provisioned;
II as described in 1.1.2.3.2	CLIR option provisioned; PI = **restricted**	**CLIP** option provisioned 2CLI option provisioned;
III as described in 1.1.2.3.3	CLIP option provisioned; PI = restricted	CLIP override option provisioned 2CLI option provisioned.

1.1.2.3.1 Configuration I:

- Calling User: Special arrangement applies
- Called User: CLIP
- Terminator: Two number delivery supported

Originator: ETSI-PRI/International H.323	optional: ETSI-ISUP V2	Terminator: International H.323/ETSI PRI
Calling party number IE: TON = international national subscriber ***1** NPI = unknown or ISDN PI = Presentation allowed SI = not relevant digit = any digits	**Generic number parameter:** NOA = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation allowed SI = User provided, not verified digit = digits as received	**1. Calling party number IE:** TON = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation allowed SI = User provided, not screened digit = digits as received
	Calling party number parameter: NOA = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN	**2. Calling party number IE:** TON = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN
Calling party number IE: TON = 'unknown' or 'private network' or NPI != unknown or ISDN or digits = not available	**Generic number parameter:** not mapped	**Calling party number IE:** TON = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN
	Calling party number parameter: NOA = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN	

Notes: 1 - only for certain markets, e.g. Germany. N/A to France. Controlled by Market of Office or other market datafill.

1.1.2.3.2 Configuration II:

- Calling User: Special arrangement applies
- Calling User: Temporary CLIR, Presentation restricted
- Called User: CLIP
- Terminating ETSI-PRI: Two number delivery supported

Originator: ETSI-PRI/International H.323	optional: ETSI-ISUP V2	Terminator: International H.323/ETSI PRI
Calling party number IE: TON = international national subscriber ***1** NPI = unknown or ISDN PI = Presentation restricted SI = not relevant digit = any digits	**Generic number parameter:** NOA = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation restricted SI = User provided, not verified digit = digits as received **Calling party number parameter:** NOA = national NPI = ISDN/Telephony PI = Presentation restricted SI = Network provided digit = Default DN	**Calling party number IE:** TON = unknown NPI = unknown PI = Presentation restricted SI = Network provided digit = not included/empty
Calling party number IE: TON = 'unknown' or 'private network' or NPI != unknown or ISDN or digits = not available	**Generic number parameter:** not mapped **Calling party number parameter:** NOA = national NPI = ISDN/Telephony PI = Presentation restricted SI = Network provided digit = Default DN	**Calling party number IE:** TON = unknown NPI = unknown PI = Presentation restricted SI = Network provided digit = not included/empty

Notes: 1 - only for certain markets, e.g. Germany. N/A to France. Controlled by Market of Office or other market datafill.

1.1.2.3.3 Configuration III:

- Calling User: Special arrangement applies
- Calling User: Temporary CLIR, Presentation restricted
- Called User: CLIP **override category**
- Terminating ETSI-PRI: Two number delivery supported

Originator: ETSI-PRI / International H.323	optional: ETSI-ISUP V2	Terminator: International H.323/ETSI-PRI
Calling party number IE: TON = international national subscriber ***1** NPI = unknown or ISDN PI = Presentation restricted SI = not relevant digit = any digits	**Generic number parameter:** NOA = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation restricted SI = User provided, not verified digit = digits as received	**1. Calling party number IE:** TON = international national subscriber ***1** NPI = ISDN/Telephony PI = Presentation allowed SI = User provided, not screened digit = digits as received
	Calling party number parameter: NOA = national NPI = ISDN/Telephony PI = Presentation restricted SI = Network provided digit = Default DN	**2. Calling party number IE:** TON = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN
Calling party number IE: TON != international/national (or subscriber ***1**) or NPI != unknown or ISDN or digits = not available	**Generic number parameter:** not mapped	**Calling party number IE:** TON = national NPI = ISDN/Telephony PI = Presentation allowed SI = Network provided digit = Default DN
	Calling party number parameter: NOA = national NPI = ISDN/Telephony PI = Presentation restricted SI = Network provided digit = Default DN	

Notes: 1 - only for certain markets, e.g. Germany. N/A to France. Controlled by Market of Office or other market datafill.

1.1.2.4 International H.323 to ETSI ISUP V2 Base Variant

This functionality already exists and is not changed by this feature, but is not explicitly documented for H323 yet, hence this section is included for information only.

In the French market configuration the mapping is identical to that for PRI to ETSI ISUP V2 Base Variant as documented in feature A59027509. Any additionalSourceAddresses field or 2nd CGN IE received from H323 will be ignored by the CS2000.

This is in alignment with the mapping as specified in Q.699 with Special Arrangement and ITU-T H.246 Annex C Gateway/Terminal interworking case with Special Arrangement. A59027509 has some clarifications to the handling of some field coding cases not explicitly defined in Q699/H.246 and not normally expected.

1.1.2.5 International H.323 to SPIROU

This functionality already exists and is not changed by this feature, but is not explicitly documented for H323 yet, hence this section is included for information only.

In the French market configuration the mapping of Calling Party Number and Generic Number Parameter in the IAM from the SETUP message are as described in the TWOCLI FN document.

1.1.3 Network Number editing

When the Network Number is delivered on H323 in the additionalSourceAddresses field the digits contained may be edited by the CLGDMI option against the outgoing H323 trunk.

The Presentation Number sent in the CGN IE will also be edited by CLGDMI as in the current 1 CLI delivery case.

1.2 Hardware Requirements or Dependencies

This feature requires a Gateway supporting ITU-T H.246.0 Annex C(07/2003)[4] as amended by the ITU-T H.323 System Implementors' Guide(30th January 2004). The terminating International H.323 Gateway/terminal must be capable of receiving 2CLIs in the H.225.0 SETUP message. The first CLI is coded in the Calling Party Number Information Element and the second CLI in the additionalSourceAddresses field.

1.3 Software Requirements or Dependencies

None

1.4 Limitations and restrictions

- This feature requires a Gateway supporting ITU-T H.246.0 Annex C(07/2003)[5] as amended by the ITU-T H.323 System Implementors' Guide(30th January 2004). This feature will not work with gateways implementing older versions of the ITU-T H.246 Specification.
- Only Public E164 type (User Provided) Presentation Number CLIs are supported and will always be sent in the Calling Party Number IE field.
  - as per Section 5.8.1 Interworking for Conveying Two Calling Party Number, Section C.7.2.3 Calling Line Identification Presentation (CLIP) /Calling Party Name Presentation (H.450.8), Table C.56/H.246 "CLIP information sent to the called user" of the ITU-T H.323 System Implementors' Guide shall not use the SourceAddress of the SETUP message and shall use the Calling

4. Older versions of the H.323 and H246 specifications had different unrobust schemas.
5. Older versions of the H.323 and H246 specifications had different unrobust schemas.

Party Number IE field because the number being sent is a public number.

– As per Section 7.8.2.1 Calling party address information of the ITU-T H.323 (07/2003) the SourceAddress field of the SETUP message is used to encode numbers belonging to the Private numbering plan.

– The mapping of parameters from the H.225.0 SETUP to ISUP IAM as per Table C.20.1/H.246 Calling Party Number and Table C.20.2/H.246 Calling Party Number of the ITU-T H.323 System Implementors' Guide which refers to cases where SourceAddress fields are received is not supported.

- The Gatekeeper to Gatekeeper scenarios described in H.246 are not supported,

  — any received additionalSourceAddresses field will be ignored by the CS2000. Only the 1st CGN IE is used.

  — The mapping of parameters from the H.225.0 SETUP to ISUP IAM for SETUP messages received from the Gatekeeper when Special Arrangement applies is not supported.

  — The mapping of 2CLIs received from the Gatekeeper as per Section 5.8.1 Interworking for Conveying Two Calling Party Numbers, Section C.6.2.1.1 Special Arrangement Applies - "Setup Received from the Gatekeeper" of the ITU-T H.323 System Implementors' Guide is not supported.

- 'Special Arrangement does not apply' scenarios are not applicable - these are 1 CLI scenarios:

  – This feature does not support carrying of the GNP in the IAM message for International H.323 to ETSI ISUP v2 Base Variant for "without special arrangement" case.

  – The mapping of parameters from the H.225.0 SETUP to ISUP IAM as per Table C.21/H.246 "CLIP - Special Arrangement does not apply" of ITU-T H.246.0 Annex C is out of the scope of this feature and should be provided by the base H.323 feature.

  – The mapping of parameters from the H.225.0 SETUP to the ISUP IAM as outlined in Section 5.8.1 Interworking for Conveying Two Calling Party Number, Section C.6.2.1.2 Special Arrangement does not apply "Setup Received from the Gatekeeper" of the ITU-T H.323 System Implementors' Guide is not a supported configuration for this feature.

1.5 Interactions

None

1.6 Applicable customer facing sections

Fault Management

Logs __N/A__

Alarms __N/A__

Configuration

Data Schema ___X___

User Interface __N/A__

Element Management __N/A__

Security __N/A__

Service Order __N/A__

Office Parameters __N/A__

Accounting (includes AMA billing) __N/A__

AMA billing information is not changed by this feature.

The NDS Billing feature as documented in fmdoc PRNDSBIL has been verified for the International H.323 to ETSI ISUP v2 calls by this feature in response to a request from N9UF telecom for this feature. The Table 11, "Digits captured in Module 046 and the OOD of the AMA record," on page 2383 shows the digits captured in the OOD field of the AMA record and that captured in the Module 046 for International H.323 to ETSI ISUP v2 calls in which the incoming SETUP message has a CGN IE present, that have been verified by this feature.

AMACLID_IC_PRI_CGN is a option present in table AMAOPTS.

Table 11 Digits captured in Module 046 and the OOD of the AMA record

BILLDN	AMACLID	DFLTCGN in table LTDATA	AMACLID _IC_PRI_CGN	OOD(AMA Base Record)*	Screening/Editing of Incoming CLI provisioned?	OOD MODULE 46
-	TRUE	Datafilled	-	DFLCGN from table LTDATA.	-	-
-	TRUE	No		CLI from the SETUP message.	-	-
Datafilled	TRUE	No	ON	BILLDN	CLI Screening Passes	Unscreened/Unedited CLI (CLI from the SETUP message).

BILLDN	AMACLID	DFLTCGN in table LTDATA	AMACLID _IC_PRI_CGN	OOD(AMA Base Record)*	Screening/Editing of Incoming CLI provisioned?	OOD MODULE 46
Datafilled	TRUE	Datafilled	OFF	BILLDN	CLI Screening Passes	Screened/Edited CLI (DFLTCGN from table LTDATA)
Datafilled	TRUE	No	ON	BILLDN	N	CLI from the SETUP message. If AMACLID_IC_PRI_CGN is OFF then 0's only are appended to the module 046.
-	-	No	-	CLI from the CGN IE in the SETUP message	Screening passes or screening fails.	-
Datafilled	-	No	-	BILLDN	Screening passes or screening fails	-

Performance (includes operational measurements) __N/A__

1.7 Glossary

Term	Description
CGN	Calling Number
CLI	Calling Line Identification
CLID	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
DN	Directory Number
ETSI	European Telecommunications Standards Institute
GN	Generic Number
GWC	GateWay Controller

H.323	A protocol supporting the Packet-based Multimedia Communications Systems
IE	Information Element
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
NN	Network Number
NPI	Numbering Plan Identifier
PI	Presentation Indicator
PN	Presentation Number
PRI	Primary Rate Interface
QSIG	Q Interface Signalling
SI	Screening Indicator
SPIROU	Signalization Pour l'Interconnexion des Réseaux Ouverts
TON	Type of Number
VPN	Virtual Private Network

1.8 References

Table 12 References

Document	Title
Requirement Document NC/France/22 v1.0	CLI Handling between ISUP V2, SPIROU and Access Protocols
NC/France/21 v2.0	CLI Handling between ISUP V2, SSUTR2 and Access Protocols PRI VN, ETSI PRI, BRI VN, ETSI BRI and Analogue line.
AJ5284	Presentation Number Feature
A59027509	ISUP 2CLI Support with VN4(PRI) and ETSI (PRI,BRI)
A59016672	ETSI-PRI CLIP/CLIR Enhancement
ITU-T Recommendation Q.699 (09/97)	Interworking between ISDN Access and Non-ISDN Access over ISDN User Part of Signalling System No. 7
ITU-T H.225.0 (07/2003)	Call Signalling protocols and media stream packetization for packet-based multimedia communication systems.
ITU-T H.323 (07/2003)	Packet-based multimedia communications systems.

Table 12 References

Document	Title
ITU-T H.246.0 Annex C (07/2003)	Annex C:ISDN User Part Function - H.255.0 Interworking
ITU-T H.323 System Implementors' Guide(30th January 2004)	Implementors' Guide for Recommendations of the H.323 System ("Packed-based multimediacommunications systems"): H.323, H.225.0, H.245, H.246,H.283, H.235, H.341, H.450 Series, H.460 Series and H.500 Series
TWOCLIFN (in FMDOC)	TWO CLI support for SPIROU and ETSI ISUP V2 interworking with PRI/BRI.

Chapter 5: Logs/faults and OMs/PMs

This chapter provides information on Logs/faults, and on operational measurements (OMs)/performance measurements (PMs). Some information appears in NE-specific Appendices to this document. Those appendices are mas351referenced in the text of this chapter where appropriate.

Logs/Faults information

A log report is a record of a message that your system generates whenever a significant event has occurred in the switch or one of its peripherals. Log reports include status and activity reports, as well as reports on hardware or software faults, test results, changes in state, and other events or conditions likely to affect the performance of the switch. Either a system action or a manual action can generate a log report.

> ***Note:*** Some of the element managers use a graphical user interface (GUI), so they display faults on the workstation monitor screen rather than generating log reports.

Alarms are generated by the system when problems or conditions are detected that can change the performance or working state of a network or network element. Daily operation of the network requires monitoring for alarms and checking that functions continue without interruption. Alarms provide notification that a system hardware or software-related event has occurred.

Using Syslog

In SN06 an alternative is introduced to log/fault delivery from each separate element management system. Syslog can be used to aggregate some of the individual fault/log streams into the SCC2/NT STD stream on the CS 2000 Core Manager/SDM.

The network will be using syslog in several ways:

- Alarms/Faults - custlog stream - Many element managers and network elements, including SDM Platform, CS 2000 SAM21 Manager, STORM, CS 2000 GWC Manager, UAS Manager, MDM (for MG15000, previously PVG), and some CS 2000 Management Tools applications, use syslog as one mechanism for notify other systems of fault events. One consumer of

those fault events is the SCC2/NT STD log converter provided on the CS2000 Core Manager/SDM. The SCC2/NT STD log converter will collect events from those sources via the custlog format and merge those events into the SCC2/NT STD stream with the CS2000 Core fault events.

- Audit trail - The network is also using syslog to capture the user audit trail our network elements and element mangers. The audit trail contains a history of significant user and OSS activity. Syslog is the only protocol which will contain the audit trail.
- Security log - The network is also using syslog to capture the security logs from our network elements and element mangers. The security log contains both success and failure history of authentication and authorization activities. This stream will also contain security related events from IPSec/KCE and other key negotiation systems. Syslog is the only protocol which will contain the security log stream.
- Debug log - some components use syslog for diagnostic and debug information used by the Nortel support personnel. This stream is not exported beyond the EMSs and is not configured or documented for end user or customer access.

Alarm reporting for DMS and SPM-based equipment

The alarm reporting system integrates event detection and alarm notification functions. An alarm becomes active when reduced service, reliability, or a test condition occurs in the network or network element. The alarm remains active until a system event or activity performed by operating company personnel clears the alarm condition. The alarm system includes audible notification and visual display through warning lights and the MAP terminal. Many alarms generate automatic logs reports when raised or cleared.

For DMS and SPM-based equipment, the MAP terminal displays alarm codes in the banner and the subsystem status summary field (SSSF). The alarm banner displays alarm codes that indicate the effect of the alarm event on the network or network element. The SSSF displays alarm codes that indicate equipment faults of system states.

Log Delivery Service application

The Log Delivery Service application collects logs generated by the Communications Server 2000 (CS2000) and from the CS2000 Core Manager log stream, formats these logs, and can deliver them as a single stream to the downstream Operational Support Systems (OSS).

The CS2000 log feed includes logs for itself and all peripherals managed by it, such as: MG 4000, IW-SPM, DPT-SPM and SPM. Logs are generated locally on the CS2000 Core Manager for its own faults and status changes and are merged with the CS2000 feed. The Log Delivery Service application provides log reports in ASCII text format at a single interface for inbound or

outbound TCP/IP connections.

Log formats

The Log Delivery service provides reports in either Switching Control Center 2 (SCC2) or Standard (STD) format. Some of the high-level differences between SCC2 format logs and STD format logs are as follows:

- SCC2 has no CS2000 identifier as found in the top left hand corner of the STD log. This field is datafilled on the CS2000 in table OFCVAR, tuple LOG_OFFICE_ID.
- SCC2 logs do not contain the date in the header on which the log was generated.
- SCC2 logs only give the minutes past the hour in which the log was generated, while the STD log gives the hour, minutes, and seconds.
- A critical severity log is represented by *C in SCC2 format, and by *** in STD format.
- If applicable, the SCC2 log will have the name of the component and/or peripheral generating the log in the log header.
- When ECORE_FORMAT (table OFCVAR on the CS2K) is enabled, SCC2 formatted logs display the optional parameter NodeName on a new line immediately following the header. This new line is not indented and has the following format: Log from node <NodeName>.
- SCC2 headers (having less information) are less likely to have the Equipment Identifier field found in some logs wrapped to the next line. (See NT STD format definition section below).

See the following example to see the difference in the formats, using a CARR811 log.

Standard format:

```
ASN06SWITCH   * CARR811 FEB24 00:45:05 3320 TBL  CARRIER SPM  39
   CKT: 63  CarrName: SPM39_STS1P_1_VT15P_1_DS1P_28
   Carrier: STS1P  1 VT15P 28 DS1P   1
   UAS-N  Threshold Crossing Alert:         10
   Accumulation Interval:  0:00:10    Period: 15 minutes
   Location: SPM 39  Type: SMG4      Fabric: ATM
```

SCC2 format:

```
ASN06SWITCH   * CARR811 FEB24 00:45:05 3320 TBL  CARRIER SPM  39
   CKT: 63  CarrName: SPM39_STS1P_1_VT15P_1_DS1P_28
   Carrier: STS1P  1 VT15P 28 DS1P   1
   UAS-N  Threshold Crossing Alert:         10
   Accumulation Interval:  0:00:10    Period: 15 minutes
   Location: SPM 39  Type: SMG4      Fabric: ATM
```

NT Standard log format and definitions

NT Standard log format:

<SOL><LogOfficeId>_<NodeName>_<POA><Threshold><LogName><ReportNumber>_<DateIndicator>_<TimeIndicator>_<SequenceNumber>_<EventType>_ <EventLabel>_<EquipmentIdentifier><EOLine><LOG BODY><EOLine><EOLog>

where:

- The < and > denote the beginning and end of a field.
- Bold text denotes optional fields that may or may not be there.
- _ denotes a space delimiter between fields.
- <SOL> = Start of Log delimiter - default is 0A0D in hexidecimal for NT STD and SCC2. (Line Feed followed by Carriage Return).
- <EOLine> = End of Line delimiter - default is 0A0D in hexidecimal for NT STD and SCC2. (Line Feed followed by Carriage Return).
- <LOG BODY><EOLine> = This sequence represents 0 to n lines of text in the log body each ending with EOLine - usually each line begins following an indentation of 8 spaces.
- <EOLog> = End of Log delimiter - default (in hexidecimal) is 200A0D0A0D00 for NT STD and 0A190A0D for SCC2

Office Identifier <LogOfficeId>:

Field Length/Format: variable length (1 to 12 characters)
Field Value(s): typically an 11-character Office CLLI name
Comment: This field's value corresponds to what is datafilled in your switch's table OFCVAR, tuple LOG_OFFICE_ID. A maximum of 12 characters can be datafilled into the LOG_OFFICE_ID tuple. Normally though, the value of this tuple in customer sites matches that of the Office CLLI name. The Office CLLI name has a standard length of 11 characters. In the switch it is datafilled in table OFCENG, tuple OFFICE_CLLI_NAME. (So OFFICE_CLLI_NAME and LOG_OFFICE_ID would be datafilled the same). In a log sent downstream to an OSS, the Office Identifier field will be seen by the OSS as 1 word with no spaces. No padding of spaces with occur with this field to make it 12 characters. ie If the log_office_id value is 6 characters in length, the space following the field will be the delimiter to the next field.

Node Name:

Field Length/Format: fixed length (8 characters)

Field Value(s): Node name that is left justified within the 8 character field.

Padding of spaces will occur to ensure 8 character length.

Comment: This optional field is generally not recommended for implementa-

tion. The value of the field is often "CM" which has low value and the extra 9 characters (8 + space) increases the length of the header. A longer header may result in line wrapping of the Equipment Identifier field which is present in some logs. A wrapped header is difficult for OSSs to accomodate.

Alarm Level Indicator / Priority of Action (POA) / Severity:
Field Length/Format: fixed length (3 characters)
Field Values: '***' or ' **' or ' *' or ' ' (Note the right justification of the *s).

Threshold:
Field Length/Format: 1 character field (Note: there are no space delimiters before/after)
Field Value(s): A + sign if the log is thresholded. A space if the log is not thresholded.

Log Name/Report Name/Log Prefix:
Field Length/Format: fixed length (4 characters)
Field Value(s): The log name is right justified within the 4 character field. Padding of spaces will occur at the beginning for names less than 4 characters. Eg. 'CARR' or ' SPM'. Note that the Log Name are the Report Number are considered a single entity. ie The SPM300 log.

Report Number:
Field Length/Format: fixed length (3 characters)
Field Value(s): The number will always be 3 digits. ie 100 to 999.

Date Indicator:
Field Length/Format: fixed length (5 characters); MMMDD where MMM is JAN through to DEC and DD is 01 through to 31
Field Value(s): Eg. DEC04

Time Indicator:
Field Length/Format: fixed length (8 characters); HH:MM:SS where HH is 00 through 23, MM is 00 through 59, and SS is 00 through 59
Field Value(s): Eg: 20:39:13 or 00:00:00 or 23:59:59

Sequence Number:
Field Length/Format: fixed length (4 characters); NNNN where the range is 0000 through 9999

Field Value(s): Eg. 0000 or 2358 or 9999. Once 9999 is reached, the number will go back to 0000. In SDM, STD_OLD and SCC2_OLD formats should increment the sequence number by 1 and SCC2/STD formats increment the sequence number in the same fashion as the CS2K does. In IEMS, SCC2/STD formats increment the sequence number by 1.

Event Type:
Field Length/Format: fixed length (4 characters);
Field Value(s): Left justified text with spaces at the end to pad to 4 character length. Examples: 'INFO', 'TBL ', 'FLT ', 'OFFL', 'SYSB', ' ', and so on.

Event Label:
Field Length/Format: variable length of characters; can contain more than 1 word separated by spaces
Field Value(s): Eg: "SDM BASE MAINTENANCE", or "CARRIER".

Equipment Identifier: (last field to be considered part of the header)
Field Length/Format: fixed length (4 characters) node type, followed by a space, followed by a numeric node number
Field Value(s): Node type portion is left justified and padded with spaces at the right if less than 4 characters. The node number portion is left justified. Eg. 'SPM 0', 'LIU7 43', 'SPM 71'.
Comment: This field is not found in all logs and should be considered rare. Known log types where this field is present are CARR and in some PM logs.

Log Body: (Not part of header. It follows the header).
Field Length/Format: Text in the log body usually follows an indentation of 8 spaces. Each line of text is variable in length.
Field Value(s): Can be anything but each unique log should typically always get sent out the door in the same format.

Notes

- Not all logs have an Equipment Identifier at the end of the header. There is no list of logs that have an Equipment Identifier and it would be an exhaustive task to determine all of which they are. Known log types that make use of the Equipment Identifier are CARR and PM. Since the Event Label can be any number of words separated by spaces, there is no obvious delimiter between the Event Label and the Equipment Identifier beyond the space that will be present. There are a couple things OSSs can do with this: take the Event Label and Equipment Identifier as just 1 string of

characters OR try to extract the Equipment Identifier out of the header independently of the Event Label. Note that the latter may not always be necessary because the body of the log may mention the Node as well. The presence of the Equipment Identifier in logs appears to be very rare and appears to be an old legacy thing that was done but isn't common practice anymore.

- For logs originating from the CS2000/XA-Core/DMS, Event Types and Event Labels for specific logs can be determined on the switch using the 'logutil' tool. In logutil, the 'listreps' and 'listroute' commands can be used to view that information. Note that the presence of a log in the tool's output list of logs does not mean that the log is actually active code where an OSS will see it downstream. Some are benign logs or development not yet completed that are sometimes listed there.

Example

```
LOGUTIL:
>listreps spm
Log  Rep.    Event              Suppressed/
Name  No. Class Type  Event Label Thresholded Syslog
-------------------------------------------------
 SPM  650   0   PASS
 SPM  651   0   FAIL
 SPM  300   0   TBL   Device Fault Report
 SPM  331   0   TBL   Failed Device Pro...
 ....
 SPM  709   0   INFO  SPM ISDNPROT DDM ...
 SPM  710   0   INFO  SPM ISDNPROT DDM ...
XX report(s)  printed
>listroute report spm 710
REPORT   SPM 710 (SPM ISDNPROT DDM Audit)  IS CLASS  0
ADDED:
DELETED:
```

- An actual SDM log sample file or feed should be analyzed for determination of a log's character by character format information. For determining things such as how many carriage returns there are between logs, or where spaces are, this is crucial. Note that a log header for a specific log very rarely changes in going from one software release to the next. The only fields that could change is the Severity, Event Type, Event Label and presence of an Equipment Identifier. Changes would be as a result of a feature change or resolve an issue with those fields' values.

Audio Codes Media Server (AMS)--available logs/faults

The following table lists the AMS logs available. The MS2010 server is for IP networks and uses the AudioCode TP-1610 card. For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference.*

AMS Logs/Faults available

Log/Fault	Description
AMS300	ac Board Resetting Cleared only by a acBoardEvBoardStarted trap; or ac Board Fatal Error
AMS301	ac Board Configuration Error
AMS302	ac Board Temperature Alarm
AMS303	ac Feature Key Error
AMS304	ac Board Call Resources Alarm
AMS305	ac Board Controller Failure Alarm
AMS306	ac Board Ethernet Link Alarm
AMS307	ac Board Overload Alarm
AMS308	ac Active Alarm Table Overflow
AMS500	ac Board Event Board Started. This trap is a signal to clear the active alarm table.
AMS501	cgw Administrative State Change

Audio Provisioning Server (APS)--available logs/faults

The following table lists the APS logs available. For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference.*

APS Logs/Faults available

Log/Fault	Description
APS398	Indicates a raised alarm in the APS device.
APS399	Indicates an alarm clear in the APS device.

Compact Call Agent (CCA)--available logs/faults

The following table lists the Compact Call Agent (formerly Call Agent (CA)) Logs/Faults available. These logs were also previously referred to as 3PC. For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference.*

Compact Call Agent supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled “IEMS Functionality.”

For details on the SDM protocol/format, refer to FCAPS documentation NN10023-111.

CCA Logs/Faults available

Log/Fault	Description
Network Element: Call Agent	For details on these Logs/Faults, refer to the Fault section of documentation related to Compact CS2K, NN10023-911.
CCA300	Response to a minor, major, or critical alarm; indicates that free space in RAM is low. Severity is determined by the amount of free space remaining.
CCA301	Response to a minor, major, or critical alarm; indicates one or more time segments has exceeded the threshold. Severity is determined by the number of time segments affected.
CCA302	Response to a minor, major, or critical alarm; indicates that free space on the root file system is low. Severity is determined by the amount of free space remaining.
CCA303	Response to minor, major, or critical alarm; indicates that one or more software processes have terminated abnormally. Severity is determined by the number of process affected.
CCA304	Response to a minor, major, or critical alarm; indicates that one or more Network File Systems is inaccessible. Severity is determined by the number of systems affected.
CCA305	Response to a minor, major, or critical alarm; indicates that time synch is lost to one or more NTP servers. Severity is determined by the number of servers affected.
CCA309	Response to a major or critical alarm; may be a PCI bus fault, an ECC memory fault, or a parity error. A critical alarm requires card replacement.
CCA315	SOS application simplex
CCA316	SOS application is out-of-service
CCA322	Image test failed
CCA331	Unable to communicate to mate via ethernet/fiber
CCA335	Ethernet interface down
CCA336	Unable to communicate to the network
CCA351	Response to major CON and APL alarms because the mate Call Agent unit is unavailable.
CCA355	Response to a minor alarm; indicates the inactive unit is jammed to prevent a SWACT.
CCA362	Response to a minor alarm; indicates at what point one or more REx tests has failed.
CCA365	System REx has not started for over 7 days
CCA375	One unit has a different CPU type than the other
CCA380	One unit has a different committed patch file version than the other
CCA600	Indicates the alarm referenced in log CCA300 has been cleared.
CCA601	Indicates the alarm referenced in log CCA301 has been cleared.
CCA602	Indicates the alarm referenced in log CCA302 has been cleared.
CCA603	Indicates the alarm referenced in log CCA303 has been cleared.

CCA Logs/Faults available

Log/Fault	Description
CCA604	Indicates the alarm referenced in log CCA304 has been cleared.
CCA605	Indicates the alarm referenced in log CCA305 has been cleared.
CCA609	Indicates the alarm referenced in log CCA309 has been cleared.
CCA615	Alarm referenced in CCA315 has been cleared
CCA616	Alarm referenced in CCA316 has been cleared
CCA620	Image test started
CCA621	Image test finished
CCA631	Able to communicate via ethernet/fiber
CCA635	Ethernet interface ok
CCA636	Able to communicate to the network
CCA651	Indicates the alarm referenced in log CCA351 is cleared and duplex operation is restored.
CCA655	Indicates the alarm referenced in log CCA355 is cleared.
CCA660	Response to a minor alarm; indicates that a REx test has started.
CCA661	REx test finished
CCA663	REx test rejected
CCA665	Alarm referenced in CCA365 has been cleared
CCA670	Swact failover started
CCA671	Swact failover finished
CCA675	Alarm referenced in CCA375 has been cleared
CCA680	Alarm referenced in CCA380 has been cleared
CCA685	An INFO log which indicates that the CCA disabled OSPF in the local ERS8600 (formerly Passport 8600).
CCA686	An INFO log which indicates that the CCA enabled OSPF in the local ERS8600 (formerly Passport 8600).

CS2000--available logs/faults

The following table lists the CS 2000 Logs/Faults available.
CS 2000 supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. The SDM would remain the CS2000 Core Manager but can forward the CS2000 logs to IEMS instead of directly to the OSS. For details on the IEMS interface, refer to the chapter in this document titled “IEMS Functionality.” For details on the logs/faults themselves, refer to the Fault Management section of CS 2000 FCAPS documentation, NN10083-911. For information on XA-Core logs and faults,

refer to NTP 297-8991-810, *XA-Core Reference Manual* and NN10275-909, *Fault Management Log Reference.*

CS2000 Logs/Faults available

Log/Fault	Description	
Network Element: CS2000 XA-Core		
ABI messaging alarms	Links down	ABI external messaging alarm Links Down - Alarm Set (or Alarm cleared).
	Severely Degraded	ABI external messaging alarm Severely Degraded - Alarm Set (or Alarm cleared).
	Degraded	ABI external messaging alarm Degraded - Alarm Set (or Alarm cleared).
Alarm Database logs	Report Alarm Log	Sent when requested by the entity that is reporting an alarm.
	Clear Alarm Log	Generated when a client clears an existing alarm in the alarms database managed by Alarmd.
	Alarm Summary Log	Sent periodically by Alarmd to summarize the Alarms in the database managed by Alarmd.
ATM log	ATM606	Generated when the network receives a UNI Release Complete message informing the craftsperson of an unsuccessful attempt to set up ATM bearer path (SVC) through the ATM network.
AUDT logs	AUDT105	Trunk state incorrect.
	AUDT106	Call is forced down due to the release of a trunk.
	AUDT109	Trouble conditions detected.
	AUDT110	Terminal trunk state is invalid.
	AUDT116	Terminal state indicator (TSI) of an idle trunk is invalid.
	AUDT117	TSI (terminal state indicator) of a given call state and the CCB (call condense block) TSI do not match.
	AUDT209	Generated whenever the audit process finds a problem with a multi CPTLB.
Authorization logs	SESM MI2 applications have user authorization by group. Authorization failures generate logs through the SSPFS log reporting service.	
Baseln alarm		“Baseln” alarm is raised whenever any XA-Core Field Replaceable Unit (FRU) installed in the shelf is not at Hardware (HW) or Firmware (FW) baseline. Only the Major level is used.
BKM logs	BKM600	Generated if a system backup is successful.
	BKM601	Generated if a system backup fails.
	class_security.ver01	Generated when a user attempts to invoke the Backup Manager and does not have the correct permissions.

CS2000 Logs/Faults available

Log/Fault	Description	
C7UP logs	C7UP100	No acknowledgment received from far-end office after circuit reset, group circuit reset, blocking or unblocking, group blocking or unblocking, or release messages. For field descriptions and actions, see Logs Reference Manual (Volume 1), 297-2621-840.
	C7UP101	Unreasonable message received on trunk.
	C7UP102	CCS7 connection is released due to abnormal condition.
	C7UP103	Blocked or unblocked circuit conditions.
	C7UP104	Group blocking or unblocking conditions.
	C7UP105	Unsuccessful ISDN call attempt.
	C7UP106	Shortage of resources.
	C7UP107	Request for continuity check test by an IAM (Initial Address Message), a continuity check request (CCR) message, or a demand continuity test (DCT) from the MAP.
	C7UP109	ISUP trunk state change to match far-end office trunk state.
	C7UP110	Serious communication problem with far-end office.
	C7UP111	Outgoing call attempt failure.
	C7UP112	Call in progress has received an unreasonable message in the current call state.
	C7UP113	ISUP trunk maintenance problem.
	C7UP114	Response from far-end office not received from a REL (circuit release) or RSC (reset circuit) message.
	C7UP119	ISUP has not received, from the far-end office, second GRS (circuit group reset), CGB (circuit group blocking), or CGU (circuit group unblocking) message.
	C7UP120	ISUP invalid number in circuit-group message RANGE field (0 or a number greater than 23).
	C7UP130	System has detected that the hop counter (HC) limit has been exceeded. For details, see Logs Reference Manual (Volume 2), 297-2621-840 and the CS2000 fault information.
	C7UP300	ISUP trunk time-out waiting for acknowledgement from first RLC (remote line controller).
	C7UP301	System has received a release message with the value “Exchange Routing Error.”
CALX logs	CALX300	Indicates unknown cause for a Calix-related issue.
	CALX301	Indicates a service-affecting issue related to Calix.
	CALX302	Indicates a non-service-affecting issue related to Calix.

CS2000 Logs/Faults available

Log/Fault	Description	
	CALX501	Indicates a Calix remove event.
	CALX502	Indicates a Calix restore event.
	CALX800	Indicates a Calix Threshold Crossinig alert is cleared.
	CALX801	Indicates a Calix Threshold Crossinig alert is standing.
	CALX802	Indicates a Calix Threshold Crossinig alert is transient.
	CALX803	Indicates a Calix Threshold Crossinig alert is not applicable.
CARR logs	CARR300	Carrier failure event occurred. Also applies to STS-1 carrier. For more info, see general SPM fault information.
	CARR310	Carrier failure events are cleared. Also applies to an STS-1 carrier. For more info, see general SPM fault information.
	CARR330	A protection switch has occurred. A previously inactive carrier in the protection group takes over as the active carrier.
	CARR331	A protection switch was attempted but failed.
	CARR340	The inactive carriers in a protection group have changed state in such a way that they cannot carry traffic. The protection group is now running in simplex mode.
	CARR341	Both carriers have become available and normal protection switching can occur.
	CARR500	Carrier state change to InSv from ManB or SysB. For more info, see general SPM fault information.
	CARR501	Carrier state change to CBsy from ManB or SysB. For more info, see general SPM fault information.
	CARR510	Carrier state change to SysB from InSv or CBsy. For more info, see general SPM fault information.
	CARR511	Carrier state change to SysB from InSv or CBsy. For more info, see general SPM fault information.
	CARR512	OC3 carrier state change to CBsy from InSv, ManB, or SysB. For more info, see IW-SPMgeneral SPM fault information.
	CARR600	Value of an instance of apsChanSwitchover increments.
	CARR800	Threshold crossing alert (TCA) for a metered performance parameter has been cleared. For more info, see general SPM fault information.
	CARR810	TCA event for metered performance parameter has occurred. For more info, see general SPM fault information.
	CARR811	TCA event for non-metered performance parameter has occurred. Also applies to STS-1 carrier on MG4000. For more info, see general SPM fault information.

CS2000 Logs/Faults available

Log/Fault	Description	
CICM logs	Component initializes on master	An INFO log for a normal start-up event.
Component initializes on slave		An INFO log for a normal start-up event.
Slave component requests a bulk sync		An INFO log for a normal start-up event.
Bulk sync of data completes		An INFO log for a normal start-up event.
Component on master receives notification to SWACT		An INFO log generated as components perform an operator-initiated switch of activity.
Component on slave receives request from its counterpart to assume the role of the master		An INFO log generated as components perform an operator-initiated switch of activity.
Component on slave completes transition to active		An INFO log generated as components perform an operator-initiated switch of activity.
Component on master receives acknowledgment from mate that i t is now active		An INFO log generated as components perform an operator-initiated switch of activity.
CICM logs	CICM351	An alarm log to warn that , although started, the CICM/CICM-EM was unable to retrieve its basic configuration data, so it may be using old configuration data that is not up to date.
	CICM363	Raised when an INFO alarm occurs that indicates Subtract ConnectionAck cannot determine the destination for a message.
CEM logs	CSEM300	The log that encapsulates CS2K logs which have severity and are part of set and clear pairs.
	CSEM600	The log that encapsulates CS2K log which do not have severity.
CHKPT logs	CHKPT401	INFO log to inform the administrator that the Checkpointing OMs have been reset to 0 on the Active instance.

CS2000 Logs/Faults available

Log/Fault	Description	
Client Session Monitor Security logs		The following security INFO logs are generated when the Client Session Monitor processes the notification of the authentication and client lifetime events: • User authenticated. • Successful session start. • Session stopped due to user exit. • Active session manually marked as done. • Client start or stop event is requested, but session ID is not valid.
CPU Occupancy Alarms		CPU occupancy alarm Minor occurs at 80%, Major at 85%, and Critical at 90%.
CRTM logs	CRTM700	An INFO log which indicates that the user has requested a new private key.
	CRTM701	An INFO log which indicates that the user selected to generate a self-signed certificate.
Database logs	DB600	Generated when an attempt to allocate a database connection encounters an I/O error. These errors can occur when the database has been stopped momentarily for administrative purposes.
	DB601	Generated when an attempt to allocate a database connection encounters detects that the connection is already closed. These errors can occur when the database has been stopped momentarily and then again started.
	DB602	Generated when an attempt to allocate a database connection encounters an invalid password error. These errors can occur when the database log in password for a database user is changed.
	DB603	Generated when an attempt to allocate a database connection encounters maximum database sessions exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity.
	DB604	Generated when an attempt to allocate a database connection encounters maximum database processes exceeded error. These errors can occur when an unusual event has occurred that caused sustained high levels of system activity.
Data Server process logs		Desc Msg: Could not read switch name Desc Msg: Could not create tuple Desc Msg: Could not read VRINV table Desc Msg: Could not initialize OM Acess Desc Msg: Could not initialize OM Acess Desc Msg: Could not get keyinfo object, excluding group , <group> Desc Msg: Could not get key, excluding group , <group>

CS2000 Logs/Faults available

Log/Fault	Description	
		Desc Msg: Could not get info, excluding group , <group>
		Desc Msg: Could not register initialization timer
		Desc Msg: Rejecting register request for excluded group: <group>
		Desc Msg: Could not open listening connection
		Desc Msg: Could not open listening connection: <service name>
DBSE log	DBSE300	A Session Server Provisioning Trouble (TBL) log which is generated any time a change in database connectivity is detected. It reports 'No Solid DB Connection' when database connectivity is lost. It reports 'Solid DB Connection Restored' when database connectivity is reestablished. Correlates to the critical alarm "No Database Connection" raised when a loss of connectivity to the database is detected.
DPL logs	DPL100	DPL100 indicates that reconstruction of the VID resource pool has started.
	DPL101	DPL101 indicates that reconstruction of the VID resource pool has completed.
DQoS alarm	This raises a DQoS link alarm when link failure occurs.	
EMJS logs	EMJS340	Raise/Clear Alarms for the state of SNMP Communication with the device during its OM Collection.
	EMJS341	Log for Complete failure of SNMP Collection Job
	EMJS350	FTP/SFTP/STREAM communication Failure Event per device.
	EMJS360	Raise or Clear log for the error occurred in generating a Report File.
	EMJS371	Raise or Clear log for the error/successful execution of Transfer jobs. Or, Raise log for Transmit failures during FTP or SFTP.
	EMJS540	Collection Job State Changed Logs. Executed. Stopped. Disabled.
	EMJS560	Report Job State Changed Logs. Executed. Stopped. Disabled.
	EMJS570	Report Job State Changed Logs. Executed. Stopped. Disabled.
	EMJS607	Log for MDM Performance & Fault Swact.
	EMJS640	Log for: Invalid Template Version. Invalid OIDs for the device. Invalid CVS File Format.
	EMJS641	Log Successful processing of SNMP Collection Job.
	EMJS642	Partial/Complete Failure of SNMP Collection Job.
	EMJS651	Log for Successful Processing of CSV Collection Job.
	EMJS652	Log for Partial/Complete failure in processing of CSV Collection Job.
	EMJS661	Log for complete success for Report Job.
	EMJS662	Log for partial/complete failure for Report Job.
	EMJS671	Log for Successful transfer job Attempts.

CS2000 Logs/Faults available

Log/Fault	Description	
	EMJS672	Log for partial/complete failure of transfer job attempts.
	EMJS840	Threshold raise alarm.
	EMJS841	Threshold clear Alarm.
EMSS logs	EMSS300	Produced when ever the client side PAM + RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
	EMSS301	Poroduced when ever a serious problem is detected by the RADIUS Server in the process of handling a given authentication request. Problems that fall into this category are unexpected exceptions thrown by RADIUS Server plug-ins (as a result perhaps of improper RADIUS server setup/configuration or a critical RADIUS server dependency being unavailable). Recovery Action: Check the status of Sun IS and restart if necessary.
	EMSS302	Produced when the radius server policy plugin detects no single-sign-on token is available indicating there is a problem with the Sun Identity Server or that it is in fact not running.
	EMSS303	Indicates a communication failure with the PAM+Radius group daemon. This log indicates that the pam_radius_auth cannot establish or maintain a communications session with the group daemon on the client machine.
	EMSS304	Produced when the pam_mkhomedir module invokes the script mkhomedir but the script does not return within the timeout time (default 30 seconds).
	EMSS305	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
	EMSS306	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
	EMSS307	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
	EMSS308	Produced when ever the client side Pam + RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
	EMSS309	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
	EMSS310	Produced when ever the client side PAM+ RADIUS SPI is unable to communicate with the server-side RADIUS Interface.
	EMSS311	Produced when ever the client side PAM+ RADIUS SPI is unable to read information for required to communicate with the configured RADIUS server(s) from the /etc/raddb/server file
	EMSS312	Produced when ever the pam_mkhomedir module tries to get the user information from NSSwitch by using getpwnam and fails.
	EMSS313	Produced when ever the radius server health monitor detects the radius process is not functional.

CS2000 Logs/Faults available

Log/Fault	Description	
	EMSS314	Produced when ever the identity server health monitor detects the identity server process is not functional.
	EMSS315	Produced when ever the PAM login servlet health monitor detects the PAM login servlet is not functional.
	EMSS316	Produced when ever the pam_mkhomedir module checks the ownership of the script and the script is not owned by the user root.
	EMSS317	Produced when ever the pam_mkhomedir module tries to get the script and the script is not there.
	EMSS318	Produced when ever the pam_mkhomedir module tries to check the euid of the current process and finds the euid is not root.
	EMSS319	Produced when ever the module tries to get the configuration file and the file is not there.
	EMSS320	Produced when ever the module tries to read the contents of the configuration file but fails.
	EMSS321	Produced when ever the module tries to get the auth url but the url got is null.
	EMSS322	Produced when ever the module is timed out during the authentication. The default timeout is 30 seconds.
	EMSS323	Produced when ever the module tries to get the configuration file and the file is not there.
	EMSS324	Produced when ever the module tries to read the contents of the configuration file but fails.
	EMSS325	Produced when ever the module tries to get the auth url but the url got is null.
	EMSS326	Produced when ever the module is timed out during the validation. The default timeout is 30 seconds.
	EMSS327	Produced when ever the script has an error to access the directory or files.
	EMSS330	Produced when ever the module failed to initialize single sign on facility. SSO tokens will not be generated.
	EMSS331	Produced when ever the module could not authenticate user due to unhandled internal error.
	EMSS332	Produced when ever there is no single-sign-on token available after authentication.
	EMSS333	Produced when ever the module could not generate single-use tokens due to unhandled internal error.
	EMSS334	Produced when ever the module could not read user's unix profile due to unhandled internal error.
	EMSS351	Produced when ever an exception is caught while making request to the servlet.

CS2000 Logs/Faults available

Log/Fault	Description	
	EMSS352	Produced when ever the module failed to authenticate.
	EMSS353	Produced when ever there is an error processing response from the servlet.
	EMSS354	Produced when ever the module failed to attempt to access the shadow database by user with uid <uid>.
	EMSS360	Produced when ever the module failed to initialize SAML.
	EMSS361	Produced when ever the module failed to process the configuration file.
	EMSS362	Produced when ever the module failed to configure log4cpp.
	EMSS363	Produced when ever the module failed to read the "password_file" roperty from the configuration file.
	EMSS364	Produced when ever the module failed to find the configuration file.
	EMSS600	An INFO log produced when ever the PAM Radius daemon modifies the /etc/passwd or /etc/group files.
	EMSS601	An INFO log produced when ever there are successful or failed authentication requests of the authentication module.
	EMSS602	An INFO log produced when there are successful or failed PAM SPI events from PAM + Plug-Ins.
	EMSS603	An INFO log that indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token create event. Sensitive token information is not included in these logs.
	EMSS604	An INFO log that indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token destroy event. Sensitive token information is not included in these logs.
	EMSS605	An INFO log that indicates a SunOne Identity Server Single Sign On (SSO) token activity for a token timeout event. Sensitive token information is not included in these logs.
EXT log	EXT108	Generated upon raising and clearing of EXT alarm HIGH_MEM_BLOCKING.
EXT alarm	HIGH_MEM_ BLOCKING	Appears at the MAPCI EXT alarm banner when there is a high memory blocking level detected in the system. Correlates to XACP300 log when raised, and to XACP500 log when cleared.
FPS log	FPS100	Generated when the FPS counter of a subscriber is loaded.
GAME logs	GAME101	Created if the RSPTMOUT OM count is greater than zero. The log is created during the RSPTMOUT OM transfer period and records the RSPTMOUT OM count value.
	GAME102	Created if RSPTMOUT OM count becomes equal to the office parm T1_TIMER _EXPIRY_MSG_SUPPRESS threshold value.
IAA logs	IAA314	Generated whenever an IAA module fails to initialize. The reason text field may contain one of 7 possible strings.

CS2000 Logs/Faults available

Log/Fault	Description	
	IAA342	Generated whenever an IAA module cannot communicate with other IAA modules, i.e., EMDA.
	IAA343	Generated when a PCEM processing error occurs. The reason text field may contain one of 6 possible strings.
	IAA344	Generated when an IAA module cannot create an audit entry.
	IAA345	Generated when an IAA module detects a configuration problem. The reason text field may contain one of 2 possible strings.
	IAA346	Generated when an IAA cannot communicate to the downstream RKS pair or DF. The reason text field may contain one of 4 possible strings.
	IAA347	Generated when an IAA module detects a problem when trying to manage its filesystem storage.
	IAA641	Generated when an IAA module goes into service.
	IAA646	Generated when communications between the IAA and the downstream RKS pair or DF has been restored.
	IAA701	Generated when the data being process by the IAA is corrupted.
IEMS logs	IEMS350	Indicates that an IEMS device is changed to an unmanaged state by the user.
	IEMS398	Raise Log for a Loss of Communication with the EMS/NE
	IEMS399	Clear Log for regain of Communication with the EMS/NE
	IEMS601	SNMP trap from unknown device Log
	IEMS602	Unknown SNMP trap from managed device Log
	IEMS603	Missed Notifications Log. Also generated whenever IEMS detects a trap loss, i.e. when the sequenceNumber in the trap is greater than the previous sequenceNumber plus one.
	IEMS604	Generated only if the incoming clear log does not have a logname and lognumber in it AND does not have a matching raise alarm in the IEMS database.
	IEMS605	Log for Manually Cleared Alarms by the user in IEMS GUI
	IEMS606	Log generated by DBCleanUpPolicy. Threshold crossed log. Log for Data clean up
	IEMS607	Automatic Clear alarms by IEMS during resynchronization of alarms.
	IEMS608	Generated when an alarm in IEMS has been cleared automatically due to an aging policy coming due. In SN08, by default the ERS8600 (formerly Passport 8600) has a 7 day aging policy implemented.

CS2000 Logs/Faults available

Log/Fault	Description	
	IEMS609	Generated by IEMS when it clears the entire active alarm list for a managed component. Generally this might happen for SNMP managed devices when they send a cold start trap. OSSs can use this log as an indicator that IEMS no longer considers the alarms against that component valid and has removed them. The OSS may wish to consider clearing the trouble tickets against that managed component.
	IEMS610	Generated by IEMS when the /data disk partition of the SSPFS platform in which it resides exceeds 80% utilization and the disk space cleanup job detects it. When detected, IEMS will attempt to bring /data under 80% utilization by removing OM report directories under /data/oms. Sub-directories will be removed as required and will start with the oldest first (that named 7), then 6 and end with 2. The 1 directory will not be removed.
	IEMS614	Generated whenever IEMS receives an OSI State Change SNMP Notification (nortelNMIneOSIstateChangeNortification).
	IEMS615	Generated whenever IEMS receives a Stateless Clear (Orphaned Clear), that is, whenever IEMS receives a Clear from the Southbound device, for which IEMS could not identify the matching raise from its database. Hence the OSS should use this log to identify some kind of misleading log information that is being sent from the Southbound devices. NOTE: This log is not generated for MDM devices.
	IEMS650	Indicates that an IEMS device is changed to a managed state by the user.
IEMS Security logs		Generated for any unauthorized configuration access attempts of measurement collection jobs.
		Generated for any unauthorized configuration access attempts of measurement transfer jobs.
		Generated for any unauthorized configuration access attempts of measurement report jobs.
		Generated when a tuple is added for the IP address in the security server.
		Generated when the RADIUS secret is updated for the IP address in the security server.
		Generated when a delete operation occurs for the IP address in the security server.
		Database password change logs: successful change, invalid user, and invalid machine used.
		Certificate creation and change logs: fresh certificate installed, and certificate changed.
		ssh Key creation and change logs: ssh key change, and invalid user for ssh key change.

CS2000 Logs/Faults available

Log/Fault	Description
	IPSec IKE policy creation and deletion logs: • IKE rule or entry added or deleted • Problem occurred loading IPSec rules on other cluster unit • Could not Sync IPSec data • IKE rule, key, or entry could not be added or deleted • IKE configuration data or preshared key data could not be updated IPSec IKE Key Change logs: • Preshared key modified • Attempt to modify Preshared key • Could not change Preshared key • IKE preshared key data could not be updated • Problem occurred loading IPSec rules on other cluster unit IPSec IKE Key Change logs (continued): • Could not Sync IPSec data • Could not modify preshared key
IEMS Security alarms	Password expiration warning alarm (Info), relates to SPFS350 log. Password expiration alarm (Minor), relates to SPFS350 log. Account expiration warning alarm (Info), relates to SPFS350 log. Account expiration alarm (Minor), relates to SPFS350 log. Certificate expiration alarm (Minor), relates to SPFS350 log. Certificate expiration alarm clearing, relates to SPFS350 log.
logNormalizer and log NormSAF Process logs	Desc Msg: Event file <EventFileName> was not found ...logNormalizer exiting Desc Msg: Event delimiter cannot be more than one charcter long ...logNormalizer exiting Desc Msg: Event file "<<EventFileName<<" is empty ..logNormalizer exiting Desc Msg: Event file "<<EventFileName<<" had errors ..logNormalizer exiting Desc Msg: Mapper file "<<MapperFileName<<" was not found ...logNormalizer exiting Desc Msg: Mapper delimiter cannot be more than one charcter long ...logNormalizer exiting Desc Msg: Mapper file "<<MapperFileName<<" is empty ..logNormalizer exiting Desc Msg: Mapper file "<<MapperFileName<<" has errors .."<<argv[0]<<" exiting Desc Msg: Mapping information parsing error for log "<<logName<<" empty information or wrong delimiter used

CS2000 Logs/Faults available

Log/Fault	Description	
	Desc Msg: output file "<<outputFileName<<" could not be opened	
	Desc Msg: lostLogFile "<<lostLogFileName<<" could not be opened	
	Desc Msg: lostLogFile "<<outputFileName<<" is empty	
	Desc Msg: lostLogFormat string is empty	
	Desc Msg: lostLogTriggerSize is empty	
	Desc Msg: lostLogVisibleMsg string is empty	
	Desc Msg: lostLogVisLog string is empty	
	Desc Msg: sdmLogList is empty	
	Desc Msg: probeTimer string is empty	
	Desc Msg: checkLen string is empty	
	Desc Msg: No Lost Log Trigger message has been specified	
	Desc Msg: Could not send events to agent. Agent removed from output list	
	Desc Msg: Unknown log format. No mapping will be done for input	
LOST logs	LOST101	Generated when an outgoing message fails to find an open path to the destination or an incoming message fails checks done by the receiving application.
	LOST102	Generated when an incoming message cannot be forwarded to Call Processing because software resources (buffers) have been exhausted or the limit for outstanding messages has been exceeded and no additional messages can be enqueued.
	LOST103	Generated when a message that originated from the CM is rebounded back to the CM for additional processing because a node intermediate along the path was unable to deliver the message to the final destination. The failure code instructs the CM to attempt to re-route the message over an alternate path but the original message contains the re-route inhibit flag
	LOST104	Generated when an outgoing message fails a VID-to-TID translation or an incoming message fails sanity checks on the terminal identifier (TID).
	LOST105	Generated when an outgoing message fails to find an open CM-MS link. Also generated when a message that originated from the CM is rebounded back to the CM for additional processing because a node intermediate along the path was unable to deliver the message to the final destination. The failure code instructs the CM to attempt to re-route the message over an alternate path but sanity checks fail on the original route.
	LOST106	Generated when a message fails application sanity checks. Also generated when a message that originated from the CM is rebounded back to the CM for additional processing because a node intermediate along the path was unable to deliver the message to the final destination. The failure code indicates “unspecified reason.”

CS2000 Logs/Faults available

Log/Fault	Description	
	LOST107	Generated when an incoming message specifies an unassigned terminal identifier (TID).
	LOST108	Generated when the buffer (containing an outgoing message) is reclaimed by a system audit. The message is deemed to be stale as the buffer has not been accessed for a long period of time.
	LOST109	Generated when a message that originated from the CM is rebounded back to the CM for additional processing because a node intermediate along the path was unable to deliver the message to the final destination. The failure code instructs the CM to attempt to re-route the message over an alternate path but all alternatives have been previously tried without success.
	LOST110	Generated when Call Processing gets a failure indication on attempting to output a message).
	LOST111	Generated when an incoming message cannot be delivered. The specific failure reason is displayed in the log.
	LOST112	Generated when an outgoing message fails sanity checks on length or an incoming message fails sanity checks on length.
	LOST113	Generated when when the needed software resources are again available. The log displays the number of discarded events during the period of exhausted resources
	LOST114	Generated when an incoming (BFP) message cannot be forwarded to Call Processing due to message buffer exhaustion. This is similar to the more generic LOST102 log
	LOST115	Generated when the (BFP) buffer (containing an incoming message) is reclaimed by a system audit. The message is deemed to be stale as the buffer has not been accessed for a long period of time. This is similar to the more generic LOST108 log.
	LOST116	Generated when an outgoing message encounters a failure. The specific failure reason is displayed in the log
	LOST117	Generated when an outgoing message encounters a failure. The specific failure reason is displayed in the log.
Media Proxy alarm	Media Proxy Communications Failure	Severity varies, based on the number of media proxies that are out of service as compared to the number of media proxies provisioned checked on a 5-minute polling period. Critical - Over 50% of media proxies disabled. Major - Over 20% of media proxies disabled. Minor - Any media proxies disabled.
MGTH logs	MGTH300	MGTH300--acBoardEvResettingBoard
	MGTH301	MGTH301--acBoardFatalError
	MGTH302	MGTH302--acBoardConfigurationError
	MGTH303	MGTH303--acBoardTemperatureAlarm

CS2000 Logs/Faults available

Log/Fault	Description	
	MGTH307	MGTH307--acBoardEthernetLinkAlarm
	MGTH309	MGTH309--acActiveAlarmTableOverflow
	MGTH312	MGTH312--acOperationalStateChange
	MGTH313	MGTH313--acKeepAlive
	MGTH314	MGTH314--acNATTraversalAlarm
	MGTH500	MGTH500--acBoardEvBoardStarted
	MGTH501	MGTH501--acgwAdminStateChange
	MGTH600	MGTH600--acEnhancedBITStatus
	MGTH601	MGTH601--dsx1LineStatusChange
	MGTH800	MGTH800--acPerformanceMonitoringThresholdCrossing
NCAS logs	NCAS325	An alarm log generated when a critical alarm is raised because the NCAS Link goes down. It is also generated when the alarm is cleared when the NCAS Link comes up
	NCA501	Generated when an Out-of-Band REFER Request that has been received by the Session Server does not validate and this the request can not be accepted.
	NCAS502	Indicates Unable to Establish Connection with SCPLite.
	NCAS601	Raised when a new NCAS Link is created.
NGSS logs	NGSS700	Indicates when a SIPT CS2CS call is rejected because it would exceed the LIMIT setting of the CS2B0008 SOC.
	NGSS701	Generated when a CS2AS call is rejected because it would exceed the LIMIT setting of the CS2B0009 SOC. The SIPT call is not allowed to complete through the NGSS. The CS2ASOV register in OM group NGSSOM is pegged.
NLClient logs and NLServer logs	Desc Msg: Failed to register for connection to export Server at service<service name>	
	Desc Msg: Failed to register for connection to Data Server at port <port number>	
	Desc Msg: Failed to register for connection to Data Server at service <service name>	
	Desc Msg: Failed to register for signals	
	Desc Msg: Failed to send error	
	Desc Msg: Communications not initialized	
	Desc Msg: Input from unknown end point	
	Desc Msg: Failed to send registration message to Data Server	
	Desc Msg: Failed to send deregistration message to Data Server	
	Desc Msg: Invalid Message from archive	

CS2000 Logs/Faults available

Log/Fault	Description
	Desc Msg: store is disconnected:deregister the connection
	Desc Msg: Receive from Archive failed
	Desc Msg: Unreadable Data Server message type
	Desc Msg: Unreadable OM report
	Desc Msg: Failed to send correlation error data to Archive
	Desc Msg: OM Registration failed
	Desc Msg: Unreadable registration response
	Desc Msg: OM DeRegistration failed
	Desc Msg: Unreadable deregistration response from Data Server
	Desc Msg: Failed to send CM info request to Data Server
	Desc Msg: Failed to send deferred registration message to Data Server
	Desc Msg: Failed to send re-registration message to Data Server
	Desc Msg: Fatal status change
	Desc Msg: Unreadable OM status received from Data Server
	Desc Msg: Could not get GroupInfo
	Desc Msg: Failed to send nlGrpInfoRsp data to Archive
	Desc Msg: Unreadable CM info message from Data Server
	Desc Msg: Could not open License File
	Desc Msg: Unexpected message type from Data Server
	Desc Msg: Lost connection to Data Server
	Desc Msg: Receive from Data Server failed
	Desc Msg: Communications not initialized
	Desc Msg: Failed to send end_of_report msg to store
	Desc Msg: Connection from unknown end point
	Desc Msg: Switch name unknown
	Desc Msg: Arithmetic overflow in correlation <correlation name>
	Desc Msg: Failed to send OM data to Archive
	Desc Msg: Error while doing a send to the Agent, discard send queue
	Desc Msg: Port for the service <NLservice name> is not available
	Desc Msg: Failed to register for connection to export Server at service <service name>
	Desc Msg: Failed to register for connection to Data Server at port <port num>
	Desc Msg: Failed to register for connection to Data Server at service <service name>

CS2000 Logs/Faults available

Log/Fault	Description	
NMSS logs	NMSS115	Generated if an error occurs while sending NMS TCAP messages to SCTP.
	NMSS116	Generated if an error occurs while receiving NMS TCAP messages from SCTP.
	NMSS117	Generated if an error occurs while sending NMS REJ messages to SCTP.
	NMSS118	Generated if an error occurs while receiving NMS REJ messages from SCTP.
NWM logs	NWM102	Cancel To (CANT) control is applied to or removed from a specific trunk group. For details, see CS2000 configuration information and Solution-level configuration information.
	NWM103	Cancel From (CANF) control is applied to or removed from a specific trunk group. For details, see CS2000 configuration information and Solution-level configuration information.
	NWM104	SKIP control is applied to or removed from a specific trunk group. For details, see CS2000 configuration information and Solution-level configuration information.
	NWM107	Flexible ReRoute (FRR) control is applied to or removed from a specific trunk group. For details, see CS2000 configuration information and Solution-level configuration information.
	NWM202	HTR code has been added to or deleted from EADAS or MAP terminal. For details, see CS2000 configuration information and Solution-level configuration information.
PATC log	PATC300	Major alarm and log to indicate when a restart is required for a patch on a specific card. PATC300 is generated when a patchAlarmFault is received from an MG9000 DCC card.
RMGC log	When a major RMGC alarm is raised or cleared, an SNMP trap is sent from the GWC to the GWC EM.	
RSIP status log	The RMGC application produces a syslog performance report once an hour which is sent to the Solaris syslog daemon. It contains the counts of the total number of RSIPs processed successfully and the number failed.	
SFPS log	SFPS100	Generated when a craft person enters an invalid LFPS password three times.
SIP Gateway Application CallP Alarms	Database Access Alarm	(Critical) occurs when the CallP application tries to access the database and it fails due to a loss of connectivity between the database and the CallP application. Correlates with the 310 log.
	ACL Trouble Alarm	Raised when incoming SIP messages are dropped due to Access Control List enforcements. The severity of the alarm is based on the number of packets dropped in last 15-minute time interval. Correlates with the SIPC750 log.

CS2000 Logs/Faults available

Log/Fault	Description	
SIPC logs	SIPC301	A critical log that is generated when the SIP Gateway Call Processing Application will not receive any incoming SIP messages due to Access Control List being enabled and no valid entries in the Remote SIP server or ACL list.
	SIPC310	"SIP CallP No Database Connection" is associated with the generation of the Critical alarm due to a loss of connectivity between the database and the CallP application. The same log number is used for "SIP CallP Database Connection Established" when the connection that caused the first SIPC 310 log is re-established and the alarm is cleared.
	SIPC650	An informational log that is generated when the CallP application goes to get data from the database for a particular table and no data is found.
	SIPC750	Generated when the SIP Gateway Call Processing Application drops incoming SIP messages due to Access Control List restrictions. A Minor, Major, or Critical log is generated based on the number of SIP messages dropped in the last 15 minutes.
SIPGW log	SIPGW700	An INFO log that contains one of 34 possible log messages related to SIP call processing.
SIPM logs	SIPM300	A Trouble log which is generated any time the SIP Gateway Application Maintenance software encounters an unexpected condition.
	SIPM301	A Trouble log which is generated any time the SIP Gateway Maintenance Trouble Alarm is raised or lowered.
	SIPM302	A Trouble log which is generated any time the SIP Gateway Maintenance Sync Trouble Alarm is raised or lowered. This occurs when the SIP Gateway application state gets out of sync, or gets back in sync in a duplex Session Server configuration.
	SIPM500	An INFO log which is generated any time the SIP Gateway Application maintenance state changes.
SIPS logs	SIPS300	Generated during the alarming of dropped connection requests (due to either the threshold being crossed for throttling connections, or due to attempting to use TLS when TLS is not enabled). The severity of the alarm indicates the threshold that was crossed, 10 dropped connection requests in a minute for a MINOR, 50 dropped requests for a MAJOR, and 100 dropped requests (or more) for a critical. The alarm is raised for a minimum of 30 minutes.
	SIPS301	Generated during authentication failure events. The alarmd process log indicates the level of trouble (CRIT indicates a very serious problem, MINOR may be transient or the beginning of a series of authentication failures).

CS2000 Logs/Faults available

Log/Fault	Description	
	SIPS302	Generated as a result of the alarm process check to ensure the Local Server certificate continues to be valid. The expiration date contained in the certificate is checked on a daily basis, and when the expiration of the certificate will occur within 31 days (MINOR), 15 days (MAJOR), or 5 days (CRIT), the alarm is raised, with this log. For certificates that have already expired, the CRIT alarm and log is generated, and authentication failures will be output for any connections that are attempted.
	SIPS303	Certificate Mismatch in Server Certificate, generated if the two sets of files on the active and inactive sides do not match each other. An alarm is also raised.
	SIPS305	Generated during the initialization of the Call Processing application (i.e. during the unlock). If one of these critical logs comes out, it means that there is a problem with the initialization, and the application is unable to start.
	SIPS308	Failed Certificate Policy Check, generated when enough certificate policy failures have occurred to generate an alarm. An alarm is also raised.
	SIPS600	Generated during the connection set up of the Call Processing application. When the 'monitor OMs' log comes out, ensure that the threshold levels set for connection throttling are reasonable for the size of the office. If the 'TLS is not enabled' message comes out, ensure that the initialization of the call processing application worked correctly.
	SIPS601	Generated during authentication failure events. This INFO log indicates the reason for the authentication failures.
	SIPS604	Generated during the initialization of the Call Processing application (i.e. during the unlock). This log indicates when the current local certificate will expire. The Certificate Effective Date log is added in SN09.
	SIPS605	Generated during the initialization of the Call Processing application (i.e. during the unlock). This log indicates that TLS has been enabled. Expect a SIPS604 log along with this log.
	SIPS606	Generated when there is a problem importing the trusted certificate provisioned via the web interface in the database.
	SIPS608	TLS Certificate Policy failure, generated when the remote side of the connection presents a certificate that does not conform to the selected local certificate policy.
	SIPS609	Security Parameter Changed, generated whenever a TLS Security Parameter is changed by the user.

CS2000 Logs/Faults available

Log/Fault	Description	
SPFS logs	SPFS310	SPFS 310 is generated for the following reasons: • when the CPU load Average threshold is exceeded, or when the related Major or Minor alarm is cleared. • when the Swap Space usage threshold is exceeded, or when the related Critical or Major alarm is cleared. • when the Memory usage threshold is exceeded, or when the related Major or Minor alarm is cleared.
	SPFS350	SPFS 350 is generated when the File System is not mounted, the File System usage threshold is exceeded, a File System read/write failed, or when the related Critical, Major or Minor alarm is cleared.
	SPFS350	A Trouble log which is generated any time the SIP Gateway Maintenance Trouble Alarm is raised or lowered. Also generated to indicate Password, Account, or Certificate expiration warning.
	SPFS380	Indicates that the syslog system has failed to write logs, or that it has resumed writing logs.
SSPFS security logs	SSPFS security logs are generated whenever any security affecting parameter is changed from the CLI. They include the following events: Login Retries Limit--whenever an MSAP access threshold is changed. Login Session (User Inactivity) Timeout-- whenever an MSAP time interval that controls keyboard lockout is changed. User Termination Timeout--whenever an MSAP time interval that controls keyboard lockout is changed. User Reauthentication Disable Timeout-- whenever an MSAP time interval that controls keyboard lockout is changed. Login Session Master Server--whenever an MSAP time interval that controls keyboard lockout is changed. Socks Security Service--whenever changes to MSAP security profiles and attributes occurs. IEMS Server IP address--whenever changes to MSAP security profiles and attributes occurs. Default PAM--whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs. Radius PAM--whenever changes to the MSAP security configuration (e.g., routing to a security server) occurs.	
STGW log	STGW700	An INFO log that may indicate any one of these issues or problems: FCR Change, Babbling node detected, Babbling node timeout, All babbling node IPs re-enabled due to initialization, or CPU occupancy critical alarm.

CS2000 Logs/Faults available

Log/Fault	Description	
STOR logs	STOR605	(Critical) Output when the Store Audit has detected a corruption in the Bstree structures containing the information about the data address space STOR is responsible for.
	STOR606	Indicates that the Store Audit has found a corruption in the allocation information for data store which is dumped (such as DSPROT) and it is very likely that a attempt to perform a dump while in this state would fail.
	STOR607	Generated when the Store Audit detects a mismatch between the Store Allocator's internal setting of an address' blocking attribute and the actual setting of the attribute in memory hardware.
Syslog alarm	Major alarm to indicate that the syslog system has failed to write logs, and a clear alarm to indicate that syslog has resumed writing logs. Both alarms are reported in log SPFS380.	
TLS alarms	TLS connection request comes in above the connection throttle limit (and above the threshold for the alarm - the defined thresholds are: 10 for minor, 50 for major, and 100 for critical).	
	TLS connection handshake failures (the thresholds are: 1 for minor, 2 for major, and 5 for critical).	
	TLS local certificate expiration (expiry in 31 days or less - minor, 15 days or less - major, and 5 days or less - critical).	
TMN logs	TMN301	Application error
	TMN302	System error
	TMN303	Communication error
	TMN309	Data Server error
	TMN311	Fatal error
	TMN600	Information only
	TMN601	File IO info
	TMN604	Application status
	TMN630	DataServer OK
TOPS logs	TOPS131	Generated when problems occur in the call flow for the activity TOPS Wireless Automated Directory Assistance Call (ADACC) with Release.
	TOPS615	An INFO log to indicate the opertor teams and the number of positions in each team with auto-compression turned on.
	AUD690	Generated when a TOPS calls ends unexpectedly with an IS41TOPS extension block attached.
TRK logs	TRK101	Percentage of busy trunks in a trunk group exceeded the threshold value for a minor alarm.
	TRK102	Major alarm threshold reached or exceeded.

CS2000 Logs/Faults available

Log/Fault	Description	
	TRK103	Number of trunks in a trunk group exceeded threshold value for a critical alarm.
	TRK104	Percentage of busy trunks dropped below a threshold value.
	TRK110	Trunk state change to SysB (system busy) LO (Lockout) from CPB (call processing busy).
	TRK112	Request to take trunk off the lockout (LO) list and RTS (return to service) initiated by a manual request from the LTP MAP display level or by a system request.
	TRK122	Both planes of the trunk equipment have lost accuracy detected by central control (CC).
	TRK123	Peripheral processor (PP) has sent a wrong message to central control.
	TRK138	Call routed for treatment after system was call processing busy (CPB).
	TRK151	Blue Box Fraud (BBF) detection activated.
	TRK152	Blue Box Fraud (BBF) detection deactivated.
	TRK153	Blue Box Fraud (BBF) call detected.
	TRK154	Blue Box Fraud (BBF) call disconnected to identify calling and called parties.
	TRK155	Emergency Service Bureau (ESB) originating the call is off-hook longer than the time designated in customer table TRKGRP.
	TRK164	External call routed through local office to a distant office that has requested calling line identification (CLI).
	TRK251	UCS: trouble with an invalid authcode.
	TRK255	UCS: trouble with database.
	TRK257	UCS: trouble translating a partition number to STS due to an invalid partition.
	TRK258	UCS: trouble translating STS to partition number, due to an invalid STS.
	TRK355	Trunk idle queue sanity trouble or rebuild.
	TRK420	UCS: invalid authcode.
	TRK424	First call processing threshold error; failed diagnostic test; and call processing error threshold appears again within 15 minutes of the diagnostic test.
TRKT logs	These logs are only generated if OFCVAR office parameter GENERATE_TRKT_LOGS is activated. Otherwise, TRK138 logs are generated with an appropriate treatment reason.	
	TRKT200	ANI Database Failure.
	TRKT201	ANI Account Status Not Allowed.
	TRKT202	ANI Acct Recently Disallowed.

CS2000 Logs/Faults available

Log/Fault	Description	
	TRKT203	Calling Card Invalid
	TRKT204	Calling Card Time-out
	TRKT205	General No Circuit
	TRKT206	Reorder
	TRKT207	Restricted Date Time
	TRKT208	Storage Overflow Reorder
	TRKT209	Start Signal Time-out
	TRKT210	Start Signal Time-out
	TRKT211	Vacant Code
	TRKT212	Vacant Country Code
	TRKT213	Trigger Block
UNEM and UMUX logs	UNEM or UMUX300	Generated for a minor, major, or critical communication alarm.
	UNEM or UMUX301	Generated for a minor, major, or critical equipment alarm.
	UNEM or UMUX302	Generated for a minor, major, or critical environmental alarm.
	UNEM or UMUX303	Generated for a minor, major, or critical processing error alarm.
	UNEM or UMUX304	Generated for a minor, major, or critical quality of service alarm.
	UNEM or UMUX500	Generated when a standing alarm condition has bee cleared.
	UNEM or UMUX600	INFO log generated when an alarm is acknowledged by the UNEM system.
	UMUX501	INFO is generated to indicate a change in the operational state of a UMUX NE.
	UMUX502	INFO is generated to indicate that the UNEM's polling status of the UMUX NE has been modified.
	UMUX601	INFO is generated when a UMUX NE has been added to the UNEM topology inventory.
	UMUX602	INFO is generated when a UMUX NE has been deleted from the UNEM topology inventory.
	UMUX603	INFO is generated when a UMUX NE name is changed in the UNEM.
	UMUX604	INFO is generated when a card has been added to a managed UMUX inventory.

CS2000 Logs/Faults available

Log/Fault	Description	
	UMUX605	INFO is generated when a card has been deleted from a managed UMUX inventory.
USNBD logs	UNB300	Reports problems with USNBD shared resources used by PCES.
	UNB302	Reports problems with USNBD processes used by PCES
	UNB304	Reports success and failure of surveillance activation and deactivation, and problems with surveillance activation.
	UNB305	Reports problems that affect PCES administration data and reports all user creations and deletions.
XAC logs	XAC300	Low Shared Memory (SM) condition. Accompanied by LowSM alarm.
	XAC302	Low Processor Element (PE) condition. Accompanied by LowPE alarm.
	XAC303	MScomm (Message Switch Communication) problem. Accompanied by MScomm alarm.
	XAC304	TOD (Time of Day clock) problem. Accompanied by TOD alarm.
	XAC305	RTIF (Reset Terminal Interface) problem. Accompanied by RTIF alarm.
	XAC306	Disk problem. Accompanied by DISK alarm.
	XAC307	Tape problem. Accompanied by TAPE alarm.
	XAC308	Image Test failure. Accompanied by Image alarm.
	XAC309	Loss of communication between the AMDI packlet and any MG4000.
	XAC310	Card manual busy.
	XAC312	IOP fault. Accompanied by IOPflt alarm. Modifed in SN08 to display the new CMIC and RTIF port device and CMIC and RTIF packlets and links.
	XAC312	IOP fault. Accompanied by IOPflt alarm.
	XAC320	Cardlist Report.
	XAC321	WgSlot (Shelf Audit Failure - Card Configuration). Accompanied by WgSlot alarm.
	XAC322	PETrbl. Accompanied by PETrbl alarm.
	XAC323	SMTrbl. Accompanied by SMTrbl alarm.
	XAC324	IOTrbl. Accompanied by IOTrbl alarm.
	XAC325	RIBKEY detected. Accompanied by RIBKey alarm.
	XAC326	MS Link configuration mismatch.
	XAC327	WgSlot (Card inserted into wrong slot). Accompanied by WgSlot alarm.
	XAC329	Loss of communication with XA-Core or loss of Ethernet link redundancy. Associated with the following OM groups: XETHRMJU, XETHRCRU, XETHR, XETHRPRT, and XETHRLNK.

CS2000 Logs/Faults available

Log/Fault	Description	
	XAC330	FW version mismatch. Accompanied by FWvers alarm.
	XAC333	FW loading failure.
	XAC335	Unknown CO-3 packlet fault. Accompanied by AMDI alarm.
	XAC337	Raised when the Baseln alarm is first raised, or the Baseln alarm is still raised and the non-baseline component list changes.
	XAC400	XA-Core summary report.
	XAC413	REx schedule failure. Accompanied by RExSch alarm.
	XAC415	Routine exercise report. SN08 added “not at baseline” as a reason for not running the SREx test.
	XAC600	LowSM condition cleared.
	XAC601	MemLim condition cleared.
	XAC602	LowPE condition cleared.
	XAC603	MScomm alarm cleared.
	XAC604	TOD alarm cleared.
	XAC605	RTIF alarm cleared.
	XAC606	DISK alarm cleared.
	XAC607	Tape alarm cleared.
	XAC608	Image alarm cleared.
	XAC609	AMDI link condition cleared.
	XAC610	Card returned to service. Modifed in SN08 to display the new CMIC and RTIF port device and CMIC and RTIF packlets and links.
	XAC612	IOP alarm cleared.
	XAC613	REx schedule report.
	XAC614	XATrap alarm cleared.
	XAC615	REx started.
	XAC618	Split (Split mode entered).
	XAC619	Split mode exited.
	XAC622	PETrbl alarm cleared.
	XAC623	SMTrbl alarm cleared.
	XAC624	IOTrbl alarm cleared.
	XAC625	RIBKEY removed.
	XAC626	MS Link configuration restored.
	XAC627	WgSlot cleared (card removed).

CS2000 Logs/Faults available

Log/Fault	Description	
	XAC628	Output when provisioning or deprovisioning.
	XAC629	Loss of communication restored.
	XAC630	FWvers cleared.
	XAC631	FW soaking started. Accompanied by FWsoak alarm.
	XAC632	FW soaking completed.
	XAC633	FW loading started.
	XAC634	FW loading completed.
	XAC635	FW soaking in progress.
	XAC637	Raised when the Baseln alarm is cleared, due to an empty list of non-baseline components.
	XAC640	Manual Test Report.
	XAC641	Alarm enable/disable notification.
	XAC801	MemLim (Memory Limit). Accompanied by MemLim alarm.
	XAC814	XATrap. Accompanied by XATrap alarm.
XACP logs	XACP300	Generated every minute that the EXT alarm HIGH_MEM_BLOCKING is active.
	XACP500	Generated once when the memory blocking level has returned to normal.
	XACP600	Summarizes the minute-by-minute memory blocking level; generated once every 15 minutes. If all 15 minutes had normal blocking levels, the log has only one line of output stating that all 15 minutes had normal blocking levels. If at least one minute out of 15 reported high blocking levels, the log output reports each minute separately.
XAUD logs	XAUD395, 397, 400, 401, 430, 432, 432, 434, 500, 501, 708, 709, 714, 715, 723, 724, 725, 979, 980, 981, 982, 977, 978	These call processing resource dump logs are generated whenever a call processing resource is recovered by the audit process running on the XA-Core. The only difference in the logs is the amount of data dumped. In SN08, the location and number of bits used to represent the extension block's format code in the header (within the hex dump of the log) has changed for all extension block logs. The only noticeable difference to the customer will be the number following the XAUD string in the log title. This change is also reflected in SN09.
XNET logs	XNET600	Connection between nodes has been replaced.
	XNET601	New connection between nodes failed.
	XNET602	Connection between nodes does not exist, and attempts to connect them failed.

CS2000 Logs/Faults available

Log/Fault	Description	
	XNET605	The bearer networks of the two parties in a connection attempt are not permitted to inter-connect, based on datafill in table NET2NET.
	XNET606	Indicates a software or provisioning problem in the switch, in that an appropriate bearer network could not be determined through provisioned data for a particular party in a connection attempt.
	XNET607	Indicates that an IW SPM interworking bridge was not available for the connection request, either because of a bridge exhaust condition, or a bridge is not available.
XPKT log	XPKT340	Reports a variety of Gateway, Gateway Controller, and DPTMA resource problems, including failed anchor attempts.

CS2000 Core Manager--available logs/faults

The following table lists the CS2000 Core Manager Logs/Faults available. The CS 2000 Core Manager supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer toAppendix G in this document titled “IEMS Functionality.” For details on the faults themselves, refer to the Fault Management section of CS 2000 FCAPS documentation, NN10082-911 and NN10275-909, *Fault Management Log Reference.*

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
Network Element: CS2000 Core Manager	For details on previously existing Logs/Faults, refer to NN10082-911.
CBM upgrade log	The CBM upgrade log is generated for any CBM upgrade failure.
SDM267	Indicates a change in the condition of a CBM link
SDM300	The connection from the CS2000 Core Manager to the CM or operating company LAN server(s) is down.
SDM301	The maintenance system detects the logical volume mirroring status.
SDM302	Use of a system resource exceeds the threshold. Associated with log SDM602.
SDM303	A process has failed more than 3 times in a day, or some other application fault has occurred. Reports an application alarm condition where action is required. Associated with log SDM603 which indicates a clearing of the alarm. CR Q00537118 and CR Q00600912 also impact this log for consistent formatting changes.
SDM304	Log Delivery application has failed to reconnect to a device.
SDM305	A problem exists with DTH commissioning. The log indicates which device and suggests a recommended action. Associated with a Minor alarm.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
SDM306	Table access software versions on the CM side and the SDM side are not compatible. Associated with a Minor alarm.
SDM307	Indicates trouble with the SDMCI. The connection to the CM was lost more than 3 times. Check the telnet port.
SDM308	An I-tape or S-tape backup has failed. More generally, indictes that a backup requirement is present/not fulfilled or not yet fulfilled.
SDM309	Fault detected on HW device or user took HW device OOS.
SDM310	System found a pending transaction at startup time. Check the audit log to find out which command was involved. Rollback of the transaction was successful. Use the SDMdbAdmin tool to sync CM and SDM again. Associated with a Minor alarm.
SDM311	System found a pending transaction at startup time. Check the audit log to find out which command was involved. Rollback of the transaction was NOT successful. Use the SDMdbAdmin tool to sync CM and SDM again. Associated with a Major alarm.
SDM312	Postprocessing of a command failed. The transaction was rolled back. Use the SDMdbAdmin tool to sync CM and SDM again. Associated with a Minor alarm.
SDM313	Postprocessing of a command failed. The transaction was rolled back. Use the SDMdbAdmin tool to sync CM and SDM again. Associated with a Major alarm.
SDM314	Iindicates two SDM link connections are physically crossed. Associated with Major alarm “Crossed Link.”
SDM315	Corruption of file detected during data dictionary download.
SDM317	DCE subsystem has detected a problem.
SDM318	OM report failed to complete within one report interval. Associated with a Major alarm.
SDM321	Reports that a split-system upgrade is in progress. Associated with a Minor alarm.
SDM325	The connection to a network management component in a given domain has been lost. Log reports may be lost as a result.
SDM328	Indicates that the signal on receive/ transmit fibre to OC3 card is faulty or not present. Associated with Major alarm OC3 Card Fault.
SDM329	Indicates a probable link equipment malfunction. Associated with Minor alarm Minor Link Fault.
SDM332	Indicates the status of an unsuccessful SDM system audit. An INFO log.
SDM336	Indicates that a response to CBM 800 heartbeat is not received from the core. Associated with major alarm Core Heartbeat
SDM337	Indicates that the patch failed signature checking.
SDM338	Indicates that the OMDD audit finds omdata file system usage exceeds 60% (Minor) or 80% (Major.
SDM500	The SDM node control process has restarted.
SDM501	The node control process updated SDM run state to INSV.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
SDM502	The node control process updated SDM run state to MANB. Logs SDM502-505 are included in the CS2000 Core Manager Log Delivery stream, but do not appear on the RMI.
SDM503	The node control process updated SDM run state to SYSB.
SDM504	The node control process updated SDM run state to ISTB.
SDM505	The node control process updated SDM run state to OFFL from MANB.
SDM550	An SDM Node Status Change has occurred. Modified in SN06 so that the log occurs in only one type of format and it no longer reports application state change events of OffL, ManB, and process starts.
SDM600	An SDM maintenance connection has been re-established.
SDM601	Logical volume mirroring is re-established.
SDM602	A system resource is below the threshold.
SDM603	The SDM303 alarm has been cleared. Or a state change has occurred that does not require manual intervention to clear. With SN06, this log now reports application state change events of OffL, ManB, and process starts. CR Q00600912 also impacts this log for consistent formatting changes.
SDM604	CM had too little time to format log(s) and log(s) is/are lost.
SDM607	Internal CS 2000 Core Manager log; indicates when a process controller starts or restarts a process. The system does not send SDM607 to the OSS. You can see the SDM607 report from the remote maintenance interface (RMI), when logged onto the CS 2000 Core Manager.
SDM608	I-tape or S-tape process has completed. More generally, indictes that the backup requirement has been fulfilled or is no longer present.
SDM609	A hardware device has returned to the INSV state.
SDM614	Reports that the crossed link alarm associated with SDM314 is cleared.
SDM615	Log Thresholding is in effect for logs managed by exception application. Exception reports may be inaccurate
SDM616	An unauthorized connection attempt is detected by the Log Delivery application. The connection is refused.
SDM617	A DCE problem has been cleared.
SDM618	Logical volume /var is 98 percent full. Log files in /var/adm have been deleted.
SDM619	OM Access Service detected a corrupt OM group during an OM schema download.
SDM620	Reports current system performance data at set times.
SDM621	The split-system upgrade is finished.
SDM622	Max file size reached for a file device handled by GDD.
SDM625	The connection to a Network Management component in a given domain has been re-established.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
SDM626	An info log generated whenever the OMDD application starts and it detects that the tuple number option has been changed since the last time the application was launched. The log is used to inform the OSS of the state change, which inherently signifies a change in the OMDD CSV files. The log will indicate the new (current) state as being either ACTIVATED or DISABLED.
SDM630	Indicates the SDM REX Test start and complete time. An INFO log.
SDM631	An info log generated when a file in *closedNotSent* directory is deleted by audit to make morethan 80% available space in the omdata file system.
SDM632	Indicates the status of a successful SDM system audit. An INFO log.
SDM633	A CBM info log that indicates a change in the condition of a CBM link.
SDM634	Indicates that the OC3 Card Fault alarm raised with SDM328 has been cleared.
SDM635	Indicates that the Minor Link Fault alarm raised with SDM329 has been cleared.
SDM636	Indicates that the heartbeat alarm raised with SDM336 has been cleared.
SDM637	Indicates that that patch check status is cleared by the user.
SDM638	A clear log generated when the OMDD audit finds omdata file system usage goes below 80% or below 60%.
SDM639	Critical--indicates that the OMDD audit finds omdata file system usage exceeds 90%. All the OM files from the closedSent directory will be deleted.
SDM650	Link maintenance requests a report on a failed link maintenance action.
SDM700	Reports a Warm, Cold, or Reload restart or a norestartswact on the core.
SDM739	Indicates file transfers between the FTP Client and the CORE and to show user log-ons to the CORE..
SDMB logs	**(SDM billing)**
SDMB300	Memory allocation failed for SDM billing system.
SDMB310	Indicates a communication problem with the SDM Billing System.
SDMB315	A software-related problem has occurred.
SDMB316	A billing-related process has been manually killed.
SDMB320	A billing-backup problem affecting more than one file.
SDMB321	A billing-backup problem affecting one file.
SDMB350	The billing application has reached a death threshold (a process has died > 3 times < 1 minute apart) and there is a request to restart.
SDMB355	A disk-related problem has occurred, such as problems writing to disk (related to alarm DSKWR) or with disk utilization (related to alarm LODSK).
SDMB365	A new version of the billing application does not support a stream format on an active stream present in previous load.
SDMB367	Value has been set on a trappable MIB object.

CS2000 Core Manager Logs/Faults available

Log/Fault	Description
SDMB370	CDR-to-BAF conversion encountered a problem that prevented it from converting CDR to BAF; BAF record lost.
SDMB375	Generated when a problem occurs during the transfer of a file to the data processing management system (DPMS). It may be problems and alarms related to FTP, RTB (real-time billing), AFT (automatic file transfer), or Secure File Transfer Protocol.
SDMB380	The file transfer mode for the stream indicated has an invalid value.
SDMB390	A schedule-related problem has occurred.
SDMB400	Generated every hour for every active stream to list all current active alarms.
SDMB530	The configuration or status of a stream has changed.
SDMB531	Configuration for backup volumes was changed correctly.
SDMB550	The billing application has shut down.
SDMB600	Generic information for the overall SDM Billing System.
SDMB610	A communications-related problem has been resolved.
SDMB620	A backup-related problem has been resolved.
SDMB621	A new backup file is being started.
SDMB625	Recovery has started on a backup file.
SDMB650	The billing application is restarting one or more processes.
SDMB655	Indicates file state changes and disk utilization, OR disk utilization has dropped below a threshold, OR the billing application cannot move a file to the closeSentProcessed directory.
SDMB665	A software problem on the CM prevents the downloading (synch) of FLEXCDR data at the SDM.
SDMB675	An information log that identifies a event related to the transfer of billing files. An event may be a normal operation, a problem, or the resolution of a problem related to SDMB375.
SDMB680	Information not related to the file system or creating links needs to be communicated to the customer.
SDMB690	Indicates that an SBAIF alarm and the fault that caused it have cleared.
SDMB691	Generates when a problem occurs with the scheduled transfer of billing files and when that fault clears. It also generates when a file transfer schedule is manually deactivated or deleted.
SDMB820	A backup has hit a threshold.
SDM security log	An Authentication and Authorization Security Syslog, generated when a security event occurs on a SDM.
SDM patch check alarm	This minor alarm is generated under the “sdmmtc sys” level, raised upon a patch signature check failure.

CS2K Management Tools (CMT)--available logs/faults

The following table lists the CS2000 Management Tools logs available. CS2K supports supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled “IEMS Functionality.” For details on these logs, refer to the Fault Management section of CS2K Management Tools, NN10325-900 and to NN10275-909, *Fault Management Log Reference.*

CS2K Management Tools Logs/Faults available

Log/Fault	Description
CMT300	Critical. Data is mismatched between the SESM server and the Core. The SESM audit, CS2K Data Integrity Audit, has 10 unresolved problems. To view and correct the problems, open the audit problem report from the Audit System found under the SESM Maintenance menu item.
CMT301	Critical. The GWC element manager cannot download data to GWC on recovery so the process has terminated early, and the GWC remains out of service. To clear, determine and remedy the cause of the data download failure.
CMT302	SNMP Timeout. Critical. SNMP poller cannot communicate to the network device due to an SNMP timeout.
CMT303	A Critical automatically generated log upon the raising/clearing of a CMT alarm.
CMT399	Indicates a cleared alarm in the CMT device
CMT500	Generated by the SESM alarm system to indicate the system is initializing.
CMT501	Generated by the SESM alarm system upon shutdown.
CMT502	Generated by the SESM alarm system to inform northbound alarm clients that alarm notifications cannot be generated. This log will be sent via the SSPFS syslog feed to the customer log.
CMT600	Generated when an RMGC overflow condition is detected. This log is propagated to the IEMS under the “other” category.
Alarm log for Corrupt Certificate	The log lists additional detail for the Corrupt Certificate alarm.
Alarm log for Changed Certificate	The log lists additional detail for the Changed Certificate alarm.
Corrupt Certificate	Minor alarm, raised when a syntax error is recognized in a Certificate or a disallowed combination of fields is present.
Duplicate Certificate	Minor alarm, raised when more than one Certificate with the same name is detected in the Nortel or Third Party certificate directories.
Delete Certificate	Minor alarm, raised if a Certificate file is removed that has GWs associated with it.

CS2K Management Tools Logs/Faults available

Log/Fault	Description
Certificate Changed	Minor alarm, raised when an existing profile is changed and one or more of the fields that are changed are not allowed.
Missing Certificate	Minor alarm, raised when a Nortel Certificate has been removed from the Nortel directory or changed to a different name.
No Available Call Server IP	A Critical alarm, raised if the SESM cannot get any available C-Side IP address from the Core.

GWC--available logs/faults

The following table lists the GWC Logs/Faults available.
GWC supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled "IEMS Functionality." For details on the logs/faults themselves, refer to the Fault Management section of GWC FCAPS documentation, NN10090-911 and NN10275-909, *Fault Management Log Reference*.

GWC Logs/Faults available

Log/Fault	Description
Network Element: GWC (PGC load)	
The PM180, 181, 185, and 177 faults are first sent to the core and are then sent northbound from the CS2000 Core Manager in SCC2 format. The remaining faults are sent from the GWC to the GWC EM and are then sent northbound via CORBA.	
PM180	Indicates a software error (SWERR) has occurred.
PM181	Generates for a variety of GWC-to-core-related communications issues. Modified in SN08 to indicate that the ABI of an ABI-hosted XPM is attempting to or successfully exit(s) ESA.
PM185	Indicates that the GWC has trapped.
PM777	Indicates a hardware fault. Reason text identifies the suspected hardware.
The remaining faults are sent from the GWC to the GWC EM and are then sent northbound via CORBA. The following alarms are generated by the GWC, except for the first one generated by the alarm browser.	
SNMP Timeout	Critical; indicates a communications sub0system failure.
Test	Minor; a test alarm generated from the pmdebug interface.
Active unit disabled	Critical; indicates a unit is out of service and not available.
Standby unit disabled	Critical; indicates a unit is out of service and not available.

GWC Logs/Faults available

Log/Fault	Description
Core communication lost	Major if active unit; Minor if inactive unit. No response received to Core heartbeat.
Mate unit communication lost	Minor; no response received to mate heartbeat.
Gateway communication lost	A gateway has stopped responding to heartbeat.
EM communication lost	Major. No response received for Persistent Data Verification SNMP Trap; EM not responding. Problem may be “EM not present, provisioned data loaded from local flash,” OR “EM audit indicates provisioned inservice data is old, need manual intervention to recover.” Cleared with a busy RTS.
FLASH error	Minor. Error in writing Flash; erase of Flash sector failed. Cleared with hardware replacement.
FLASH life span exceeded	Minor. The number of writes to FLASH has exceeded the recommended/intended limit.
Security_SA_ capacity	Minor or Major. Security Association alarms are nearing capacity. Cleared by the security alarms application which monitors the resource level and cleared the alarm when the alarm condition as been cleared on the GWC. Currently alarms are only managed on the active GWC unit (i.e., data is not mirrored to the inactive unit), and for this reason during a SWACT alarms are automatically cleared on the unit dropping activity.
Security_SA_ fail	Major. The number of Security Association alarms has exceeded the threshold. Cleared by the security alarms application which monitors the resource level and cleared the alarm when the alarm condition as been cleared on the GWC. Currently alarms are only managed on the active GWC unit (i.e., data is not mirrored to the inactive unit), and for this reason during a SWACT alarms are automatically cleared on the unit dropping activity.
Recovery alarm	A GWC recovery process has terminated early, and the GWC remains out of service.
DQOSMTC_ DQoSLinkLoss	A DQoS/COPS connection failure has occurred. Cleared by DCCNXMGR (via DCALARM) when the connection is reestablished or the connection is deleted via provisioning.
Datasync alarm	The GWC does not contain the latest provisioned data. This alarm may be raised by the GWC EM noting the problem and sending a message to the GWC to raise the alarm.
Unit Out of Service	Critical if active unit; minor if inactive unit. The GWC Profile failed to validate, probably because no profile is available to activate. Cleared with a GWC reload.
QOS error log	If the QCA detects an event or an error, a syslog message is generated and a non-QoS record is written to the output stream (file).
QOS connection alarm	An alarm is generated whenever a message cannot be sent to the server. The alarm is cleared as soon as the QoS report application is able to send QoS reports to the server.

GWC Logs/Faults available

Log/Fault	Description
GWC Alarm Logs	
GWC300	Active unit disabled. Critical; indicates a unit is out of service and not available.
GWC301	Standby unit disabled. Indicates a unit is out of service and not available. Minor if the unit is ManB, but Major if the unit is SysB.
GWC302	Core communication lost. Major if active unit; Minor if inactive unit. No response received to Core heartbeat.
GWC303	Mate unit communication lost. Minor; no response received to mate heartbeat.
GWC304	Gateway communication lost. A gateway has stopped responding to heartbeat. This log is triggered only for gateways that have 64 or more endpoints.
GWC305	This is a test alarm generated from pmdebug interface. Severity level changed in SN06; can have a severity level of critical, major, minor or warning.
GWC306	DQOSMTC_DQoSLinkLoss. A DQoS/COPS connection failure has occurred. Cleared by DCCNXMGR (via DCALARM) when the connection is reestablished or the connection is deleted via provisioning
GWC307	EM communication lost. Major. No response received for Persistent Data Verification SNMP Trap; EM not responding. Problem may be “EM not present, provisioned data loaded from local flash,” OR “EM audit indicates provisioned inservice data is old, need manual intervention to recover.” Cleared with a busy RTS. Datasync alarm The GWC does not contain the latest provisioned data. This alarm may be raised by the GWC EM noting the problem and sending a message to the GWC to raise the alarm.
GWC308	FLASH error Minor. Error in writing Flash; erase of Flash sector failed. Cleared with hardware replacement.
GWC309	Security_SA_capacity. Minor or Major. Security .Association alarms are nearing capacity. Cleared by the security alarms application which monitors the resource level and clears the alarm when the alarm condition has been cleared on the GWC. Currently alarms are only managed on the active GWC unit (i.e., data is not mirrored to the inactive unit), and for this reason during a SWACT alarms are automatically cleared on the unit dropping activity.
GWC310	Security_SA_ fail. Major. The number of Security Association alarms has exceeded the threshold. Cleared by the security alarms application which monitors the resource level and cleared the alarm when the alarm condition as been cleared on the GWC. Currently alarms are only managed on the active GWC unit (i.e., data is not mirrored to the inactive unit), and for this reason during a SWACT alarms are automatically cleared on the unit dropping activity.
GWC311	Provisioned GWC Profile not yet activated.
GWC312	QOS connection alarm. An alarm is generated whenever a message cannot be sent to the server. The alarm is cleared as soon as the QoS report application is able to send QoS reports to the server.

GWC Logs/Faults available

Log/Fault	Description
GWC313	Major. RMGC can't process all coming requests. RMGC can't process all coming requests. It is in the processing error category. The probable cause is the resource at or nearing capacity.
GWC314	Raised in connection with a Location Id Reporting connection failure alarm.
GWC317	An alarm log raised whenever PreSwact audit fails. An alarm will be raised with proper text which explains which component has led Preswact audit to fail. The specific problem displayed at the GWC level for the alarm raised will match with the swact failure reason at the SESM GUI.
GWC398	SNMP Timeout Critical; indicates a communications sub0system failure.
GWC399	Is the clear log for all GWC alarms and for CMT alarms. This log is triggered only for gateways that have 64 or more endpoints.
GWC501	Unable to maintain connection to remote gateway of 64 or fewer endpoints.
GWC502	Connection to remote gateway restored.
GWC503	Connection drop initiated by remote gateway.
GWC506	Generated for any of 3 events: Time to Live Expired, Gateway Unregistration by CS2K Successful, or Gateway Initiated Unregistration Successful.
GWC507	Generated to indicate Gateway Registration Successful.
GWC603	Indicates that a netfail event occurred from the GW and was reported to the connection broker. The log shows on which GWC the problem occurred, the Gateway name, IP address of the GW, the Endpoint name, the terminal ID, and the reason for the netfail event.
GWC604	Indicates that a connection broker exception occurred from the GW and was reported. The log shows on which GWC the problem occurred, the Gateway name, IP address of the GW, the Endpoint name, the terminal ID, and the reason for the exception.
GWC alarms	External Host Interface Signal Loss, based on the number of gateways that are out of service as compared to the number of gateways provisioned checked on a 5 minute polling period.
	External Host Interface Configuration Error, based on a 5 minute polling period.
	External Host Interface Protocol Error, based on the number of USP connections that are not active but do have heartbeat messages checked on a 5 minute polling period.
GWC security logs	telnet connection from remote host
	serial connection
	login attempted
	login result
	authentication server unreachable
	logout (by request, force out, or idle timeout)
	local account login

GWC Logs/Faults available

Log/Fault	Description
	local password change/reset
	GWC restart
	GWC reload

MG4000-available logs/faults

The following table lists the MG4000logs available. MG 4000 supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled "IEMS Functionality." For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference.*

MG4000 logs available

MG4I 300	Media Integrity Failure
MG4I 301	GigE Audit Failure
MG4I 320	Counter overflow in the Operational Measurement pegs
MG4I 501	SCTP Core Connection State Change
MG4I 502	SCTP Peer Connection State Change

MG9000--available logs/faults

The following table lists the MG 9000 Faults available.
MG 9000 supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled "IEMS Functionality." For details on the logs/faults themselves, refer to the Fault Management section of MG 9000 FCAPS documentation, NN10074-911 and NN10275-909, *Fault Management Log Reference.*

MG 9000 Faults available

Network Element: MG 9000	
Fault	**Description**
ATM50 alarm	Raised if the SSI (Signal State Interrupt) count gets too high.
BW300	Reserved bandwidth used on the indicated shelf has exceeded the Bandwidth Congestion Threshold. Correlates with Warning alarm bwResBandwShelfFault.
BW301	Reserved bandwidth use on the network interface has exceeded the Bandwidth Congestion Threshold. The alarm is cleared when reserved bandwidth on the network interface is 10% less than the threshold. Correlates with Warning alarm bwResBandwTotalFault.

MG 9000 Faults available

BW302	Reserved bandwidth dedicated to switched lines connections on the network interface has ex- ceeded the Bandwidth Congestion Threshold with respect to the amount of bandwidth configured the network interface for switched lines.. Correlates with Warning alarm bwResBandwSloaFault.
BW304	An overall cell queue congestion alarm has occurred when overall atm cell queue is at least 90% full, or the alarm has been cleared. Correlates with Warning alarm bwSwitchFabricTotalFault.
BW305	A CBR cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricCbrFault.
BW306	An RT-VBR cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricRtVbrFault.
BW307	An NRT-VBR cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricNrtVbrFault.
BW308	A UBR cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricUbrFault.
BW309	A UBR-plus cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricUbrPlusFault.
BW310	A control channel cell queue congestion alarm has occurred or been cleared. To occur, atm cell queue for this service type is at least 90% full. Correlates with Warning alarm bwSwitchFabricControlFault.
BW311	Reserved bandwidth dedicated to ABI lines connections on the network interface has exceeded the Bandwidth Congestion Threshold with respect to the amount of bandwidth configured the network interface for switched lines. Correlates with Warning alarm bwResBandwAbiFault.
CES305	No cells are being received from the ATM network. Correlates with Major alarm cesLossOfCell.
ESA300	Communication between GWC and GW is lost. Entered ESA mode. Correlates with Critical alarm Entered ESA.
ESA302	This log corresponds to the nnESADownloadFault.
ESA304	Generated by the EM in response to a Major alarm from the MG9000 (nnEsaCoIFault) trap. The MG9000 sends this trap when it detects communication problems to other nodes in the same community of interest.
ESA312	Generated by the EM when a failure occurs while trying to provision internodal community of interest data for a given NE (Major alarm).
ESA601	ESA601 is generated from alarm nnESAFault. This alarm was added in Gateway to notify the data inconsistency when MG 9000 finds intenral ESA data mapping inconsistency after the ESA data dowloading is completed.

MG 9000 Faults available

ESA602	ESA602 is generated from alarm nnESARetrieveFault, an alarm generated by the EM for ESA Data Retrieval failutre.	
ESA fault nnESADownloadFault	Indicates a failure to download ESA data to a given VMG. This alarm will only be generated for autonomous download attempts. This was indicated by a log in releases previous to SN08.	
GIGE alarms	301 LOS	Loss of Signal, Critical
	302 RFI	Remote Failure Indication, Critical
	304 TEM	Temperature Threshold Exceeded, Critical
	305 POW	Low power indicated, Critical
	306 RxSD	Receive Signal Degraded, Critical
	307 RxEED	Receive Excessive Error Ratio, Critical
	308 TBC	Transmit Bias Current, Critical
	309 LINT	Link Initialization, Critical
	310 OPT	Transmit Optical Power, Critical
	311 OPR	Receive Optical Power, Critical
	312 GARP	GARP Failure, Critical
	313 LKINT	Link Integrity Failure, Critical
	314 AUTONEG	Auto Negotiation Failure, Critical
	315 NON PREFLINK	Non-preferred Link is active, Critical
GIGE logs	GIGE301	Indicates a Communications Subsystem Failure, loss of signal.
	GIGE302	Indicates a Communications Subsystem Failure,r emote failure.
	GIGE303	Indicates a Communications Subsystem Failure, transmit failure.
	GIGE304	Indicates a Communications Subsystem Failure, temperature threshold exceeded.
	GIGE306	Indicates a Communications Subsystem Failure, low power indicated.
	GIGE307	Indicates a Communications Subsystem Failure, transmit excessive error ratio.
	GIGE308	Indicates a Communications Subsystem Failure, transmit bias current.
	GIGE309	Indicates a Communications Subsystem Failure, link initialization.

MG 9000 Faults available

	GIGE310 Indicates a Communications Subsystem Failure, transmit optical power.
	GIGE311 Indicates a Communications Subsystem Failure, receive optical power.
	GIGE312 Indicates a Communications Subsystem Failure, GARP failure.
	GIGE313 Indicates a Communications Subsystem Failure, link integrity failure.
	GIGE314 Indicates a Communications Subsystem Failure, autonegotiation failure.
	GIGE315 Indicates a Communications Subsystem Failure, non-preferred link is active.
HW Mismatch alarm	The Hardware Mismatch alarm indicates an incorrect replacement card has been installed.
QoS alarms	New QoS alarms are generated when any of four configured threshold parameters are exceeded. The alarm browser (at the VMG level) is extended to view these alarms.
Provisioning failure logs	If an operation fails when provisioning Tone, Class, or Physical Ringing data, a customer log is generated.
“Authorization Failed” Security Log	Generated when a user attempts to perform an unauthorized action.
MG9K Server Log	A warning log generated when the MG9K server is either starting up or shutting down.
MGAUxxx	Generated when audit task starts.
MGAUxxx	Generated when audit task is paused.
MGAUxxx	Generated when audit task is resumed.
MGAUxxx	Generated when audit task is completed with a summary of corrections.
MGAUxxx	Generated when audit schedule is deleted.
MGAUxxx	Generated when audit could not correct a mismatch.
MGCA301	Loss of signal fault has occurred or been cleared. Correlates with Critical alarm LOS (on OC3) or Minor alarm los (on DS1).
MGCA302	Alarm indication signal fault has occurred or been cleared. Correlates with Critical alarm AIS (on OC3) or Minor alarm ais (on DS1).
MGCA303	Loss of frame fault has occurred or been cleared. Correlates with Critical alarm LOF (on OC3) or Minor alarm lof (on DS1).
MGCA304	Remote alarm indication. Correlates with Minor alarm RAI (on DS1).
MGCA305	Bit error rate signal fault has occurred or been cleared. Correlates with Critical alarm bit error ratio signal default (BERSF) (on OC3).
MGCA306	Bit error rate signal degraded fault has occurred or been cleared. Correlates with Major alarm bit error ratio signal default (BERSD) (on OC3).
MGCA307	Remote defect indication fault has occurred or been cleared. Correlates with Minor alarm remote defect indication (RDI) (on OC3).

MG 9000 Faults available

MGCA308	Path label mismatch fault has occurred or been cleared. Correlates with Minor alarm alarm path label mismatch (PLM) (on OC3).
MGCA309	Loss of pointer fault has occurred or been cleared. Correlates with Minor alarm loss of pointer (LOP) (on OC3).
MGCA310	An unequipped fault has occurred or been cleared. Correlates with Minor alarm UNEQ (on OC3).
MGCA311	Loss of cell delineation fault has occurred or been cleared(supported in EM only). Correlates with alarm LOD.
MGCA312	IMA link- Loss of IMA Frame. Correlates with Minor alarm imaLinkLif.
MGCA313	IMA link- Loss of delayed synchronization. Correlates with Minor alarm imaLinkLods.
MGCA314	IMA link- Remote failure indication. Correlates with Minor alarm imaLinkRfi.
MGCA315	IMA link- Transmit misconnect. Correlates with Minor alarm imaLinkTxMisConnect.
MGCA316	IMA link- receive misconnect. Correlates with Minor alarm imaLinkRxMisConnect.
MGCA317	IMA link- transmit fault. Correlates with Minor alarm imaLinkTxFault.
MGCA318	IMA link- receive fault. Correlates with Minor alarm imaLinkRxFault.
MGCA319	IMA link- transmit unusable far end. Correlates with Minor alarm imaLinkTxUnusableFe.
MGCA320	IMA link- receive unusable far end. Correlates with Minor alarm imaLinkRxUnusableFe.
MGCA321	IMA group startup far end. Correlates with Major alarm imaGroupStartupFe.
MGCA322	IMA group configuration abort. Correlates with Critical alarm imaGroupCfgAbort.
MGCA323	IMA group configuration abort far end. Correlates with Major alarm imaGroupCfgAbortFe.
MGCA324	IMA group insufficient links. Correlates with Critical alarm imaGroupInsuffLinks.
MGCA325	IMA group insufficient links far end. Correlates with Major alarm imaGroupInsuffLinksFe.
MGCA326	IMA group blocked far end. Correlates with Minor alarm imaGroupBlockedFe.
MGCA327	IMA group timing synchronization. Correlates with Major alarm imaGroupTimingSynch.
MGCA328	ABI Loss of Clock on DS512 optical link. Correlates with Critical alarm abiLossOfClock.
MGCA329	ABI Loss of Frame on DS512 optical link. Correlates with Critical alarm abiLossOfFrame.
MGCA330	ABI Loss of Signal (low light level) on DS512 optical link. Correlates with Critical alarm abiLowLightLevel.
MGCA331	ABI Channel parity error on DS512 optical link. Correlates with Minor alarm abiChannelParityError.
MGCA332	SDH Path Trace Identifier Mismatch Alarm (only applies to SDH and not SONET). The Path Trace Identifier being seen by the OC3 card at the carrier Path level does not match what has been provisioned for that carrier. Correlates with Minor alarm tim.
MGCA333	AlarmIndicationSignal (ds3ais) generates log MGCA333 when an AlarmIndicationSignal fault is received from the Gateway.

MG 9000 Faults available

MGCA334	LossofFrame (ds3lof) generates log MGCA334 when a LossOfFrame fault is received from the Gateway.
MGCA335	RemoteAlarmIndication (ds3rai) generates log MGCA335 when a RemoteAlarmIndication fault is received from the Gateway.
MGEM300	Generated when MG9000 EM is not able to make connection to the Element Manager Database. Correlates with Major alarm EmDbUnavailable.
MGEM301	In SN06, the NE301 log name changed toMGEM301. Generated when the MG 9000 Manager loses SNMP communication with the MG 9000. Correlates with Critical alarm CommsLostToNE.
MGEM302	In SN06, NE302 log name changed to MGEM302. The MG9000 Manager has added an ne MG9000 and tries to discover the NE. It will check the MG9000 EM IP address provisioned at the MG9000 and if it is incorrect will raise this alarm. Correlates with Major alarm invalidEMIPAddress.
MGEM303	In SN06, the NE303 log name changed to MGEM303. The description of t his log is restored faults: “Faults seen while active.” Diagnostics will not clear restored faults. The card with the restored faults may not be in the same state it was in before the restart that caused the faults to be restored. The MG9000 sends too many alarms within a 5 second window. When this happens the MG9000 Manager will request this particular MG9000 stop sending Alarms and display thia particular alarm. This condition will clear when the number of alarm within 5 sec falls below a set number. Correlates with Critical alarm AlarmsBeingThrottled.
MGEM704	Indicates that an attempt to correct the database has failed
MGEM705	Indicates that the Database is unavailable and correction failed.
MGEM714	Raised each time the MG9K Upgrade Tool is executed.
NE300	In SN06, the NE300 log (corresponding to all NorNode Faults) split into several logs (grouped according to the clearning procedures). Log NE300 should only be generated if the GW is running on pre-SN06 loads and the MGEM is running on SN06+ loads. It is purely for backward compatibility.
NE301	The NE301 log (Critical) is generated when an incorrect replacement card has been installed.
NE302	The NE302 log indicates software faults of any severity.
NE303	The NE303 log indicates restored faults: “Faults seen while active.” Diagnostics will not clear restored faults. The card with the restored faults may not be in the same state it was in before the restart that caused the faults to be restored.
NE304	The NE304 log indicates faults that are ambiguous with regard to the card that is causing the fault. Usually, the alarm on card A indicates that there is a problem on card A, card B, or the link in between card A and B.
NE305	The NE305 log indicates serial device faults of any severity.
NE306	The NE306 log indicates GLAN-related faults of any severity. The GLAN hub is located on the active ITP in the shelf where the fault appears.
NE307	The NE307 log indicates ABI faults of any severity.

MG 9000 Faults available

NE308	The NE308 log indicates inband messaging faults of any severity.
NE309	The NE309 log indicates clock sync faults of any severity.
NE310	The NE310 log indicates unused hardware faults of any severity.
NE311	The NE311 log indicates time of day faults of any severity - attempts to access the provisioned time server have failed.
NE312	The NE312 log indicates cable faults of any severity -- one of the cables to the ITPs has been connected in an unsupported way.
NE313	The NE313 log indicates an activity cable fault of any severity; the activity control cable is a small cable on the front of the ABI cards that is used for activity determination.
NE314	The NE314 log indicates backplane faults of any severity; the carriers between the two DCC cards cannot communicate.
NE315	The NE315 log indicates bandwidth fault of any severity; some of the carriers are not providing bandwidth.
NE316	The NE316 log indicates line alarms of any severity.
NE317	The NE317 log indicates shelf faults of any severity.
NE318	The NE318 log indicates proxy alarms of any severity; the card referred to in the alarm text (description) is not communicating.
NE319	The NE319 log indicates MTA alarms of any severity.
NE320	The NE320 log indicates data audit faults of any severity; data audit required.
NE609	A software image log generated whenever a user executes an image request.
OMC300	Indicates that the OM Collector failed to collect OM files from the MG9K during a particular collection interval. Also indicates that the OM Collector is able to restart collecting OM files from the MG9K.
OVLD808	(Critical) Indicates that an external messaging link has closed and cannot send/receive message.
OVLD809	(Major) Indicates that the message loss is high enough such that the message link is in a degraded service state.
OVLD810	(Minor) Indicates message retransmissions are high enough that system is starting to see performance degradation.
SHLF301	SIC talk battery A alarm occurs. Correlates with Critical alarm shelfTalkBatteryA.
SHLF302	SIC talk battery B alarm occurs. Correlates with Critical alarm shelfTalkBatteryB.
SHLF303	SIC signal battery A alarm occurs. Correlates with Major alarm shelfSignalBatteryA.
SHLF304	SIC signal battery B alarm occurs. Correlates with Major alarm shelfSignalBatteryB.
SHLF305	SIC signal battery A fuse alarm occurs. Correlates with Major alarm shelfSignalBatteryAfuse.
SHLF306	SIC signal battery B fuse alarm occurs. Correlates with Major alarm shelfSignalBatteryBfuse.

MG 9000 Faults available

SHLF307	SIC shelf fail LED alarm occurs. Correlates with alarm shelfFailLED.
SHLF308	BIP signal battery A1 alarm occurs. Correlates with Major alarm bipSignalBatteryA1.
SHLF309	BIP signal battery A2alarm occurs. Correlates with Major alarm bipSignalBatteryA2.
SHLF310	SIC talk battery B1 alarm occurs. Correlates with Major alarm bipSignalBatteryB1.
SHLF311	BIP signal battery B2 alarm occurs. Correlates with Major alarm bipSignalBatteryB2.
SHLF312	BIP talk battery A alarm occurs. Correlates with Minor alarm bipTalkBatteryA.
SHLF313	BIP talk battery B alarm occurs. Correlates with Minor alarm bipTalkBatteryB.
SHLF314	BIP filter A fail alarm occurs. Correlates with Minor alarm bipFilterA.
SHLF315	BIP filter B fail alarm occurs. Correlates with Minor alarm bipFilterB.
SHLF316	BIP scan point 1 is activated. Correlates with alarm bipScanPoint1.
SHLF317	BIP scan point 2 is activated. Correlates with alarm bipScanPoint2.
SHLF318	BIP scan point 3 is activated. Correlates with alarm bipScanPoint3.
SHLF319	BIP scan point 4 is activated. Correlates with alarm bipScanPoint4.
SHLF320	BIP scan point 5 is activated. Correlates with alarm bipScanPoint5.
SHLF321	BIP scan point 6is activated. Correlates with alarm bipScanPoint6.
SHLF322	BIP scan point 7is activated. Correlates with alarm bipScanPoint7.
SHLF323	BIP scan point 8is activated. Correlates with alarm bipScanPoint8.
SHLF324	BIP scan point 9is activated. Correlates with alarm bipScanPoint9.
SHLF325	BIP scan point 10is activated. Correlates with alarm bipScanPoint10.
SHLF326	BIP scan point 11 is activated. Correlates with alarm bipScanPoint11.
SHLF327	Talk Battery A1 Power Feed. Correlates with Major alarm bipTalkBatteryA1.
SHLF328	Talk Battery A Power Feed. Correlates with Major alarm bipTalkBatteryA2.
SHLF329	Talk Battery B1 Power Feed. Correlates with Major alarm bipTalkBatteryB1.
SHLF330	Talk Battery B2 Power Feed. Correlates with Major alarm bipTalkBatteryB2.
SHLF331	BIP circuit breaker fan alarm occurs (EM only). Correlates with Minor alarm bipFanBreaker.
SHLF332	BIP environmental control unit 0 temperature alarm occurs. Correlates with Minor alarm bipEcuTemp0.
SHLF333	BIP environmental control unit 1 temperature alarm occurs. Correlates with Minor alarm bipEcuTemp1.
SHLF334	BIP environmental control unit 0 fan alarm occurs. Correlates with Minor alarm bipEcuFan0.
SHLF335	BIP environmental control unit 1 fan alarm occurs. Correlates with Minor alarm bipEcuFan1.

MG 9000 Faults available

SHLF336	BIP remote alarm cut off alarm occurs. Correlates with alarm bipRemoteAlarmcutoff.
SHLF337	BIP local alarm cut off alarm occurs. Correlates with alarm bipLocalAlarmcutoff.
SHLF338	BIP ABS fuse fail alarm occurs. Correlates with Major alarm bipAbsFusefail.
SHLF339	BIP ABS battery power supply alarm occurs. Correlates with Critical alarm bipAbsPowerSupply.
SHLF340	BIP shelf circuit breaker trip alarm occurs. Correlates with Major alarm bipShfBreakerTrip.
SHLF341	Presence of BIP's Current-Sense Card A. Correlates with Major alarm bipCsApresence.
SHLF342	Presence of BIP's Current-Sense Card B. Correlates with Major alarm bipCsBpresence.
SHLF343	Presence of BIP's Alarm Relay Card. Correlates with Major alarm bipAlmRelayPresence.
SHLF344	Current-Sense Card A Shelf 0 High Threshold exceeded. Correlates with Minor bipCSAshf0HighThres alarm.
SHLF345	Current-Sense Card A Shelf 1 High Threshold exceeded. Correlates with Minor bipCSAshf1HighThres alarm.
SHLF346	Current-Sense Card A Shelf 2High Threshold exceeded. Correlates with Minor bipCSAshf2HighThres alarm.
SHLF347	Current-Sense Card A Shelf 3High Threshold exceeded. Correlates with Minor bipCSAshf3HighThres alarm.
SHLF348	Current-Sense Card BShelf 0 High Threshold exceeded Correlates with Minor bipCSBshf0HighThres alarm.
SHLF349	Current-Sense Card B Shelf 1 High Threshold exceeded. Correlates with Minor bipCSBshf1HighThres alarm.
SHLF350	Current-Sense Card B Shelf 2 High Threshold exceeded. Correlates with Minor bipCSBshf2HighThres alarm.
SHLF351	Current-Sense Card B Shelf 3 High Threshold exceeded. Correlates with Minor bipCSBshf3HighThres alarm.
SHLF352	Current High Temperature Threshold exceeded. Correlates with Minor bipTempHighThres alarm.
SHLF353	Current-Sense Card A Shelf 0 Low Threshold exceeded. Correlates with Minor bipCSAshf0LowThres alarm.
SHLF354	Current-Sense Card A Shelf 1 Low Threshold exceeded. Correlates with Minor bipCSAshf1LowThres alarm.
SHLF355	Current-Sense Card A Shelf 2 Low Threshold exceeded. Correlates with Minor bipCSAshf2LowThres alarm.
SHLF356	Current-Sense Card A Shelf 3 Low Threshold exceeded. Correlates with Minor bipCSAshf3LowThres alarm.
SHLF357	Current-Sense Card B Shelf 0 Low Threshold exceeded. Correlates with Minor bipCSBshf0LowThres alarm. Correlates with Minor bipCSBshf1LowThres alarm.

MG 9000 Faults available

SHLF358	Current-Sense Card B Shelf 1 Low Threshold exceeded. Correlates with Minor bipCSBshf1LowThres alarm.
SHLF359	Current-Sense Card B Shelf 2 Low Threshold exceeded. Correlates with Minor bipCSBshf2LowThres alarm.
SHLF360	Current-Sense Card B Shelf 3 Low Threshold exceeded. Correlates with Minor bipCSBshf3LowThres alarm.
SHLF361	Current Low Temperature Threshold exceeded. Correlates with Minor bipTempLowThres alarm.
SHLF362	Status of the Signal Battery Fuse. Correlates with Major bipSignalBatteryFuse alarm.
SHLF363	Status of Talk Battery A Fuse. Correlates with Major bipTalkBatteryAFuse alarm.
SHLF364	Status of Talk Battery B Fuse. Correlates with Major bipTalkBatteryBFuse alarm.
SHLF365	Status of Cooling Unit 0 Fuse. Correlates with Minor bipEcuFuse0 alarm.
SHLF366	Status of Cooling Unit 1 Fuse. Correlates with Minor bipEcuFuse1 alarm.
SHLF367	Status of the End-Aisle Fuse. Correlates with Minor bipEndAisleFuse alarm.
SHLF368	BIP Signal Distribution Point 1. Correlates with bipSignalDistribution1 alarm.
SHLF369	BIP Signal Distribution Point 2. Correlates with bipSignalDistribution2 alarm.
SHLF370	BIP Signal Distribution Point 3. Correlates with bipSignalDistribution3 alarm.
SHLF371	BIP Signal Distribution Point 4. Correlates with bipSignalDistribution4 alarm.
SHLF372	BIP Visual Critical. Correlates with bipVisualCritical alarm.
SHLF373	BIP Visual Major. Correlates with bipVisual Major alarm.
SHLF374	BIP Visual Minor. Correlates with bipVisualMinor alarm.
SHLF375	BIP Audible Critical. Correlates with bipAudibleCritical alarm.
SHLF376	BIP Audible Major. Correlates with bipAudibleMajor alarm.
SHLF377	BIP Audible Minor. Correlates with bipAudibleMinor alarm.
SHLF378	BIP Alarm CutOff LED. Correlates with bipAlarmCutOffLED alarm.
SHLF379	BIP Talk Battery A Fail LED. Correlates with bipTalkBatteryFailALED alarm.
SHLF380	BIP Talk Battery B Fail LED. Correlates with bipTalkBatteryFailBLED alarm.
SHLF381	BIP Critical LED Bank. Correlates with bipCriticalLEDbank alarm.
SHLF382	BIP Major LED Bank. Correlates with bipMajorLEDbank alarm.
SHLF383	BIP Minor LED Bank. Correlates with bipMinorLEDbank alarm.
SHLF384	BIP Environmental Control Unit 0 LED. Correlates with bipEcu1LED alarm.
SHLF385	BIP Environmental Control Unit 1 LED. Correlates with bipEcu2LED alarm.
SHLF386	BIP Alarm Processor Card Fail LED. Correlates with bipAlarmFailLED alarm.
SHLF387	BIP Aisle Alarm. Correlates with bipAisleAlarm alarm.

MG 9000 Faults available

SHLF388	BIP Frame Alarm. Correlates with bipFrameFail alarm.
SHLF389	Presence of BIP's Alarm Relay Card LED. Correlates with bipAlmRelayLed alarm.
SHLF390	Status of Current-Sense Card A LED. Correlates with bipCsAled alarm.
SHLF391	Status of Current-Sense Card B LED. Correlates with bipCsBled alarm.
SHLF392	Generated when a shelfCompatibility fault is received from the MG9kEM server.
SHLF393	Generated when a cardDiscovery fault is received from the MG9kEM server.
SHLF501	A catch-all INFO log for all shelf events. Changed in SN06 to show a Severity of Indeterminate, which means no priority has been assigned to the related BIP event. If a severity had been datafilled, then SHLF383 would generate instead of SHLF 501.
SWLN301	Line in Fault occurred or is cleared. Correlates with Minor lineFault alarm.
SWLN302	Hazardous Voltage line fultat occurred or is cleared. Correlates with Minor alarm lineProtectionFault.
SWLN303	Line in Babbling state linie fault occurred or is cleared. Correlates with Minor alarm lineBabbleState.
VC301	Minor: atmVcl Alarm indication signal. Correlates with Minor alarm vclTpAis.
VC302	Minor: atmVcl Remote Detection Indicator. Correlates with Minor alarm vclTpRdi.
VC303	Minor: loss of continuity, vcl. Correlates with Minor alarm vclLoc.
VC304	Minor: atmVcc Alarm indication signal. Correlates with Minor alarm vccTpAis.
VC305	Minor: atmVcc Remote Detection Indicator. Correlates with Minor alarmvccTpRdi.
VC306	Minor: loss of continuity, vcc. Correlates with Minor alarm vccLoc.
VC307	Minor: loss of cell delineation on If (only on the EM). Correlates with alarm atmLcd.
VMG300	Generated when Root Termination goes out of service (Communication between Gateway and GWC is lost and ESA is not enabled). Correlates with Critical alarm VMG OOS.
VMG301	QoS Alarm that is generated when the number of bad call reaches a certain threshold.
VMG302	QoS Alarm that is generated when the number of Packet Loss reaches a certain threshold.
VMG303	QoS Alarm that is generated when IP message Jitter reaches a certain threshold.
VMG304	QoS Alarm that is generated when IP message Latency reaches a certain threshold.
VMG322	Generated when a vMGAdminStatusOutOfService fault is received from the MG9kEM server (Warning).
VMG323	Generated when a cardLocked fault is received from the MG9kEM server (Warning).
VMG324	Generated when a cardDisabled fault is received from the MG9kEM server (Warning).
VMG325	Generated when a cardInitializing fault is received from the MG9kEM server (Warning).
VMG328	Generated when a lineMtceNotReady fault is received from the MG9kEM server (Critical).

MG 9000 Faults available

VMG329	Generated when a MegacoMtceNotReady fault is received from the MG9kEM server (Critical).
VMG373	Generated when a GWCUnreachable fault is received from the MG9kEM server (Critical).
VMG374	Generated when a noReplyFromGWC fault is received from the MG9kEM server.
VMG376	Generated when an aal1BearerSubsystem OnPairNotReady fault is received from the MG9kEM server.
VMG377	Generated when an ipBearerSubsystem OnPairNotReady fault is received from the MG9kEM server.
VMG600	Indicates that termination data was successfully provisioned in all appropriate areas except for the database.
VMG601	Indicates that an attempt to correct termination data in the database has passed.
VMG Admin State is OOS	Generated when a vMGAdminStatusOutOfService fault is received from the MG9kEM server (Warning). Relates to log VMG322.
VMG Initializing	Generated when a cardInitializing fault is received from the MG9kEM server (Warning). Relates to log VMG325.
VMG OOS-card locked	Generated when a cardLocked fault is received from the MG9kEM server (Warning). Relates to log VMG323.
VMG OOS-card disabled	Generated when a cardDisabled fault is received from the MG9kEM server (Warning). Relates to log VMG324.
VMG OOS- Line Maintenance is not Ready	Generated when a lineMtceNotReady fault is received from the MG9kEM server (Critical). Relates to log VMG328.
VMG OOS- Megaco Maintenance is not Ready	Generated when a MegacoMtceNotReady fault is received from the MG9kEM server (Critical). Relates to log VMG329.
VMG OOS- GWC is not reachable	Generated when a GWCUnreachable fault is received from the MG9kEM server (Critical). Relates to log VMG373.
VMG OOS- no reply from GWC	Generated when a noReplyFromGWC fault is received from the MG9kEM server. Relates to log VMG374.
VMG OOS- AAL1 bearer subsystem not ready	Generated when an aal1BearerSubsystem OnPairNotReady fault is received from the MG9kEM server. Relates to log VMG376.
VMG OOS- IP bearer subsystem not ready	Generated when an ipBearerSubsystem OnPairNotReady fault is received from the MG9kEM server. Relates to log VMG377.
XDSL301	Generated when a loss of signal - local modem fault occurs. Correlates with Minor alarm losATUC.
XDSL302	Generated when a loss of frame - local modem fault occurs. Correlates with Minor alarm lofATUC.
XDSL303	Generated when a loss of power - local modem fault occurs. Correlates with Critical alarm lprATUC.

MG 9000 Faults available

XDSL304	Generated when a loss of link - local modem fault occurs. Correlates with Minor alarm lolATUC.
XDSL305	Generated when a loss of signal - remote modem fault occurs. Correlates with Minor alarm losATUR.
XDSL306	Generated when a loss of frame - remote modem fault occurs. Correlates with Minor alarm lofATUR.
XDSL307	Generated when a loss of power - remote modem fault occurs. Correlates with Minor alarm lprATUR.
XDSL308	Generated when a loss of link - remote modem fault occurs. Correlates with Minor alarm lolATUR.
XDSL309	Generated when a no modem present fault occurs. Correlates with Minor alarm aturNotPresent.
XDSL310	Generated when a local modem clock failure occurs. Correlates with Critical alarm noClock.
XDSL311	Generated when a protocol error occurs. Correlates with Critical alarm handshakeFail.
XDSL312	Generated when a configuration error occurs. Correlates with Critical alarm linkMismatch.
XDSL313	Generated when an ATM traffic dropped at WAC upstream fault occurs. Correlates with Critical alarm vpiNonzero.
XDSL314	Generated when a loss of sync of ATM cells - upstream fault occurs. Correlates with Critical alarm lcdIATUC.
XDSL315	Generated when a loss of sync of ATM cells - downstream fault occurs. Correlates with Critical alarm lcdIATUR.
XDSL316	Generated when a local modem Critical failure - not responding, in Kernel mode, download failure, or message corrupted fault occurs. Correlates with Critical alarm failATUC.
XDSL317	Generated when a general hardware fault indication - circuit fault occurs. Correlates with Critical alarm circuitHardwareFault.
xDSL600	ATUCs transmit rate has changed (RADSL mode only).
xDSL601	ATUC initialization failed.
xDSL602	ATURs transmit rate has changed (RADSL mode only).
xDSL800	Loss of Framing 15-minute interval threshold reached.
xDSL801	Loss of Signal 15-minute interval threshold reached.
xDSL802	Loss of Power 15-minute interval threshold reached.
xDSL803	Errored Second 15-minute interval threshold reached.
xDSL805	Loss of Framing 15-minute interval threshold reached.
xDSL806	Loss of Signal 15-minute interval threshold reached.
xDSL807	Loss of Power 15-minute interval threshold reached.

MG 9000 Faults available

xDSL808	Errored Second 15-minute interval threshold reached.
xDSL809	A DSL Interface exceeds the specified threshold on a given performance measurement.
The following items describe the MG9K Clock Sync alarms.	
Loss of Phase Lock	Minor: Phase PLD [altera 7064b] detected a minimum phase difference greater than eight nano seconds.
Loss of Frame Pulse Lock	Minor: Frame pulse alignment did not get established with the active card -- it should occur in the inactive card only
Loss of My Clock	Minor: The high and low levels of the SYNC PLL clock are not toggling.
Loss of Mate Clock	Minor: The high and Low levels of the mate clock are not toggling.
Loss of Clock Output	Major: Phase PLD reference clock oscillator not toggling.
Single Reference Failure	Minor: Single monitored reference source has been lost.
All Reference Failure	Major: Absolute and Delta reference source signals have been lost.
Single Sync Unit Failure	Major: Stratum 3 unit on ITP failed.
Clock Stability	Clock mode can be Acquiring, Acquired, Hold Over, or Free Run.
DACV alarms	DACV at Rail is a Major alarm to indicate the ITP clock circuitry has attempted to acquire sync and has traversed the frequency range to the extreme end of its capture range..
	DACV Out of Range is a Major alarm to indicate that the ITP 's DACV clock circuitry is in an invalid condition and the values are out of range.
Signal LOS	Minor: Single/All source reference occurred due to loss of signal.
Signal LOF	Minor: Single/All source(s) reference occurred due to out of frame.
No Signal	Minor: Sync source reference selected does not provide a signal.
MG9K alarms	Unable to communicate with RADIUS Server.
	Secure link Down with GWC.
	Packet Discard (depends on the threshold set).
	Overload Controls--these alarms will now also apply to the ABI & ITP Card as well as the DCC Card.
MG9K Threshold logs	SAD: Discard Policy, or Looup failed.
	IKE: Main mode failed, or Mismatched PSK, or Quick mode failed, or Proposal mismatch, or NULL ESP & authentication = null, or en/decryption failures, or Packet discarded, or decryption errors, or Auth errors.

MG 9000 Faults available

	IPSec Security: Decryption error or Authentication error.
MG9K security alarms	Non-responsive RADIUS Server
	Expired Links to Security Peers
	Replayed Packet threshold
	Packet Discard threshold
MG9K security events logs	IKE negotiation errors
	IP packet authentication failures
	Packet discard
	Replayed packets
IPSec Syslog messages	There is a wide variety of IKE failure messages generated to syslog. Refer to feature A00005561 in this document for the complete list.

ERS8600 (previouslly Passport 8600)--available traps/faults

ERS8600 (formerly Passport 8600) suppports SCC2 format through the IEMS interface. For details on the IEMS interface, refer to the chapter in this document titled “IEMS Functionality.” The following table lists the Passport 8600 traps available.

ERS8600 (previously Passport 8600) Traps available

Trap Name	Description
Network Element: ERS8600 (formerly Passport 8600) Faults from the ERS8600 (formerly Passport 8600) are provided via an SNMP Northbound interface that is provided on the ERS8600 (formerly Passport 8600) itself.	
risingAlarm	Minor, correlates with PP310.
fallingAlarm	Cleared, correlates with PP311.
Default Trap	Indeterminate, correlates with PP312.
coldStart	Cleared, correlates with PP313.
warmStart	Cleared, correlates with PP315.
linkDown	Major, correlates with PP317.
linkUp	Cleared, correlates with PP318.
authenticationFailure	Warning, correlates with PP319.
rcnChasPowerSupplyDown	Critical, correlates with PP322.
rcnChasPowerSupplyUp	Cleared, correlates with PP323.
rcnChasFanDown	Critical, correlates with PP324.
rcnChasFanUp	Cleared, correlates with PP325.
rcn2kCardDown	Major, correlates with PP326.
rcn2kCardUp	Cleared, correlates with PP327.

ERS8600 (previously Passport 8600) Traps available

Trap Name	Description
rcn2kTemperature	Critical, correlates with PP328.
rcnErrorNotification	Warning, Major, Critical, correlates with PP329.
rcnLinkOscillation	Major, correlates with PP330.
rcnMacViolation	Warning, correlates with PP331.
rcnSonetTrap	Warning, correlates with PP332.
rcnStpNewRoot	Warning, correlates with PP333.
rcnStpTopologyChange	Warning, correlates with PP334.
rcnStpTCN	Warning, correlates with PP335.
rcn2kAtmPvcLinkStateChange	Indeterminate, Minor, Major, correlates with PP336.
rcnSmltIstLinkUp	Cleared correlates with PP337.
rcnSmltIstLinkDown	Major, correlates with PP338.
rcnSmltLinkUp	Cleared, correlates with PP339.
rcnSmltLinkDown	Major, correlates with PP340.
rcnPasswordChange	Warning, correlates with PP341.
rcnPcmciaCardRemoved	Warning, correlates with PP342.
rcnSmartCpldTimerFired	Major, correlates with PP343.
rcnCardCpldNotUpDate	Warning, correlates with PP344.
rcnIgapLogFileFull	Major, correlates with PP345.
rcnCpLimitShutDown	Major, correlates with PP346.
rcnSshServerEnabled	Cleared, correlates with PP347.
rcnSshServerDisabled	Major, correlates with PP348.
rcnSshSessionLogin	Cleared, correlates with PP349.
rcnSshSessionLogout	Major, correlates with PP350.
rcnSshUnauthorizedAccess	Major, correlates with PP351.
rcnHaCpuState	Warning, correlates with PP352.
rcnInsufficientMemory	Warning, correlates with PP353.
rcnSaveConfigAction	Minor, correlates with PP354.
rcnLoopDetectOnPort	Warning correlates with PP355.
vrrpTrapStateTransition	Warning, correlates with PP356.
rcnEmError	Warning, correlates with PP357.
ospfVirtIfStateChange	Warning, Cleared, correlates with PP358.
ospfNbrStateChange	Warning, Cleared, correlates with PP359.
ospfVirtNbrStateChange	Minor, Cleared, correlates with PP360.
ospfIfConfigError	Major, correlates with PP361.
ospfVirtIfConfigError	Major, correlates with PP362.

ERS8600 (previously Passport 8600) Traps available

Trap Name	Description
ospfIfAuthFailure	Major, correlates with PP363.
ospfVirtIfAuthFailure	Major, correlates with PP364.
ospfIfStateChange	Warning, Cleared, correlates with PP365.
rcnCardDown	Major, correlates with PP366.
rcnCardUp	Cleared, correlates with PP367.
rcnbgpEstablished	Cleared, correlates with PP368.
rcnbgpBackwardTransition	Cleared, correlates with PP369.
rcnAggLinkUp	Cleared, correlates with PP370.
rcnAggLinkDown	Cleared, correlates with PP371.
rcnIgmpNewGroupMember	Cleared, correlates with PP372.
rcnIgmpLossGroupMember	Cleared, correlates with PP373.
rcnIgmpNewQuerier	Cleared, correlates with PP374.
rcnIgmpQuerierChange	Cleared, correlates with PP375.
rcnDvmrpIfStateChange	Cleared, correlates with PP376
rcnDvmrpNewNbrChange	Cleared, correlates with PP377.
rcnDvmrpNbrLossChange	Cleared, correlates with PP378.
rcnFdbProtectViolation	Cleared, correlates with PP379.
rcnLogMsgControl	Cleared, correlates with PP380.
rcnSaveConfigFile	Cleared, correlates with PP381.
rcnDNSRequestResponse	Cleared, correlates with PP382.
pingProbeFailed	Cleared, correlates with PP383.
pingTestFailed	Cleared, correlates with PP384.
pingTestCompleted	Cleared, correlates with PP385.
traceRoutePathChange	Cleared, correlates with PP386.
traceRouteTestFailed	Cleared, correlates with PP387.
traceRouteTestComplete	Cleared, correlates with PP388.
UDPEapSessionEndTrap	Cleared, correlates with PP389.
UDPEapSessionStartTrap	Cleared, correlates with PP390.
Trap raised by idi_PP8600.pol to indicate Device-Rediscovery	This trap indicates that a device re-discovery has been initiated.
OSPF v2 trap	This trap indicates a variable ospfAddressLessIf (var(2)) takes the value 0 on interfaces with IP addresses and the corresponding value of ifIndex for interfaces having no IP address.

See the design description of feature A00002920, which supports and generates ERS8600 (formerly Passport 8600) logs that are received by the PLS

application. The design description of this feature is in the Feature Deltas section of the SN06.2 OSS Guide.

MG15000 (previously PVG) Logs/Faults

For Logs/Faults available for MG15000 (previously PVG), refer to NTP NN10600-500, *Nortel Multiservice Switch 6400/7400/15000/20000 Alarms Reference*.

Multiservice Data Manager logs/faults

For logs and faults information for the Multiservice Data Manager (MDM), refer to the following documents: 241-6001-500, *MDM Alarms Reference,* and 241-6001-011, *MDM Fault Management Tools*.

NPM--available logs/faults

The following table lists the Network Patch Manager (NPM) Logs/Faults available.
NPM supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled “IEMS Functionality.” For details on the logs, refer to the Fault section of the FCAPS documentation on CS 2000 Management Tools, NN10325-900 and NN10275-909, *Fault Management Log Reference.*

NPM Logs/Faults available

Log/Fault	Description
Network Element: Network Patch Manager	
NPM360	Reports that an alarm has been raised.
NPM370	Reports when an alarm has been cleared.
NPM400	Reports the results of attempted apply, remove, and audit commands.
NPM600	Reports when the NPM server has been started, either by reboot or manually.
NPM601	File failure; reports general problems that could be service affecting. The log contains lines of trouble information text.
NPM603	There are problems between the database and the device during a device audit.
NPM605	General trouble log; reports general problems that could be service affecting. The log contains lines of trouble information text.
NPM610	Provides information related to the execution of a task.
NPM660	Reports problems when a plan fails to execute.

NPM Logs/Faults available

Log/Fault	Description
NPM680	Reports problems when a plan is automatically executed.
NPM System Alarms	
Alarm name	Description
ACT_NOT_APP	Activated patch not applied to all applicable devices.
ACT_NOT_ACT	Active patch applied to all applicable devices but not activated in all devices.
DEBUG_APP	Debug patches applied. Minor.
DISABLED_APPLIED	Applied patches that can be enabled, but are disabled. Major.
DNR_NOT_APP	Do Not Remove (DNR) patches not applied. Critical.
EMG_NOT_APP	Emergency patches not applied. Critical.
ENABLED_REMOVED	Patches which can be enabled but are not enabled. Major.
GEN_NOT_APP	General patches not applied. (No severity)
LTD_NOT_APP	Limited patches not applied. (No severity)
OBS_NOT_REMOVED	Obsolete patches not removed. Major.
OBE_NOT_REMOVED	Obsolete emergency patches not removed. Critical.
REMOVED_PATCHES	Removed patches when are not category OBS, OBE, or DBG. (No severity)
PATCH_ONHOLD	Patches on hold. Minor.
DEVICE_ONHOLD	Devices on hold. Minor.
REL_GEN_NOT_APP	A Major alarm raised when a released patch has not been applied. Relates to log NPM360.
PFRSGETPATCH	A Major alarm raised when the PFRS GENREPORT task has failed. Relates to log NPM360.
PFRSGENREPORT	A Major alarm raised when the PFRS GETPATCH task has failed. Relates to log NPM360.

QCA Logs/Faults

The following table lists the QCA Faults/Alarms available. QCA supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled “ IEMS Functionality.” For details on the logs,

refer to the Fault section of the FCAPS documentation on CS 2000, NN10083-911 and NN10275-909, *Fault Management Log Reference*.

QCA Logs/Faults

Log/Fault	Description
QCA201	Warning. Qca.properties not available at QCA start-up, or other problems related to properties/qca.properties.
QCA202	No priority. Old file retention directory (today-x) is being removed, OR file found in active directory when QCA started..
QCA203	QCA cannot be stopped for one of several possible reasons. Examples: the qca.properties file may be missing, the system cannot determine the QCA port number, QCA not running on specified port, an out-of-range port number is specified, or similar issues.
QCA300	No priority. File handler or server socket could not be started.
QCA301	Minor or Major. Minor: QoS Record received with Unsupported Length or Unsupported Version. Major: 10 sequential QoS Records received with Unsupported Length or Version.
QCA302	No priority. Out of sequence QoS record received, OR problem processing binary QoS record.
QCA305	No priority. Connection to client is closed. OR, The binary QoS Record header could not be processed.
QCA310	Minor, Major, or Critical. Minor: disk space is below the minimum threshold. Major: Disk space is below 500Mb. Critical: disk space is below 100 Mb.
QCA315	No priority, or Warning. Generated for one of many possible file writing or file access problems. For the Warning level, it means that a request to get a new file name has failed, or the QCA has failed to write the footer information to the active file while attempting to close. Ohter reasons, for example, mighjt be: could not get new file to write records; file <fileName> is corrupted or removed; could not write to the activefile; active file exists but cannot write records to it. In some cases, QCA will shut down.
QCA322	No priority. New GWC connection received.
QCA399	No pirority. Clear log for QCA301 or QCA310.

SAM21--available logs/faults

The following table lists the SAM21 Logs/Faults available. The Shelf Controller Unit (SCU) raises alarms on behalf of itself or on behalf of the cards in the I/O slots, power sleds, fan sleds and power supply. Therefore, the alarm IDs for some of the alarms will have the same label, but the slot location that is included in the body of the alarm will indicate the actual card that is having problem. Alarms with the label IPOA are the alarms raised by the SCU with the PMC ATM card.

SAM21 supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled “IEMS Functionality.” For details on the logs/faults themselves, refer to the Fault Management

section of SAM21 FCAPS documentation NN10089-911 and NN10275-909, *Fault Management Log Reference.*

SAM21 Logs/Faults available

Log/Fault	Description
Network Element: SAM21 Platform	
SCU310	Shelf controller unit. CPU load is high Major. The One minute load average is greater than 20. Critical. The five minute load average is above 15, or the fifteen minute load average is above 7.
SCU332	Shelf controller unit. Memory usage is high Major. Total free memory has fallen below 15%. Critical. Total free memory has fallen below 10%.
SCU349	Shelf controller unit Disk usage is high. Major. Total free space on the root file system has fallen below 10%. Critical. Total free space on the root file system has fallen below 5%.
SCU346	Shelf controller unit. Large number of processes abnormally terminated Major. More than 4 zombie processes in system. Critical. More than 15 zombie processes in system.
SCU329	Shelf controller unit. Loss of communications either to its mate or to the SDM. Minor. The upper or lower serial cable connection is down. Major. This shelf controller cannot ping its mate through the ethernet interface Major. This shelf controller cannot ping the SDM, but can ping its mate Major. Both the lower (upper) serial cable and the mate's Ethernet are not connected. Major. This shelf controller cannot ping the SDM, but can ping its mate. The upper (lower) serial cable connection is down. Major. Both serial cable connections are down. Critical. Shelf cannot ping its mate or the SDM through the Ethernet interface. Critical. Shelf cannot ping its mate or the SDM through the Ethernet interface. The upper (lower) serial cable connection is down. Critical. This shelf controller cannot ping its mate through the Ethernet interface. Both serial cable connections are down. No synching of state changes are occurring. Critical. The shelf cannot see out at all.
SCU335	Major: Power Supply in Sled 1/2/3 has been removed. Most likely the whole sled has been removed. Critical. Power Supply in Sled 1/2/3 is down. The power supply in that sled has failed.
SCU315	Major. Fan in Sled 1/2/3 has been removed. Fan has been removed from the sled, or the entire sled has been removed.

SAM21 Logs/Faults available

Log/Fault	Description
	Critical. Fan in Sled 1/2/3 is down Fan has failed.
SCU335	Critical. Power feed 1/2 is down. Either the feed has failed, or the cable has been removed.
SCU356	Critical. Mate Shelf Controller Down. Operating in Simplex Mode. The inactive SC has been detached, or Mama on the active SC has not received a ping from the inactive SC in 20 seconds.
SCU315	Major. Temperature in Sled 1/2/3 is High. Temperature in the sled has reached about 40 degrees.
	Critical. Temperature in Sled 1/2/3 is High. Temperature in sled has reached about 50 degrees.
SCU301	Critical. Extension Bridge in Slot 15/16 is Down/Up. Depending on the actual text, one or both of the Extension Bridges has been detached and/or removed.
SCU315	Major. Diagnostic Failed during testing in a non-system card at the specified I/O Slot A diagnostic test was run, and the board failed at least one of the tests.
	Major. Diagnostic Failed due to SWACT in a non-system card at the specified I/O Slot. A diagnostic test was interrupted by a SWACT.
	Major. Diagnostic Failed n a non-system card at the specified I/O Slot for a specified reason. The diagnostic failed due to the reason stated. (There are 11 possible statements.)
SCU346	Critical. Firmware Flashing could not connect to the non-system card at the specified I/O Slot. Either there is another process currently attached to the board, or the bus is too busy to allow the request. Auto Flash is now turned off on the SC for this slot.
	Critical. Firmware Flashing failed at downloading firmware to the non-system card at the specified I/O Slot. The firmware file does not exist on the SDM or has incorrect parameters.
	Critical. Firmware Flashing failed at validating firmware to the non-system card at the specified I/O Slot.The firmware file is corrupt on the SDM, or there was an error in the transfer.
	Critical. Firmware Flashing failed at backing up the firmware to the non-system card at the specified I/O Slot. The copy operation from one bank to the other failed. Possible bad memory.
	Critical. Firmware Flashing failed flash to the non-system card at the specified I/O Slot. Could not connect to the board after the flash.
	Critical.Provision of a non-system card at the specified I/O Slot. Provisioning of the board failed due to some system problem. System may have been abnormally busy.
SCU500	Reports a change in state of a card. The new state can be Unlocked, Enabled, or None.

SAM21 Logs/Faults available

Log/Fault	Description
SCU501	Reports an equipment insertion, specifying the shelf, card, and slot.
SCU502	Reports an equipment removal, specifying the shelf, card, and slot.
IPOA301	A system log in response to a loss of cell delineation (LCD) alarm from SC-IPoA card.
IPOA302	A system log in response to a SONET carrier fault of type AIS from the SC-IPoA card
IPOA303	A system log in response to an ATM connection fault from the SC-IPoA card
IPOA304	A system log in response to an ATM connection set fault detected by the SAM21 Element Manager.
IPOA801	A system log in response to an ATM CRC32 threshold fault.
SM21300	A system log in response to an alarm that there has been a loss of communication, and the remote network is down.
LOS/LOF AIS-L/RDI-L AIS-P/RDI-P	These section, line and path faults indicate that SONET connectivity between the SC and the far end node is unavailable on one fiber.
LOP	
ATM Overrun Count	Indicates the number of times cells were dropped due to a shortage of buffer space.
BootServerUnavailable	Indicates that the boot server cannot be reached. Severity may vary.
ATM Overrun Date	Indicates the date of the last overrun.
CPU load high	Major. The One minute load average is greater than 20. Critical. The five minute load average is above 15, or the fifteen minute load average is above 7.
Disk usage high	Major. Total free space on the root file system has fallen below 10%. Critical. Total free space on the root file system has fallen below 5%.
Large number of processes abnormally terminated	Major. More than 4 zombie processes in system. Critical. More than 15 zombie processes in system.
Loss of Communications: Serial Connection 1 (2) is down	Minor. The upper (lower) serial cable connection is down.
Loss of Communications: Mate Ethernet is down	Major. This shelf controller cannot ping its mate through the ethernet interface.

SAM21 Logs/Faults available

Log/Fault	Description
Loss of Communications: Remote network is down.	Major. This shelf controller cannot ping the SDM, but can ping its mate.
Loss of Communications: Mate Ethernet, Serial Connection 1 (2) is down.	Major. Both the lower (upper) serial cable and the mate's Ethernet are not connected.
Loss of Communications: Remote network, Serial connection 1 (2) is down.	Major. This shelf controller cannot ping the SDM, but can ping its mate. The upper (lower) serial cable connection is down.
Loss of Communications: Serial Connection 1, Serial Connection 2 is down.	Major. Both serial cable connections are down.
Loss of Communications: Local Ethernet interface is down.	Critical. Shelf cannot ping its mate or the SDM through the Ethernet interface.
Loss of Communications: Local Ethernet interface, Serial Connection 1 (2) is down	Critical. Shelf cannot ping its mate or the SDM through the Ethernet interface. The upper (lower) serial cable connection is down.
Loss of Communications: Mate Ethernet, Serial Connection 1, Serial Connection 2 is down	Critical. This shelf controller cannot ping its mate through the Ethernet interface. Both serial cable connections are down. No synching of state changes are occurring.
Loss of Communications: All Communications Paths Down	Critical. The shelf cannot see out at all.
Memory usage high	Major. Total free memory has fallen below 15%. Critical. Total free memory has fallen below 10%.
NFSMountsDown	Raised for any mounts that remian down after the check and attempt to re-mount.

SAM21 Logs/Faults available

Log/Fault	Description
Power supply in Sled 1/2/3 has been removed.	Major. Most likely the whole sled has been removed.
Power supply in Sled 1/2/3 is down.	Critical. The power supply in that sled has failed.
Fan in Sled 1/2/3 has been removed	Major. Fan has been removed from the sled, or the entire sled has been removed.
Fan in Sled 1/2/3 is down	Critical. Fan has failed.
Power Feed 1/2 is down.	Critical. Either the feed has failed, or the cable has been removed.
Mate Shelf Controller Down. Operating in Simplex Mode.	The inactive SC has been delatched, or Mama on the active SC has not received a ping from the inactive SC in 20 seconds.
Temperature in Sled 1/2/3 is High	Major. Temperature in the sled has reached about 40 degrees.
Temperature in Sled 1/2/3 is High.	Critical. Temperature in sled has reached about 50 degrees.
Extension Bridge in Slot 15/16 is Down/Up.	Critical. Depending on the actual text, one or both of the Extension Bridges has been detached and/or removed.
Diagnostic Failed at test case.	Major. A diagnostic test was run, and the board failed at least one of the tests.
Diagnostic Failed due to SWACT	Major. A diagnostic test was interrupted by a SWACT.
Diagnostic Failed, xxxxxx	Major. The diagnostic failed due to the reason stated. (There are 11 possible statements.)
Firmware Flashing could not connect to the board.	Critical. Either there is another process currently attached to the board, or the bus is too busy to allow the request. Auto Flash is now turned off on the SC for this slot.
Firmware Flashing failed at downloading firmware	Critical. The firmware file does not exist on the SDM or has incorrect parameters.
Firmware Flashing failed at validating firmware	Critical. The firmware file is corrupt on the SDM, or there was an error in the transfer.

SAM21 Logs/Faults available

Log/Fault	Description
Firmware Flashing failed at backing up the firmware.	Critical. The copy operation from one bank to the other failed. Possible bad memory.
Firmware Flashing failed flash	Critical. Could not connect to the board after the flash.
Provision failed: process ended abnormally. Provision failed, could not connect to board. Provision failed to set application type.	Critical. Provisioning of the board failed due to some system problem. System may have been abnormally busy.
UnderlyingResourceUnavailable	A minor alarm when it indicates that an application card is locked and is not available, but a major alarm when it indicates that an application card is being autorecovered.

MCS Manager Logs/Faults

The following table lists the MCS Manager Faults and Alarms available through equipment such as MAS, BCP7200, SSLines, and MCS5200. Note that only alarms are sent northbound. MCS Manager can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled "IEMS Functionality." For details on the logs, refer to NN10383-900, *Fault Management Alarm and Log Reference,* NN10332-911. *Session Server Fault Management,* and NN10035-111, *MCS5200 RTP Media Portal Basics*.

MCS Manager Logs/Faults

Log/Fault	Description
AC102	Trunk Framing settings on the connected PSTN switch do not match those provisioned on the Audiocodes Mediant 2000.
AC105	The port on the gateway is unable to tell the trunk is in-service. At this point, the trunk will attempt to send an Alarm Indication Signal (AIS).
AC107	There is a physical problem in the connectivity of the trunk to the gateway. In order to receive this alarm, the far end could be offline or disconnected.
AC128	The gateway is no longer responding to SNMP polling. Either SNMP is misconfigured, the gateway is network isolated, or the gateway is not operational.
DBCM101	A network element has lost communication with the database.

MCS Manager Logs/Faults

Log/Fault	Description
DBMN101	The System Manager cannot communicate with the SNMP agent that provides the database monitoring raw data.
DBMN102	Indicates an inability of the database SNMP agent to process the requests sent by the System Manager.
DBMN103	Indicates that the operational state of the database server process is a value other than "UP".
DBMN401	Indicates that the amount disk space used by the database is approaching its limit.
EMTC401	A threshold has been crossed. The number of unreachable static clients has reached or exceeded the configured percentage of 100 % ... currently there are 20000 unreachable clients. Also functions as a Clear log.
FTP703	The FTP operation of OAM records to the OSS destination failed due to the error encountered in creating directory on the base directory configured.
FTP704	Indicates the FTP operation of OAM Record to the OSS destination failed with an error message.
FTP706	Indicates the FTP operation of OAM records failed because of failure of login for the userid and password configured.
IMDB700	Indicates an internal cache in the network element (NE) has failed to load its data from the database during system initialization.
IMDB701	Indicates an internal cache in the network element (NE) has failed to synchronize its data with the database during regular system operation.
IMDB702	Indicates an internal table of the network element (NE) that is kept in memory has reached or is nearing its capacity.
KCRE201	Indicates a license key code resource owner is unable to update the resource management tables with its new key code limit from a newly applied license key.
LKEY470	Indicates the license key limit for a resource has reached or exceeded thresholds licensable limits.
LKEY750	Indicates the System Manager is not able to retrieve the license key from the database.
LKEY751	Indicates that the license key file could not be decrypted. This can be caused by: an invalid license key file, incompatible version of the license key file, or a corrupt license key file.
LKEY752	Indicates an error occurred during validation of the license key.
LKEY753	Indicates an error occurred during validation of the license key file when a license key has keycodes that are not compatible with the installed software.
LKEY754	Indicates an error occurred validating the license key file against the target system hardware.
LKEY755	Indicates that the license key upgrade failed because the supplied license key was intended for a system with a newer software release.
LOAD801	Indicates a new load becomes available in the loads directory (/var/mcp/loads).

MCS Manager Logs/Faults

Log/Fault	Description
MAS102	Indicates the MAS Provisioning Manager is unable to communicate with the database.
MAS103	Indicates the MAS Provisioning Manager is unable to communicate with one of the Media Application Server(s) configured in the system.
MAS300	Indicates that all initial connections upon startup are being established.
MAS301	Indicates the MediaController has lost connectivity with one or more processes.
MAS302	Indicates one or more MAS system components have failed to properly initialize.
MAS303	Indicates the MediaController is having some difficulty communicating with a particular process.
MAS304	Indicates the license key provided to the MediaController was invalid.
MAS305	Indicates the MediaController could not find the MAS license key.
MAS306	Indicates that all G711 licenses have been exhausted.
MAS307	Indicates all G729 licenses have been exhausted.
MAS308	Indicates the G711 license counter is getting close to exhausted.
MAS309	Indicates the G729 license counter is getting close to exhausted.
MAS310	Indicates the primary MediaController peer connectionhas failed.
MAS311	Indicates the MediaController peer backup connection has failed.
MAS312	Indicates the MediaController component is in a shutdown state.
MAS313	Indicates the MediaController is in a lock-pending state.
MAS314	Indicates the MediaController is in a locked state.
MAS327	Indicates a CStore is configured with a Content Store Mirrored Peer Server but is not connected to it.
MAS328	Indicates that a synchronization is in progress and that data may still be in the process of being copied with the peer content store. Occurs upon System restart or connection reestablishment with peer Content Store.
MAS329	Indicates CStore determined the pre 3.0 data format is present in the storage root.
MAS330	Indicates the CStore has been shutdown and is not running.
MAS331	Indicates the disk containing the Storage Root is at or near capacity (less than 1073741824 bytes available).
MAS351	Indicates the IvrMP component is in a shutdown state.
MAS361	Indicates the ConfMP component is in a shutdown state.
MAS371	Indicates the StreamSource component is in a shutdown state.
MAS382	Indicates the ConferenceManager process on the MAS has been shutdown and is not running.
MAS383	Indicates the connection between the MAS and the Web Collaboration Server is down.

MCS Manager Logs/Faults

Log/Fault	Description
MAS504	Indicates the number of pending transactions in the database exceeds 100,000.
MAS701	Indicates an error was encountered during the initialization of the MAS Provisioning Manager.
MAS705	Indicates more than two Media Application Servers have been found for a given pooled entity configured in the system.
NCAS101	An NCAS link has been disconnected from a specified IP address. Also functions as a Clear log.
NECM101	Indicates the System Manager is unable to communicate with an online network elelment (NE) instance.
NECM102	Indicates that the Fault/Performance Manager (FPM) that is configured to manage network element (NE) has no running instance.
NED101	Local communication with NED (Network Element Daemon) lost. This normally indicates NED has died, in which case it should automatically be restarted. Also functions as a Clear log.
NIF100	Indicates a network element instance configured with a floating IP address is unable to send a gratuitous ARP to associate the IP address with a logical interface.
NIF200	The logical interface for a specified floating IP Address is not up. Also functions as a Clear log.
NIF201	Failed to down logical interface for a specified floating IP Address. Also functions as a Clear log.
OLC401	Indicates the calls will be failing as the component has gone in overload mode.
OLC402	Indicates the database has gone into overload mode.
OLC403	Indicates the memory is exhausted.
R6AS700	R6AS configuration modified while instance is not offline. Also functions as a Clear log.
RESM701	Indicates the resource management partition audit raised an alarm when the resource management partition table usage values differ from the actual usage values returned from the resource owner.
RESM702	Indicates the resource management partition audit raised an alarm when the resource management partition table usage percentage are above the alarm thresholds.
RTA101	Indicates that the status of the standard recording stream is down.
RTA201	Indicates that there is an exception occurred when recording a data record into the spool directory of the network element instance.
RTP101	Critical. Raised from alarm “Blade Out of Service.” Occurs when Managed IP or MCP Service network difficulties (communication problems) are encountered when attempting to communicate with the Media Blade specified by BladeName.
RTP102	Critical or Major. Raised from alarm “RTP Media Portal Out of Service.” Occurs when timer activated event checks availability of Media Blades that are currently configured or when a OutOfServiceAlarm is raised.

MCS Manager Logs/Faults

Log/Fault	Description
RTP103	Critical. Raised from alarm “Best Blade Selection.” Occurs during session setup when the host attempts to determine which media blade should handle the session.
RTP104	Critical, Major, or Minor. Raised from alarm “Port Usage.” Occurs when timer activated event checks to see what percentage of the configured Managed IP Network ports are in use. Alarm severity is based on the percentages configured for the parameters: "Minor Port Usage Alarm Level," "Major Port Usage Alarm Level," and "Critical Port Usage Alarm Level."
RTP105	Major. Raised from alarm “Host Interface Failure.” Occurs when a timer activated event checks the status of host network interfaces.
RTP106	Major. Indicates a communications problem (e.g. network difficulties) was encountered when attempting to communicate with the Media Blade specified by Blade Name ($1).
RTP107	Major. Indicates link issues (e.g. carrier sense fails) were encountered when attempting to communicate over a problem interface (specified by Interface Name $2) on the identified Media Blade (specified by Blade Name $1).
RTP108	Critical. Indicates a Session Manager does not receive responses to requests made to the only available RTP Media Portal in its media resource pool.
RTP109	Major. Indicates a Session Manager does not receive responses to requests made to an available RTP Media Portal in its media resource pool.
RTP801	Minor. Indicates there is a change made to configuration data for an in-service RTP Media Portal.
RTP802	Critical. Indicates this RTP Media Portal is not configured correctly.
RTPB804	An error occurred during initialization. test-string. The RTP Media Portal is NOT operational. Also functions as a Clear log.
RTPB805	The RTP Media Portal Blade in slot 1 is in Standby. Also functions as a Clear log.
RTPB806	Cluster is in a 1+0 configuration with 0 node(s) shutting down and should be in a 1+1 configuration. Also functions as a Clear log.
RTPB815	Live Update of Media Portal Cluster Configuration Parameters Data is NOT supported. Also functions as a Clear log.
RTPB816	Live Update of Media Portal Cluster Fault Tolerance Data is NOT supported. Also functions as a Clear log.
RTPB817	Live Update of Media Portal Cluster Gateway Controllers Data is NOT supported. Also functions as a Clear log.
RTPB818	Live Update of Media Portal Cluster Session Managers Data is NOT supported. Also functions as a Clear log.
RTPB819	Live Update of Media Portal Cluster Static Routes Data is NOT supported. Also functions as a Clear log.
RTPB820	Live Update of Media Portal Cluster Service Instance Data is NOT supported. Also functions as a Clear log.

MCS Manager Logs/Faults

Log/Fault	Description
SEC820	Minor, Major, or Critical. Indicates a certificate in the internal keystore will expire in 89 days or less.
SEC821	Minor, Major, or Critical. Indicates a certificate in the internal truststore will expire in 89 days or less.
SIP401	The number of 500 Server Internal Error responses to SIP 9273429374@47.102.244.146 requests in OM group SIP_Inbound_Response_Report exceeds the specified percentage of responses. Also functions as a Clear log.
SIP703	Raise: Message received that contained bad syntax information. Bad headers will be discarded. Also functions as a Clear log.
SMCM101	Major. Indicates an online network element (NE) instance cannot communicate with the System Manager.
SRVR101	Major. Indicates the SNMP agent on the server cannot be contacted.
SRVR102	Major. Indicates the Server Monitor encountered unexpected error responses to the SNMP queries.
SRVR401	Indicates the CPU Occupancy of the monitored Server equals or exceeds the configured threshold.
SRVR402	Indicates the RAM Utilization of the monitored Server equals or exceeds the configured threshold.
SRVR403	Indicates the disk space utilization for a partition on the monitored Server equals or exceeds the configured threshold.
SRVR404	Indicates the interface utilization for a physical interface on the monitored Server equals or exceeds the configured threshold.
SVCA801	The System Manager service address has changed. Also functions as a Clear log.
SYNC200	Indicates that the configuration data for an NE instance is out-of-sync.
SYS101	Major. Peer network element instance presumed failed.
SYS102	Major. Indicates a fault tolerant Status message was received by a network element instance when no peer is provisioned for that instance.
SYS103	Major. Indicates a fault tolerant Status message was received by a network element instance when from a peer whose IP address is different from that of the provisioned peer..
SYS104	Major. Indicates a network element is in a fault tolerant configuration and a peer instance informs an instance that it believes it to be failed. This can happen if there is one way network failure or congestion from the instance to its peer.
SYS105	Major. Indicates a network element instance is isolated from the network. This indicates a failure in all network interface cards connected to that network.
SYS106	Critical. Indicates an unusual condition where a peer network element instance believes it is network isolated but is still able to communicate the isolation condition to the local instance.

MCS Manager Logs/Faults

Log/Fault	Description
SYS703	Major. Indicates a network element instance in a fault tolerant configuration when a peer instance is in the ACTIVATING phase but fails to transition to ACTIVE within the time specified by the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout".
SYS704	Major. Indicates a network element instance in a fault tolerant configuration when a peer instance is in the DEACTIVATING phase but fails to transition to SHUTDOWN within the time specified by the engineering parameter "FaultTolerance:PeerActivityTransitionTimeout".
SYS707	A request to receive synchronization from peer is rejected. Also functions as a Clear log.
TCF902	Major. Indicates a network element is in a fault tolerant configuration and a peer instance informs an instance that it believes it to be failed. This can happen if there is one way network failure or congestion from the instance to its peer.
TCF903	Critical. Indicates a failure to create a TCP server or UDP based socket.
THLD401	Indicates a generic threshold alarm provided by the OM framework.
THLD402	Indicates a generic threshold alarm provided bythe OM framework.
TSVR700	Critical. Indicates the failure by the session manager to connect to the terminal server provisioned in the voicemail server configuration page on the provisioning client.
TSVR701	Major. Indicates that the session manager failed to connect to the terminal server on the specified address and port..

SPM--available logs/faults

The following table lists the SPM family Logs/Faults available.
The SPM family supports SCC2 or NT STD formatted logs through SDM functionality, or it can be supported through IEMS. For details on the IEMS interface, refer to the chapter in this document titled “IEMS Functionality.” For details on the logs/faults themselves, refer to the Fault Management section of the appropriate SPM FCAPS documentation and NN10275-909, *Fault Management Log Reference.*

- SPM: NN10075-911
- DPT-SPM: NN10079-911 (IP)
- IW-SPM: NN10077-911 (IP)

General SPM Logs/Faults available

Log/Fault	Description
Network Element: SPM (all variants)	
ATM300	Generated when a Loss of Cell Delineation (LCD) alarm condition is raised on an SPM with ATM RMs.
ATM50	An alarm that is raised if the SSI (Signal State Interrupt) count gets too high. The alarm is reported as an NE305 log, which is changed to allow a new or additional reason code

General SPM Logs/Faults available

Log/Fault	Description
ATM501	The system's ATM signaling status has changed.
ATM600	The ATM framework has gained a registered ATM address.
ATM601	The ATM framework has been de-registered by the ATM network.
ATM604	System software cannot recover the ATM Framework (ATM RM will be busied and RTS'ed)
ATM605	ATM overload event.
ATM606	ATM service failure.
ATM800	A trouble log that indicates possible degradation of service related to ATM Performance Monitoring thresholds.
ATMBCN	This alarm is raised when the ATM framework cannot support bearer connections. The alarm causes the SPM to show at the PM portion of the alarm banner as "SPM *C*." This alarm complements the ATMFW alarm currently displayed beneath the APPL banner.
BITS300	A clock sync critical alarm has been raised for one of these: MTIE Performance, Alarm Indication Signal, Loss of Signal, or Out of Frame. Correlates with BITS600.
BITS301	A clock sync non-critical alarm has been raised for one of these: Timing Link Degradation, Bipolar Violation, or Cyclic Redundancy Check. Correlates with BITS601.
BITS500	BITS link state change capturing old/new states and reason for change (including degradation of carrier (LOS, LOF)).
BITS600	BITS Fault Report Cleared; critical alarm from BITS300 is cleared.
BITS601	BITS Fault Report cleared; non-critical alarm from BITS301 is cleared.
BITS610	Reference Quality Change to a new SSM state.
BITS612	BITS Reference Switch; indicates the reason for the reference switch.
C7UP109	A CQ state change has occurred.
C7UP113	Indicates ISUP maintenance trouble.
C7UP114	Generated for an ISUP alert.
C7UP120	An invalid range field exists.
C7UP130	The HOP counter has expired.
C7UP301	The HC value is not sufficient.
CARR300	A carrier failure event cleared. Correlates to alarms AIS, APSAM, APSCHMM, APSIC, APSMM, BERSD, BERSF, LOF, LOP, LOS, PLM, RAI, RFI, SIMPLEX, TIM. Correlates with CARR310.
CARR310	A carrier failure event has occurred. Correlates to alarms AIS, APSFC, APSFEPLF, APSLCK, APSMAN, BERSD, BERSF, LOF, LOP, LOS, PLM, RAI, RFI, SIMPLEX, TIM.
CARR315	A trouble log that includes the actual fault description text sent by the MG9K.
CARR330	A protection switch has occurred. A previously inactive carrier in the protection group takes over as the active carrier.

General SPM Logs/Faults available

Log/Fault	Description
CARR331	A protection switch was attempted but failed.
CARR340	The inactive carriers in a protection group have changed state in such a way that they cannot carry traffic. The protection group is now running in simplex mode.
CARR341	Both carriers have become available and normal protection switching can occur.
CARR500	A carrier changes to an in service (InSv) state from manual busy (ManB) or system busy (SysB). Correlates to a MANB and SYSB alarm. Correlates with CARR511.
CARR501	A carrier changes to central-side busy (CBsy) from ManB or SysB. Correlates to a MANB and SYSB alarm.
CARR510	A carrier changes to ManB from InSv, SysB, or CBsy. Correlates to a MANB and SYSB alarm.
CARR511	Carrier state change to SysB from InSv or CBsy. Correlates to a SYSB alarm.
CARR512	OC3 carrier state change to CBsy from InSv, ManB, or SysB. Correlates to a MANB and SYSB alarm.
CARR800	Threshold crossing alert (TCA) for a metered performance parameter has been cleared.
CARR801	Indicates that maintenance limits have been re-set.
CARR810	TCA event for metered performance parameter has occurred. Correlates with CARR800.
CARR811	TCA event for non-metered performance parameter has occurred. Also applies to STS-1 carrier on MG4000.
DPTM500	The state of DPT Terminals changed to IDL state from any other state.
DPTM501	The state of DPT Terminals changed to SYSB state from any other state.
DPTM502	The state of DPT Terminals changed to MANB state from any other state.
DPTM503	The state of DPT Terminals changed to PMB state from any other state.
DPTM504	The state of DPT Terminals changed to INB state from any other state.
DPTM700	Bulk downloading or dynamic update of DPT data failed, so there is a data mismatch in the CM and node. Correlates with DPTM701.
DPTM701	The DDM audit process cleared a DPT data mismatch between the core and the node.
DPTM702	Indicates a call is rejected because the DPT SOC limit is reached.
DPTM800	Office-wide DPT terminal usage exceeds the level 1 threshold of 70%. Logs DPT800-803 are associated with OM group DPTOFC, registers DPUSAG and DPUSAG2; and OM group DPTNODE, registers DPTUSAG and DPTUSAG2.
DPTM801	Office-wide DPT terminal usage drops below the level 1 threshold of 70%.
DPTM802	Office-wide DPT terminal usage exceeds the level 2 threshold of 90%.
DPTM803	Office-wide DPT terminal usage drops below the level 2 threshold of 85%.
EAD115	Problems with performance data collection associated with an OSS.
EAD116	Problems with the collection of MG 4000 performance data.

General SPM Logs/Faults available

Log/Fault	Description
ENET308	ISTb state occurs or is cleared on a PSLINK. Correlates to an ISTB alarm. Associated with OM group ENLKERR.
ENET311	The SPM ATM node is SYSB, and a network error has caused it to be isolated from the ENET links or the MS ports. Correlates to a SYSBNA alarm.
IOAU112	Information log related to changes in System REX controller operation or schedule.
IWBM500	One of the following is out of service: C-side link, STS3cP carrier, ATM network state, or the ATM address state for the IW bridge software.
IWBM501	The out-of-service item in IWBM500 has returned to service.
IWBM502	Indicates that a BSY command is being requested for a set of IW SPM bridge terminals.
IWBM503	Indicates that an RTS command is being requested for a set of IW SPM bridge terminals.
IWBM504	Indicates that an OFFL command is being requested for a set of IW SPM bridge terminals.
IWBM505	Indicates that a FRLS command is being requested for a set of IW SPM bridge terminals.
IWBM600	The IW bridge receives an invalid terminal ID during an attempt to free a bridge causing a connectivity mismatch. An INFO log.
IWBM601	Automatic system audit finds a problem and performs a corresponding action. An INFO log.
IWBM602	No IDL bridges are available. An INFO log.
IWBM603	An IWBM audit is being performed. An INFO log.
IWBM700	A maintenance action is being performed. An INFO log.
IWBM800	Number of available IW bridges exceeds the first threshold (70%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.
IWBM801	Number of available IW bridges falls to less than 65% of bridges in the pool in use. This log always occurs after IWBM 800.
IWBM802	Number of available IW bridges exceeds the second threshold (90%) when attempting to retrieve an IW-bridge ID from the IW bridge manager.
IWBM803	Number of available IW bridges falls to less than 85% of bridges in the pool in use. This log always occurs after IWBM 802.
Link300	A transport resource fault indicating a mis-connected DS512 link.
NODE300	The integrated node maintenance (INM) generates this log when a trouble condition is present with the node. The log indicates INM recovery actions when the node state is system busy.
NODE302	Reports a software alarm.
NODE303	Generated to report the Wrong Application Data on the SPM.
NODE326	Generated to report a hardware fault on the SPM.
NODE500	System node state change. Correlates to a SYSB alarm.
NODE600	An INFO log to notify of a system recovery action.

General SPM Logs/Faults available

Log/Fault	Description
NODE601	An INFO log that provides system status notification.
NODE602	Indicates the reason for CEM state transition, generated only when the CEM state transitions from Insv to Istb or Insv to Sysb.
PM231	Indicates that a PM failed to acknowledge an audit request to add or delete a channel connection.
PM232	Indicates that a PM operation from an audit request to add or delete a channel connection has succeeded.
PM233	Indicates that a PM operation from an audit request to add or delete a channel connection has failed. The request is from Special Connection Table Control Facility (SPECCONN) to add or delete a channel connection. The subsystem generates the modified log when the operation to update to the correct status fails for two consecutive audit cycles.
PM234	Indicates that a PM failed to acknowledge an audit request to add or delete a channel connection.
PM236	Generated when the system finds integrity, does not find integrity, or loses integrity. Displayed when one of the following scenarios occurs: the system makes a special connection; integrity was lost or not found; or the SPECCONN audit acted on a special connection that has the status of NO_IINTEG.
PRSM400	A DPT SPM ATM loadfile containing DPT SPM ATM PRSU fixes has been datafilled in table PMLOADS.
SOC802	A warning log that the current configuration of the number of DPT ports is not authorized by Nortel, due to a conflict between the SOC limit and the setting of office parameter DPT_MAX_PORTS.
SPM300	A device fault has occurred. Correlates to a MANB, PROTFAIL, SYSB, and NOSPARE alarm.
SPM300	A device fault has occurred. Correlates to a MANB, PROTFAIL, SYSB, and NOSPARE alarm. SN08 added a new text reason showing that it is generated when a STS3L carrier experiences an RFI alarm. SN08 added the acitivty/status of the unit/device. SN08 added next text “Device Fault Report” due to being triggered via resource exhaustion/overload conditions on the ATMRM.
SPM301	SPARTS patching log. An SPM patch is missing after an RTS occurred. Correlates to the PATCHFAIL, VCXO70, and VCXO90 alarms.
SPM310	The CM has received performance data from the DPT SPM ATM as a result of the DPT SPM ATM-based automatic monitoring process.
SPM311	A software exception report (SWER) has occurred, OR one of the BITS links is out-of-service. Correlates to an LOR alarm.
SPM312	A TBL trap has occurred on the CEM.
SPM313	A fault has been recorded in the Module Information Memory (MIM) of the SPM.
SPM314	A generic IMC fault report to indicate a change in IMC status.
SPM330	The two CEMs have either come into datasync or have gone out of datasync. Correlates to an ISTB alarm.

General SPM Logs/Faults available

Log/Fault	Description
SPM331	A device had a protection switch failure. Modified to place IP RM in the circuit pack field. Correlates to a MANB, PROTFAIL, SYSB, ISTB, and NOSPARE alarm.
SPM332	The synchronization reference source was switched by manual action, switched by system action, or lost the last synchronization reference in the OC-3 protection group.
SPM333	Indicates an SPM Rex test failure.
SPM334	An alternate synchronization source is not available and the timing configuration no longer conforms to SONET specifications. Correlates to a CLKOOS alarm.
SPM335	A device had a protection switch failure.
SPM336	The clock oscillator tuning range has reached 90% of the maximum range. Correlates to a VCXO90 alarm.
SPM337	SPM has entered Holdover. Correlates with SPM637.
SPM338	SPM has been in Holdover over 24Hours. Correlates withSPM638.
SPM339	The clock oscillator tuning range has reached 70% of the maximum range. Correlates to a VCXO70 alarm.
SPM340	A CM warm switch of activity (SWACT) failed.
SPM341	A SyncRM has entered into 3E Holdover state due to a clock mode change. Correlates with SPM641.
SPM342	A SyncRM has entered into 3E Holdover 24 State. Correlates with SPM642.
SPM344	The SyncRM Loss of BITS Redundancy (LOR) alarm has been set. Correlates with SPM644.
SPM350	There is the potential for resource exhaustion of a particular resource type. Correlates to the COTLOW, DTMFLOW, MFLOW, TONESLOW, and ECANLOW alarms. The log also generates when the alarm is cleared.
SPM352	Both of the Sync RMs are in holdover, so the SPM has entered Stratum 3E Holdover. Alarm ST3EHLDOVR is raised. Correlates with SPM652.
SPM353	Both of the Sync RMs are in holdover for 24 hours, so the SPM has entered Stratum 3E Holdover24. Alarm ST3EHLDOVR24 is raised. Correlates with SPM653.
SPM354	Both of the Sync RMs are out-of-service, so the SPM has entered SMC holdover. Alarm SMCHLDOVR is raised. Correlates with SPM654.
SPM355	Both of the Sync RMs are out-of-service for 24 hours, so the SPM has entered SMC holdover24. Alarm SMCHLDOVR24 is raised. Correlates with SPM655.
SPM356	One of the Sync RMs is out-of-service, so the SPM has lost clock unit redundancy. Alarm SPMLOCR is raised. Correlates with SPM656.
SPM358	A tuple change from EXTERNAL to LINE, or from LINE to EXTERNAL, is performed, and the SPM clock reference change failed. Correlates with SPM658.
SPM370	A log report of an SPM health monitor event. Connection errors have been corrected by the DLC Audit. Correlates with SPM670, the clearing log.

General SPM Logs/Faults available

Log/Fault	Description
SPM399	Generated whenever an SPM enters or leaves an overload condition. SN08 added next text “SPM Overload Report” due to being triggered via resource exhaustion/overload conditions on the ATMRM.
SPM500	A SyncRM device state change has occurred with new state and reason for change (e.g. SYSB, MANB). Modified to place IP RM in the circuit pack field. Correlates to a MANB, PROTFAIL, SYSB, and ISTB alarm.
SPM605	Indicates that a particular resource RM protection group is excluded by the SPMRESALIGN tool, without align RMID-PWID values.
SPM610	Generated whenever an SPM node SSM value changes.
SPM611	A reference node switch has occurred.
SPM630	A device protection switch (i.e. clock unit switch) has occurred. Modified to place IP RM in the circuit pack field. Correlates to a MANB, SYSB, and ISTB alarm.
SPM632	Generated when the REX test on the SPM is successful.
SPM633	Generated when the REX test has started on an SPM node.
SPM637	The clock mode has changed from Holdover to Sync. Correlates with the HLDOVR alarm.
SPM638	The SPM recovers from the 24-hour Holdover state; the clock mode changes from Holdover to Sync. Correlates to the HLDOVR24 alarm.
SPM641	A SyncRM has exited 3E Holdover state.
SPM642	A SyncRM has exited 3E Holdover 24 state.
SPM644	The SyncRM Loss of BITS Redundancy (LOR) alarm has been cleared.
SPM645	Link Protocol & Messaging Interface Controller (LPMIC) Event Report. This log is generated on every CEM and transported to the core. The log is generated periodically and whenever the number of events crosses a threshold value.
SPM650	A successful in-service loading procedure has occurred. Modified to place IP RM in the circuit pack field.
SPM651	An in-service loading procedure has failed. Modified to place IP RM in the circuit pack field.
SPM652	SPM has exited Stratum 3E Holdover. Alarm ST3EHLDOVR is cleared.
SPM653	SPM has exited Stratum 3E Holdover24. Alarm ST3EHLDOVR24 is cleared.
SPM654	SPM has exited SMC Holdover. Alarm SMCHLDOVR is cleared.
SPM655	SPM has exited SMC Holdover24. Alarm SMCHLDOVR24 is cleared.
SPM656	SPM loss of clock unit redundancy cleared. Alarm SPMLOCR is cleared.
SPM657	Input timing signals degradation cleared. Alarm SPMTLD is cleared.
SPM658	A PM timing mode change has occurred with explicit reason (e.g. line to external due to manual request).

General SPM Logs/Faults available

Log/Fault	Description
SPM660	A continuous performance-monitored trunk member was involved in an answered echo canceller call. This log reports the performance data.
SPM661	A continuous monitoring ON/OFF command or an SPMECMON AUTO command has successfully completed.
SPM670	An INFO log to report that the health monitor “CallCount PTS no setup fault” has been cleared. Correlates with SPM370, the raise log.
SPM680	Indicates low MBM Application Buffers.
SPM682	Indicates CEM manual reset.
SPM683	Indicates lthe reason for CEM swact.
SPM684	Indicates that the erase flash command has initiated, is completed, has failed, or has been rejected. SN08 added the acitivty/status of the unit/device.
SPM701	A DDM audit has successfully updated an SPM subgroup.
SPM702	A DDM dynamic update has failed for an SPM subgroup.
SPM703	A DDM audit has updated an SPM trunk member in a with a data entry for a trunk that failed to be added during a dynamic update.
SPM704	A DDM dynamic update has failed for an SPM trunk member.
SPM705	A trunk has been set to a lockout (LO) or SysB state. Correlates to SPM706.
SPM706	A trunk has returned to service from a LO state.
SPM707	A dynamic update has failed for the ISDNPARM table.
SPM708	The DDM audit has updated the ISDNPARM table.
SPM709	A dynamic update has failed for the ISDNPROT table.
SPM710	The DDM audit has updated the ISDNPROT table.
SPRF670	Generated every 15 minutes by the SPMACT tool. The logs are a compilation of the tool’s results. Each line of the log corresponds to a performance measurement taken every minute by the tool.
SPRF671	Generated every 15 minutes by the SPUSAGE tool to summarize samples taken every minute of the call-processing events that occur in the SPM.
VOIP800 Log	This log is generated for any of the following reasons: - Cyclical Redundancy Check Error- Broadcast Packets - Undersize Packets- Jitter - Oversize Packets- Latency - Fragments- Lost Packets - Jabber- Decoder Under run - Drop Events
XAC329	Enhanced to provide more detailed reason text description for a number of failure scenarios in IRM, including a link state change. A customized text string is added for each IRM error code to help determine the causes resulting from link failure events.

General SPM Logs/Faults available

Log/Fault	Description
Sync RM alarms	
LOS	Sync RM cannot detect a signal from the BITS timing link. Cleared when a signal is detected.
OOF	Sync RM cannot detect a DS1 frame for a given BITS timing link. Cleared when a DS1 frame is detected.
AIS	Sync RM detects an AIS on an incoming BITS timing reference signal from BITS, or crossover from alternate SPM reference node. Cleared when incoming BITS timing reference signal does not have an alarm.
MTIE2	MTIE performance for input signal exceeds the GR-253 requirement mask threshold, indicating an unusable signal. Cleared when MTIE is below GR-253 requirement mask threshold.
TLD	MTIE performance for input signal exceeds the GR-253 requirement mask threshold, indicating a degraded signal. Cleared when the MTIE Level 1 degradation disappears from timing reference.
BPV	Incoming signal has BPV alarm, indicating a degraded signal. Cleared when BPV disappears from timing reference.
CRC	SyncRM detects a CRC from incoming signal, indicating a degraded signal. Cleared when the CRC disappears from the timing reference.
LOR	SyncRM cannot detect the DS1 frame from BITS timing links or signal from Mate SyncRM, indicating that redundancy is lost. Cleared when a DS1 frame is detected.
HLDOVR	SyncRM has gone into the holdover mode because both BITS timing links were lost. Cleared when SyncRM exits holdover mode.
Bearer connections alarm	An alarm for bearer connections is added to the list of alarms in table MNNODE.

Stormia (STM)-available logs/faults

The following table lists the STM logs available. STM logs will only be present in the HLR market. For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference.*

STM logs available

STM398	Indicates a raised alarm in an STM device.
STM399	Indicates a cleared alarm in an.STM device.

UAS--available logs/faults

UAS faults are sent from the UAS to the UAS EM and are then sent northbound via CORBA. UAS alarm information can also be viewed from the alarm browser that resides with the CS2000 Management Tools. For details on

the CORBA protocol/format and the logs, refer to the Fault Management section of UAS FCAPS documentation, NN10073-911 and NN10275-909, *Fault Management Log Reference.*

Refer to the New and Changed section of this document to see if there are SN09 changes in UAS logs and faults.

UAS Logs/Faults available

Network Element: UAS

UAS faults are sent from the UAS to the UAS EM and are then sent northbound via CORBA. UAS alarm information can also be viewed from the alarm browser that resides with the CS2000 Management Tools.

Fault	Description	For details on these Logs/Faults, refer to the Fault section of documentation for UAS, NN10073-911.
ATM Alarms	AS001	An ATM interface card is missing from the slot.
	AS002	There is a different ATM card module inserted in the chassis slot.
	AS003	The ATM card has detected an H.110 bus failure.
	AP001	The ATM interface port has had a loss of connectivity.
Ethernet Interface Alarms		
	EI_LINK_DOWN; Critical. “Callp was unable to initialize interface to hardware. Check configuration.” Clear with a reboot.	
88065 (366)	EI_LINK_DOWN; Critical. “Link on host network interface is down.”	
Call Agent Connection Alarms		
8193 (301)	THREAD_DEATH_ALARM; Critical. Either the “ingoing” or “outgoing” messaging thread is unable to restart because of some undetermined problem. Clears at the next startup of call processing application.	

UAS Logs/Faults available

8194 (302)	UDP_INIT_FAIL_ALARM; Critical. This alarm can be raised for various reasons during initialization. The audio server is unable to communicate with the call server. The condition clears at the next startup of the call processing application. Possible reasons and corrective actions follow: MGC IP address is not datafilled because the uas.conf file either does not exist, is unreadable, or is missing an entry for “CallAgentIPAddress.” Fix the configuration file. MGC IP address is not valid because the call agent IP address obtained from the config file is not valid. Fix the IP address in the config file. Bad return code from WSAStartup because an attempt was made to initialize the Windows socket library, but failed due to a version mismatch. Report the full text of the alarm to the support group. WinSock version is not 1.1 as expected because an attempt was made to initialize the Windows socket library, but failed due to a version mismatch. Report the full text of the alarm to the support group. Unable to create socket; an attempt was made to create a UDP communications socket, but failed. Report the full text of the alarm to the support group. Unable to bind client name to socket; an attempt was made to bind the communications socket to the port specified in the uas.conf configuration file. Another callp program may already be running. Make sure that another callp program is not running. Unable to connect to call agent socket; an attempt was made to associate the communications socket with the address of the call agent, but failed. Report the full text of the alarm to the support group.
8195 (800)	SOCKET_ERROR_ALARM; Warning. UDP Socket errors are being detected.
8196 (801)	RETRANS_ALARM Warning, Retransmissions are being detected.
8197 (802)	EXCEED_MAX_RETRANS_ALARM; Warning, Call_Agent_Connection, The number of retransmissions has now exceeded the maximum number of retransmissions.
System Alarms	
6154 (379)	NODE_NO_CARDS_INSTALLED; Critical. “There are no NMS cards installed.”
Call Engine Alarms -- associated with call processing or maintenance state machines.	
12290 (303)	CALLP_THREAD_NOT_RESTARTED; Major. The call processing software thread associated with <endpointId> died due to an unhandled software error, and was not restarted because it died too quickly after the previous start. Escalate this issue to Nortel support, providing any other logs that might have occurred. Clears at the next startup of the call processing application.
12291 (304)	CALLP_CFG_INVALID; Critical. The resource configuration for endpointId in C:\uas\etc\rm.resources is not valid. Correct the configuration for endpointId in the rm.resources file, and restart the call processing application. Clears at the next startup of the call processing application.
12295 (305)	AUDIO_VFSDIR_NOT_SET; Critical. The environment variable VFSDIR is not set to the home directory of the VFS hierarchy. Verify that the VFS software is correctly installed. Clears at the next startup of the call processing application.

UAS Logs/Faults available

12296 (306)	CALLP_CONFIG_PROB; Critical. A serious configuration problem has been detected. The Audio Server is unable to initialize. A configuration file is probably in error. Look for an error log to determine the exact cause of the problem. Clears at the next startup of the call processing application.
12297 (307)	CALLP_NO_CARDS_AVAILABLE Call_Engine There are no NMS cards available for use.
12298 (308)	CALLP_AUDIO_RESYNC_FAILURE Call_Engine Failed to communicate with aliasServer. Check audio installation and aliasServer.

AG4000 Service-level Alarms -- conditions that affect the service-level functionality of the AG4000 card in an ATM system.

14337 (315)	AG_GENERIC_ALARM; Major. An attempt was made to load software onto the card and to start the card but failed. Stop the applications, reseat the card and then restart the applications. If the problem persists, contact the Nortel support group. Clears when the applications are restarted and the operation succeeds.
14338 (315)	AG_SURPRISE_EXTRACTION Improper extraction of AG4000 card in slot <x> of the SAM 16 chassis.
14339 (316)	AG_CARD_DISABLED AG4000 card in slot <x> disabled until next application restart of the UAS.

NodeMtc Alarms -- generated by the callp application if the NMS CT daemon and NMS Clock Fallback Manager services fail to stop or start successfully.

20481 (322)	CTDAEMON_SERVICE_FAILURE; Critical. Either the NMS CT daemon service is not installed as a service, or it is in a service state where it cannot accept start and stop service requests. Make sure that the NMS CT daemon service is installed. Stop, uninstall and re-install the service if need be. Clears once the NMS CT daemon service has been successfully started or stopped.
20482 (323)	CFBM_SERVICE_FAILURE; Critical. When the NMS CT daemon service is started, it should automatically start the NMS Clock Fallback Manager service (The NMS Clock Fallback Manager service is not automatically stopping the NMS CT daemon service.). If the NMS Clock Fallback Manager service is not automatically started for some reason, either the NMS Clock Fallback Manager service is not installed as a service for it to be started or stopped, or it is in a service state where it cannot accept start and stop service requests. Make sure that the NMS Clock Fallback Manager service is installed. Stop, uninstall and re-install the service if need be. Clears once the NMS Clock Fallback Manager service has been successfully started or stopped.
20483 (324)	SERVICE_FAILURE NodeMtc The <x> service could not be _____.

ConfigMgr Alarms

UAS Logs/Faults available

26625	CM_CONFIG_ERROR; Critical. This alarm can be raised for various reasons during initialization. A serious configuration problem has been detected. The Audio Server is unable to initialize. A configuration file is probably in error. Look for an error log to determine the exact cause of the problem. The condition clears after the configuration problem is fixed. Possible reasons and corrective actions follow: The specified configuration template files are missing from c:\uas\cfg\templates. Restore the missing files. The specified configuration file is missing. Restore the missing file. ConfigMgr was unable to update the uas_pending.conf file. The file may have had incorrect permissions, or the disk is full. Check file permissions. Check to see if the disk is full. ConfigMgr attempted to create a kernel object but encountered an error. Contact the support group. ConfigMgr was unable to copy a file. The file may have had incorrect permissions, or the disk is full. Look at logs to determine which file caused the problem. Check file permissions. Check to see if the disk is full. ConfigMgr could not automatically determine how many AG cards there are in the system.he number of AG cards could not be determined. Ensure that the NMS blocate utility is present and is working properly. ConfigMgr could not update the uas.conf file with the number of AG cards. Check file permissions. Check to see if the disk is full. A configuration parameter is missing or has an invalid value. Look at logs to determine which configuration parameters are missing. ConfigMgr attempted to operate on a kernel object but encountered an error. Contact the support group.
CG6000 Service-level Alarms	
30721	CG_GENERIC_ALARM; Major. An attempt was made to load software onto the card and to start the card. The attempt failed. Stop the applications, reseat the card and then restart the applications. If the problem persists, contact the Nortel support group. Clears when the applications are restarted and the operation succeeds.
30722 (318)	CG_ETHERNET_CONN_ALARM Critical, CG6000 %d failed ethernet connection(s) on CG6000 card in slot %d.
30723 (319)	CG_SURPRISE_EXTRACTION Major, CG6000 Improper extraction of CG6000 card in slot %d.
30724 (320)	CG_CARD_DISABLED Major, CG6000 card in slot %d disabled until next application restart.
30725 (321)	CG_CLOCKING_ALARM Major, CG6000 primary clock source is %s and secondary clock source is %s in slot %d.

UAS Logs/Faults available

ATM Service Alarms--The ATM_MISSING_CARD alarm and ATM_MISMATCH_CARD alarm are raised in situations where provisioned VCs exist for a given ATM Card in a given slot, and that card has either been removed, is inoperable, or has been replaced with another ATM card.

34817	ATM_MISSING_CARD; Critical. Either the ATM card has been pulled or it has experienced a catastrophic failure and is unable to register with the cPCI chassis. A working ATM card must be inserted into the slot. Alternatively, all the VCs may be deleted which are associated with the missing card. Clears at the next start of the call processing application.
34818	ATM_MISMATCH_CARD; Critical. The ATM card has been replaced with a different model ATM card. Place the correct ATM card back in the slot which originally contained the S007 card. Alternatively, all the VCs may be deleted which are associated with the mismatched card. Clears at the next start of the call processing application.

ATM Port Alarms

34913	ATM_PORT_LOC; Critical. The fiber connecting the ATM port to the network has either been unplugged or damaged. Plug the fiber back in, or replace it if it was damaged. Clears when the signal on the fiber is back to normal.
34819 (328)	ATM_H110_FAILURE Critical ATM_Service The ATM card detected an H.110 bus failure. This alarm may be caused by a bad AG driving the H.110 bus clock or more then one card is trying to drive the clock on the bus. Clears at the next start of the call processing application.
34820 (329)	ATM_OUTDATED_FIRMWARE Major ATM_Service The ATM card in slot %d has outdated firmware ver.:%s recommended version:%s. Please run the ATMFirmware command to upgrade the firmware. This alarm is seen if the ATM card has outdated firmware. Clears at the next start of the call processing application, after the firmware has been upgraded.
34821 (330)	ATM_FIRMWARE_NON_UPGRADABLE Major ATM_Service The ATM card in slot %d has outdated firmware ver.:%s. This firmware needs to be manually updated. Please load the card with a firmware version which is 2.1.0 or later. This alarm is seen when the firmware on the ATM card is outdated and can not be automatically upgraded. A newer firmware load needs to be transfer to the card manually. Clears at the next start of the call processing application.
34822 (331)	ATM_HW_API_TOO_MANY_FAILURES Critical ATM_Service The number of consecutive API calls failures to the ATM card in slot %d, has exceeded the threshold of %d. The card is being taken out of service. Clears at the next start of the call processing application.

Carrier Alarms

40961	CARRIER_CLR_ALARM. Indicates that a carrier alarm cleared.
40962	CARRIER_RAISE_ALARM; Critical. One of these carrier alarms is raised: RAI, AIS, LOF, LOS, E1 LOMFS, or E1 16 AIS. Based on the different alarm types, check T1/E1 carrier for the cause. Clears when the CARRIER_CLR_ALARM event is received.

Activity Manager Alarms

53249 (336)	AM_COLD_START_NOT_SENT_CEM Activity_Manager.
53250 (337)	AM_COLD_START_NOT_SENT_SWACT Activity_Manager.

UAS Logs/Faults available

53251 (338)	AM_SWACT_FAILURE Critical Activity_Manager.
53252 (339)	AM_ERM_FAILURE Critical Activity_Manager.
53253 (340)	AM_ED_SOCK_FAILURE Major Activity_Manager.
53254 (341)	AM_CONFIG_ERROR_NOFILE Minor Activity_Manager.
53255 (342)	AM_DATAFILE_ERROR_NOFILE Critical Activity_Manager.
Power Supply, Disk, and Fan Maintenance Alarms	
61441 (345)	COOLING_SYSTEM_RAISE_ALARM; Major/Critical. In the case of a cooling fault, this is due to a high temperature at air intake to the chassis. In the case of a Cooling alarm, it is due to an extremely high temperature at air intake to the chassis. Check air flow and cooling equipment. Clears upon receipt of a GlobalServer Equipment fault tag with a 'cleared' alarm condition.
59393 (344)	POWER_SUPPLY_RAISE_ALARM; Major. HA Monitor received a Power Supply Fault Tag, and informed the PsFanMtc subsystem. This could be due to a faulty power supply system in the chassis that has gone down. Clears upon receipt of a Power Supply Fault tag with the "Power Good" bit set.
59393	POWER_SUPPLY_RAISE_ALARM; Major. HA Monitor received a Fan Fault Tag, and informed the PsFanMtc subsystem. This could be due to a faulty fan in the chassis that has gone down. Clears upon receipt of a Fan Fault tag with the "Fan Fault" bit unset.
63489 (346)	DISKDRIVE_RAISE_ALARM Critical Hard_Disk ALARM: Problem detected on Domain %s %s disk drive, chassis peripheral %d, due to %s.
I/O Card Base-level Alarms	
65537 (309)	CD_SURPRISE_SLOT_POWER_OFF; Major. A surprise power off on a slot can be caused by a chassis hardware problem or by a software error. The problem may clear up after a reboot. Stop the applications and perform a reboot. If the problem does not clear up, then you may be able to workaround the problem by moving the card to another slot. Refer to the appropriate card maintenance and configuration procedures. The alarm clears when power is restored to the slot.
65538 (310)	CD_SURPRISE_CARD_EXTRACTION; Major. A card was improperly extracted from the specified slot. The applications will need to be restarted. Perform these actions: 1) stop the applications 2) reinsert the card 3) restart the applications. The alarm clears when the card is reinserted and the applications are restarted.
65539 (311)	CD_LOAD_SCRIPT_FAILURE; Major. An attempt was made to load firmware onto the card in the specified slot. Stop the applications, reseat the card, and restart the applications. If the problem persists, then contact the Nortel support group. If reseating the card fixes the problem, then the alarm will clear when the applications are restarted.
65540 (312)	CD_SLOT_VERIFY_SCRIPT_FAILURE; Major. An attempt was made to verify that the card contains the correct firmware version. Stop the applications, reseat the card, and restart the applications. If the problem persists, then contact the Nortel support group. If reseating the card fixes the problem, then the alarm will clear when the applications are restarted.

UAS Logs/Faults available

65541 (313) CD_GENERIC_CARD_ALARM; Major. A problem occurred with the card in the specified slot. A brief description of the problem is supplied. No action required; no clear condition.

Shelf Controller Alarms

67585 (309) SC_SURPRISE_SLOT_POWER_OFF Major Shelf Controller Surprise power off on slot %d.

67586 (310) SC_SURPRISE_CARD_EXTRACTION Major Shelf Controller Surprise card extraction on.

67587 (311) SC_LOAD_SCRIPT_FAILURE Major Shelf Controller Firmware load script failure on card in slot %d.

67588 (312) SC_SLOT_VERIFY_SCRIPT_FAILURE Major Shelf Controller Verify script failure on card in slot %d.

67589 (313) SC_GENERIC_CARD_ALARM Major Shelf Controller Problem with card in slot %d:

Hot Swap Controller Alarms

69633 (309) HS_SURPRISE_SLOT_POWER_OFF Major Hot Swap Controller Surprise power off on slot %d.

69634 (310) HS_SURPRISE_CARD_EXTRACTION Major Hot Swap Controller Surprise card extraction on slot %d.

69635 (311) HS_LOAD_SCRIPT_FAILURE Major Hot Swap Controller Firmware load script failure on card in slot %d.

69636 (312) HS_SLOT_VERIFY_SCRIPT_FAILURE Major Hot Swap Controller Verify script failure on card in slot %d.

69637 (313) HS_GENERIC_CARD_ALARM Major Hot Swap Controller Problem with card in slot %d:

SCSI Controller Base-level Alarms

71681 (309) SS_SURPRISE_SLOT_POWER_OFF; Major. A surprise power off on a slot can be caused by a chassis hardware problem or by a software error. The problem may clear up after a reboot. Stop the applications and perform a reboot. If the problem does not clear up, then you may be able to workaround the problem by moving the card to another slot. Refer to the appropriate card maintenance and configuration procedures. The alarm clears when power is restored to the slot.

71682 (310) SS_SURPRISE_CARD_EXTRACTION; Major. A card was improperly extracted from the specified slot. The applications will need to be restarted. Perform these actions: 1) stop the applications 2) reinsert the card 3) restart the applications. The alarm clears when the card is reinserted and the applications are restarted.

71683 (311) SS_LOAD_SCRIPT_FAILURE Major SCSI_Controller Firmware load script failure on card in slot %d.

71684 (312) SS_SLOT_VERIFY_SCRIPT_FAILURE Major SCSI_Controller Verify script failure on card in slot %d.

71685 (313) SS_GENERIC_CARD_ALARM Major SCSI_Controller Problem with card in slot %d:

Chassis Even Manager Alarms

UAS Logs/Faults available

75783 (311)	SS_LOAD_SCRIPT_FAILURE Major SCSI_Controller Firmware load script failure on card in slot %d.
75784 (312)	SS_SLOT_VERIFY_SCRIPT_FAILURE Major SCSI_Controller Verify script failure on card in slot %d.
75785 (313)	SS_GENERIC_CARD_ALARM Major SCSI_Controller Problem with card in slot %d:
Local Resource Manager Alarms	
81921 (350)	LRM_CPU_C Critical, LocalResourceManager cpu_overload_critical, The CPU is overloaded, critical alarm.
81922 (351)	LRM_CPU_M Major, LocalResourceManager cpu_overload_major, The CPU is overloaded major alarm.
81923 (352)	LRM_MEM_C Critical, LocalResourceManager , mem_usage_high_critical, Memory usage is high.
81924 (353)	LRM_MEM_M Major, LocalResourceManager mem_usage_high_major, Memory usage is high
81925 (354)	LRM_DISK_C Critical, LocalResourceManager disk_usage_critical, Disk usage is high.
81926 (355)	LRM_DISK_M Major, LocalResourceManager disk_usage_major , Disk usage is high but less severe than critical where space is exhausted.
81927 (356)	LRM_CONFIG_FILE_ERR Minor, LocalResourceManager, lrm_config_fileerror
Program Manager Alarms	
83971 (357)	c_FAILED_MALLOC Critical ProgramManager.
83974 (358)	c_BAD_PARSE Critical ProgramManager.
83987 (359)	c_BAD_FORK Critical ProgramManager.
83989 (360)	c_BAD_EXEC Critical ProgramManager.
83998 (361)	c_CRIT_DEATH Critical ProgramManager.
83999 (362)	c_MAX_RETRIES Critical ProgramManager
84000 (363)	c_MAX_RETRIES_NO_RESTART Minor ProgramManager.
84009 (364)	c_FIFO_ERROR Critical ProgramManager.
84039 (365)	c_RSM_FAILED_CONNECT Critical ProgramManager.
Clock Manager Alarms	
90113 (367)	PRIMARY_CLOCK_DOWN_ALARM Minor ClockManager Primary Clock Driver trunk %d on board %d is down.
90114 (368)	SECONDARY_CLOCK_DOWN_ALARM Minor ClockManager Secondary Clock Driver trunk %d on board %d is down.
90115 (369)	BOTH_CLOCK_DOWN_ALARM Critical ClockManager System has lost all external clocking.

UAS Logs/Faults available

90116 (370)	PRIMARY_BOARD_CLOCK_DOWN_ALARM Minor ClockManager Board %d has lost its primary clock source.
90117 (371)	SECONDARY_BOARD_CLOCK_DOWN_ALARM Minor ClockManager Board %d has lost its secondary clock source.
90118 (372)	BOTH_BOARD_CLOCK_DOWN_ALARM Critical ClockManager Board %d has lost all external clocking.

Event Server Alarms

96257 (373)	LOCAL_SRVSOCK_CREATION_FAILED Critical EventServer [es_alrm_001] %s.
96258 (374)	REMOTE_SRVSOCK_CREATION_FAILED Major, EventServer [es_alarm_002] %s.
96259 (375)	SYSTEM_RESOURCE_ERR Critical, EventServer [es_alrm_003].
96260 (376)	CONFIG_ERR EventServer [es_alrm_004].
96261 (377)	HAMODE_CHECK_FAILED Critical, EventServer [es_alrm_005].
96262 (378)	MATE_EVTSVR_CONN_LOST Minor, EventServer [es_alarm_006].

UAS Logs

ATM logs	ASL001	General ATM log indicating an ATM interface card problem.
	ASL002	The ATM service has initialized successfully.
	ASL003	An ATM delete gateway request has failed.
	ASL004	An ATM delete gateway request has failed.
	ASL005	An ATM interface card port has failed to lock. The port has returned to its previous state.
	ASL006	An ATM interface card port has failed to lock. The port cannot return to its previous state.
	ASL007	An ATM Virtual Channel has experienced an AIS alarm.
	ASL008	An ATM Virtual Channel has experienced an RDI alarm.
	ASL009	An ATM Virtual Channel cleared the AIS alarm.
	ASL010	An ATM Virtual Channel cleared the RDI alarm.
	ASL013	The ATM port is configured with the wrong UNI version.
	ASL014	ILMI failure on the ATM port.
	ASL015	UNI failure on the ATM port.
	ASL016	ILMI is now ready on the ATM port.
	ASL017	UNI is now ready on the ATM port.
	ASL018	Invalid ATM SDP parameter received.
	ASL019	Invalid VCCI received in the incoming AAL2 SVC setup.
	ASL020	A specific ATM software error occurred as described in the log.

UAS Logs/Faults available

	ASL021	Failed to acquire a channel for the endpoint described in the log.
	ASL022	An error was reported by the NMS PA200 API.
	ASL023	ATM audit has started.
	ASL024	ATM audit has ended.
	ASL025	Audit has dropped a resource on the ATM board as described in the log.
	ASL026	Audit has established a resource on the board as described in the log.
	ASL027	Audit has found a missing resource on the board that can't be established. The resource is described in the log.
	APL001	The ATM interface port has initialized correctly.
UAS398	Indicates a raised alarm in a UAS device	
UAS399	Indicates a cleared alarm in a UAS device	

USP Logs/Faults

For detailed information on logs, refer to NN10275-909, *Fault Management Log Reference.*

USP faults are available to the OSS via a third-party fault probe or fault collector. The fault probe/collector must reside somewhere on the OAM&P VLAN due to security rules for accessing the network elements.

USP logs are available on the USP PC Client GUI.

USP supports SSV format. For details on this format, refer to the Performance section of the FCAPS documentation on USP, NN10137-711.

Operational measurements/performance measurements

Operating company personnel use operational measurements (OMs) and performance measurements (PMs) to obtain information on the performance and traffic load on a Succession Network. This data provides the information required for network planning and engineering.

OMs/PMs collection and delivery

There are two major OM/PM interfaces used in SN09:

- For CS2K Core OMs, SDM functionality uses either OM Data Delivery (OMDD) or EADAS. The OMs are grouped into user-defined report elements, formatted into CSV (comma-separated value) format, and delivered to a customer OSS (operations support system). The OMDD application delivers OMs only for the MG 4000, IW-SPM, DPT-SPM, SPM, and XA-Core. For more complete details on the CS2K Core OMs, refer to NN10264-709, *Carrier Voice over IP Performance Management: Operational Measurements Reference.*
- The following CS2K Network Elements use the Integrated Element Management System (IEMS) single performance interface to OSS in Common Performance Record Format (CSV or XML): GWC, Storm, ERS8600 (formerly Passport 8600), MS, USP (raw format), MSS15000, MG9000, MCS, MAS, Border Control Point (formerly RTP Media Portal).

The Integrated EMS provides a centralized location for collecting, storing and forwarding performance data in a CS 2000 central office. Its performance collection sub-system provides some basic tools for viewing and graphing the collected performance attributes. In addition, it does provide interfaces to configure the generation of threshold alarms for the collected Operation Measurement data. For detailed information on the IEMS performance management features please refer to the Integrated EMS Performance Management document (NN10327-711). You may also refer to chapter one of this document, *IEMS Functionality.*

Available OMs/ PMs

The OM/PM listings on the following pages are limited to the data accessible through OSS interfaces. These listings do not include those network elements that employ their own graphical user interfaces for delivery/viewing of OM/PM data.

CS 2000 Core OMs/PMs

The following table lists the operational measurements (OMs) and performance measurements (PMs) **that are new or changed since SN04** and

that are available from the Call Server 2000 Core network element. For a complete list of Core OMs/PMs available in Carrier Voice over IP, refer to NN10264-709, *Performance Management Operational Measurements Reference*.
CS 2000 Core supports CSV and EADAS formats through SDM functionality. For details on EADAS, refer to the Performance section of CS 2000 FCAPS documentation, NN10149-711.

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
Network Element: CS 2000 Core			
AINTRAN AIN Transports group--new in SN08			AIN
	INSCMSGO	Pegs Outgoing IN messages using SCTP	
	INSCMSGI	Pegs Incoming IN messages using SCTP	
	INSSNDFA	Pegs IN messages using SCTP for which send failed	
	INSCDERR	Pegs IN messages which encountered errors at application data	
	INSCTBIG	Pegs IN Messages which failed due to message length	
	INSCTBMS	Pegs instances when buffer errors encountered while sending IN messages over SCTP	
ATTAMA2 CAIN Triggers group (Applies only to DMS)--new in SN08 Used for register overflows from the OM group ATTAMA, only when the BAS00023 SOC is ON, and only for registers AMANS and AMUNANS.			CAIN
	QUERYSCU	Counts call attempts that are unsuccessful because switching equipment in another office handles too many calls.	
	ISCONUCC	Counts the number of times a CAIN call queries the SCU.	
AUDSRVS--provides one tuple for each Audio Server (AUD) node. These OMs appear in the Core only.			MG9K
	ANNCINSU	Announcement port in-service usage	
	ANNCOOSU	Announcement port out-of-service usage	
	ANNCTRU	Announcement port traffic usage	
	ANNCFTRU	Announcement port fast traffic usage	
	CNF3INSU	3-port conference circuit in-service usage	
	CNF3OOSU	3-port conference circuit out-of-service usage	
	CNF3TRU	3-port conference circuit traffic usage	
	CNF3FTRU	3-port conference circuit fast traffic usage	
	CNF6INSU	6-port conference circuit in-service usage	
	CNF6OOSU	6-port conference circuit out-of-service usage	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	CNF6TRU	6-port conference circuit traffic usage	
	CNF6FTRU	6-port conference circuit fast traffic usage	
CAINTRIG CAIN Triggers group			CAIN
	QUERYSCU	Counts call attempts that are unsuccessful because switching equipment in another office handles too many calls.	
	ISCONUCC	Counts the number of times a CAIN call queries the SCU.	
CICM QoS Statistics: The following QoS statistics are reported by the CICM at the end of each call:			
	Jitter Average	Average variation in packet arrival times due to transmission (routing, queuing delay, etc…) through the network.	
	Jitter High Water Mark	Max variation in packet arrival times due to transmission (routing, queuing delay, etc…) through the network.	
	Far End Originated Loss	Far end orginated loss	
	Round Trip Average	Average RTCP packets round trip time.	
	Round Trip High Water Mark	Max RTCP packets round trip time.	
	Local Silence Suppression	Indicates if silence suppression was used.	
	Local Rx and Tx Codec Type	Codec Type	
	Local Rx and Tx Packetization Rate	Frame duration in milliseconds**.**	
	End System Delay	Most recently specified/calculated end system delay in milliseconds.	
	Average One Way Delay	Average one-way delay in milliseconds.	
	Maximum One Way Delay	Maximum one-way delay in milliseconds.	
	Average Noise Level	Ratio of the silent period background noise level to overflow signal power, expressed in decibels.	
	Average Signal Power	Ratio of the signal level to overflow signal level, expressed in decibels	

OM Group or PM name	Registers	Description	Applicability
	Echo Return Loss	Sum of the measured echo return loss (ERL) and the echo return loss enhancement (ERLE) expressed in dB	
	Listening R factor	Direct measure of the call quality or transmission quality, and incorporate the effects of CODEC type, packet loss, discard, burstiness, delay etc.;	
	Conversational R factor	Segment of the call that is carried over a network segment, external to the RTP segment	
	Listening Quality MOS	Estimated mean opinion score for listening quality.	
	Conversational Quality MOS	Estimated mean opinion score for conversational quality.	
	Burst R factor	R factor during a burst period; a burst is defined as a longest sequence of packets bounded by lost or discarded packets.	
	Average Burst Density	Average percentage of MIU's lost or discarded during burst periods.	
	Burst count	Number of bursts that have occurred on the call	
	Average Burst Length in MS	Average length of all burst periods in milliseconds that have occurred on the call	
	Gap R factor	R factor during a gap period; a gap is defined as the period of time between two bursts.	
	Average Gap Density	Average MIU'S lost or discarded within gap periods.	
	Average Gap Length in MS	Average length in milliseconds of all gaps that have occurred on the call.	
	Average Loss Rate	Total average percentage of MIUs lost and/or discarded.	
	Average Network Loss Rate	Total average percentage of MIUs lost in the network.	
	Average Discard Rate	total average percentage of MIU's discarded.	
	MIU Duration	Duration of each MIU, in milliseconds.	
	MIU per packet	Total number of MIU's in each RTP packet.	
	MIU Loss percentage	Percentage of MIUs handled by the call channel that were lost in the network.	
	MIU Discard percentage	Percentage of MIUs handled by the call channel that were discarded by the endpoint.	
	MIU Out of order percentage	Percentage of MIUs handled by the call channel that is discarded by the endpoint.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	MIU Duplicate percentage	Percentage of MIUs handled by the call channel that is discarded by the endpoint.	
	Number of RTP packets rx/tx	Number of RTP packets received and transmitted.	
	Number of RTP packets out of order	Number of RTP packets received out of order.	
	Octets rx/tx	Octets sent and received.	
CMR FM OMs: The following OMs are maintained by the CMR FM application:			
	ADSI	No usage metering; no peg counts.	
	BCLID	No usage metering; no peg counts.	
	CID	Counts CID attempts and CID completions.	
	CMWI	No usage metering; no peg counts.	
	DSCWID	Counts DSCWID attempts.	
	SCWID	Counts SCWID attempts.	
CP Call Processing Software Resources group			CS2K Core
	CPLOSZ	Counts origination messages correctly attached to a call condenxe block.	
	CINITC	Counts call condense blocks that were in use at the time of a cold restart.	
	WAKESZ	Counts CPWAKEUP block seiz.ures.	
DPLOM OM group DPLOM has 13 registers for pegs and usage measurements of the VID resource pool.			CS2K Core
	DPLUSE	Usage register (100 sec sampling, with extension register) that tracks the number of VIDs in use by call processing.	
	DPLUSE2	Extension register for DPLUSE.	
	DPLFRE	Usage register (100 sec sampling, with extension register) that tracks the number of VIDs on the resource pool free list.	
	DPLFRE2	Extension register for DPLFRE.	
	DPLNOA	Peg register (with extension) that indicates the number of allocations from the resource pool.	
	DPLNOA2	Extension register for DPLNOA.	
	DPLNOD	Peg register (with extension) that indicates the number of deallocations to the resource pool.	
	DPLNOD2	Extension register for DPLNOD.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	DPLFNVA	Peg register that indicates the number of times that a failure to allocate a VID happened because the resource pool free list was empty.	
	DPLFBAL	Peg register that indicates the number of times that a failure to allocate a VID happened because the resource pool free list was unavailable due to rebalancing (part of the rebuild process).	
	DPLFREB	Peg register that indicates the number of times that a failure to deallocate a VID happened (resulting in a "lost" VID) because the resource pool free list was being rebuilt.	
	DPLRLOS	Peg register that indicates the number of "lost" VIDs that were recovered.	
	DPLRCAL	Peg register that indicates the number of VIDs that were in use by call processing, but were not returned to the resource pool free list.	
DPTNODE Dynamic packet trunk node type (SPM or DPT), PM #, and node # SN07 adds the following: If the DPT Node is a GWC, then the associated DPT protocol (i.e., BICC or SIP-T) is added to the information. If the DPT Node is an SPM (i.e., either MG4K or DTP SPM), then the associated bearer network, DPT protocol and SPM node type is added to the information.			DPT-SPM
	DPTGTAT	The number of attempts to get a DPT Terminal for a particular DPT node, pegged every time an attempt to get a DPT terminal is made within a given transfer period. For a typical SIPT call the number of pegs is in the range of 1 peg per DPT agent per call. For a typical BICC call the number of pegs is in the range of 1 to 3 pegs per DPT agent per call.	
	DPTGTAT2	Extension of DPTGTAT	
	DPTGTFL	The number of attempts to get a DPT Terminal that failed (non-optimized) for a particular DPT node, pegged every time an attempt to get a *non-optimized* DPT terminal fails within a given transfer period.	
	DPTUSAG	The number of DPT Terminals in use for a particular DPT node, pegged every one-hundred seconds within a given transfer period.	
	DPTUSAG2	Extension of DPTUSAG	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	DPTGTFLO	The number of attempts to get a DPT Terminal that failed (optimized) for a particular DPT node, pegged every time an attempt to get an *optimized* DPT terminal fails within a given transfer period. Optimized failure attempts on nodes "not DPT-enabled" are not pegged against this register. Pegs to this register do not signify call failures. The optimized failure attempt to get an optimized terminal is immediately followed by an attempt to get a non-optimized terminal instead.	
	DPTHWT	The high water mark for number of DPT Terminals in use for a particular DPT node, pegged every ten seconds within a given transfer period.	
DPTOFC Dynamic packet trunk office events			DPT-SPM
	DPGTAT	The number of attempts to get a DPT Terminal, pegged every time an attempt to get a DPT terminal is made within a given transfer period. For a typical SIPT call the number of pegs is in the range of 1 peg per DPT agent per call. For a typical BICC call the number of pegs is in the range of 1 to 3 pegs per DPT agent per call.	
	DPGTAT2	Extension register of DPGTAT incremented when DPGTAT reaches 65,535	
	DPGTFL	The number of attempts to get a DPT Terminal that failed (non-optimized), pegged every time an attempt to get a *non-optimized* DPT terminal fails within a given transfer period.	
	DPGTFL2	Extension register of DPGTFL incremented when DPGTFL reaches 65,535	
	DPUSAG	The number of DPT Terminals in use, pegged every one-hundred seconds within a given transfer period. Since this register is an accumulator and is added to itself the register can be misleading. To interpret the usage register, divide the value by the number of slow samples to determine the average usage for a given transfer period.	
	DPUSAG2	Extension register of DPUSAG incremented when DPUSAG reaches 65,535	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	DPGTFLO	The number of attempts to get a DPT Terminal that failed (optimized), pegged every time an attempt to get an *optimized* DPT terminal fails within a given transfer period. Optimized failure attempts on nodes "not DPT-enabled" are not pegged against this register. Pegs to this register do not signify call failures. The optimized failure attempt to get an optimized terminal is immediately followed by an attempt to get a non-optimized terminal instead.	
	DPGTFLO2	Extension register of DPGTFLO incremented when DPGTFLO reaches 65,535	
	DPHWT	The high water mark for number of DPT Terminals in use, pegged every ten seconds within a given transfer period.	
	DPHWT2	Extension register of DPHWT incremented when DPHWT reaches 65,535	
	DPDPL	Number of attempts to get a DPT terminal that failed due to port depletion, pegged every time an attempt to get a DPT terminal fails due to port depletion within a given transfer period.	
	DPDPL2	Extension register of DPDPL incremented when DPDPL reaches 65,535	
DPTOFCP DPT Office Protocol group--new in SN07 This OM group measures the performance of the supported dynamic packet trunk protocols for the office. The two supported protocols are BICC and SIP-T. The addition of this new DPTOFCP OM group is controlled by the value of a new SN07 office parameter, MULTINET_DISPLAY_ACTIVE. If this parameter is set to 'Y', then the new DPTOFCP OM group is displayed.			DPT-SPM
DTSRPM Pegs originations and dialtone delays grouped by the type of line making the call (DP, DTMF, or Pphone).			GWC
	DPLTOT	Dial Pulse Lines Total Originations. This value is always 0 for CS2K lines since no differentiation is made between DP and DGT.	
	DPLDLY	Dial Pulse Line Delays. Counts DP lines which got dial tone after 3 seconds. Always 0 for CS2K.	
	DGTTOT	Counts Digit Tone Line Total Originations.	
	DGTDLY	Digit Tone Line Delays. Counts DGT lines which got dial tone after 3 seconds.	
	KSTOT	Keyset (Pphone) Lines Total Originations.	
	KSDLY	Keyset (Pphone) Lines which got dial tone after 3 seconds.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
ENETPLNK ENET Peripheral Side Links group. The registers listed here are the only ones supported for SPM and MG4K applications.			DPT-SPM
	ENSPCHER	NOTE: This is an existing OM group. For details on the	
	ENLKERR	registers, see NTP 297-2621-814, available on Helmsman	
	ENLKFLT	Express.	
	ENSBLKU		
	ENMBLKU		
	ENLKPARU		
	ENSLKPAR		
	ENMLKPAR		
	ENLNKISOU		
	ENSLKISO		
	ENMLKISO		
ETHERNET OM group			CS2K Core
	Alignment Errors	The counter associated with AlignErr Collection Interval.	
	FCS Errors	The counter associated with FcsErr Collection Interval.	
	Internal MAC Receive Errors	The counter associated with Internalmacrxerr.	
	Frame Too Long	The counter associated with Frtoolongs.	
	Internal MAC TX Errors	The counter associated with Internalmactxerr.	
	Symbol Errors	The counter associated with Symbolerr.	
	Inpause Frames	The counter associated with Inpausefr.	
	Outpause Frames	The counter associated with Outpausefr.	
FCDRTM1E (Applies only to DMS) Used for register overflows from the OM group FCDRTMP1, only when the UBFR0008 SOC is ON. This OM group provides 32 pre-defined tuples. Each register is associated with the CDR template being used for a CDR billing record. The CDR template index corresponds to the register number. This OM group supports indexes 0-31.			CS2K Core

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
FCDRTM2E (Applies only to DMS) Used for register overflows from the OM group FCDRTMP2, only when the UBFR0008 SOC is ON. This OM group provides 32 pre-defined tuples. Each register is associated with the CDR template being used for a CDR billing record. The CDR template index corresponds to the register number. This OM group supports indexes 32-63.			CS2K Core
FCDRALG2 (Applies only to DMS) Used for register overflows from the OM group FCDRALGR, only when the UBFR0008 SOC is ON. For these extension registers one count here is equal to 65535 counts of the same register in FCDRALGR. .			CS2K Core
IOCAP IO Capacity for messaging over HIOP and HCMIC group			CS2K Core
	IO_SERVICE_TYPE	Indicates the service provided.	
	IOUTIL	Refers to percentage utilization of the services on the switch.	
	IOHWM	Refers to the highest level that the corresponding utilization has reached in the sample period.	
	TxMSG/S, TxSIZE, RxMSG/S, RxSIZE	Report the average transmit and receive message rates and sizes through the service.	
	IOTHRESH	Pegged every time the service average utilization for one minute exceeds the value of OFCENG office parameter IO_WARNING_THRESHOLD.	
ISUPCONN ISUP Connection group			CS2K Core
	ISCONUCC	Added to count call attempts that are unsuccessful because there are no available idle circuits in another office to handle the call.	
	ISCONUCE	Added to count call attempts that are unsuccessful because switching equipment in another office handles too many calls.	
	ISCONUCF	Added to count call attempts that are unsuccessful because of a temporary fault in the far-end network.	
IWBM Interworking bridge manager events (associated with IW SPMs)			IW-SPM
	IWGBATT	Get bridge attempts	
	IWGBATT2	Extension of IWGBATT	
	IWGBFAIL	Get bridge attempt failures	
	IWGGBABRT	Get bridge attempts aborted	
	IWFBATT	Free bridge attempts	
	IWFBATT2	Extension of IWFBATT	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	IWFBFAIL	Free bridge attempt failures	
	IWFBABRT	Free bridge attempts aborted	
	IWONSET1	Total IW SPMs in use reached 70%	
	IWONSET2	Total IW SPMs in use reached 90%	
	IWABATE1	Total IW SPMs in use less than 65%	
	IWABATE2	Total IW SPMs in use less than 85%	
MNGEMLNK Multiservice Node Gigabit Ethernet Module Link Bandwidth Engineering provides Gigabit Ethernet Link usage statistics to assist with network bandwidth Engineering.			IW-SPM
	TXOCT	Provides count for total number of bytes transmitted on a Gigabit Ethernet Link connected to a particular MG4K-IP/IW-IP node.	
	TXOCT2	Extension of TXOCT.	
	RXOCT	Provides count for total number of bytes received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	RXOCT2	Extension of RXOCT.	
	TXPKT	Provides count for total number of packets transmitted on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	TXPKT2	Extension of TXPKT.	
	RXPKT	Provides count for total number of packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	RXPKT2	Extension of RXPKT.	
	TXEROCT	Provides count for total number of bytes transmitted in errored packets on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	TXEROCT2	Extension of TXEROCT.	
	RXEROCT	Provides count for total number of bytes received in errored packets on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	RXEROCT2	Extension of RXEROCT.	
	TXERPKT	Provides count for total number of errored packets transmitted on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	RXERPKT	Provides count for total number of errored packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	CRCERPKT	Provides count for total number of packets received with Cyclic Redundancy Check (CRC) errors on a GigElink connected to a particular MG4K-IP/IW-IP node.	
	UNDERPKT	Provides count for total number of undersize packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	OVERPKT	Provides count for total number of oversize packets received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	SHORTPKT	Provides count for total number of short packets (aka fragments) received, on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
	LONGPKT	Provides count for total number of long packets (aka jabber) received on a GigE Link connected to a particular MG4K-IP/IW-IP node.	
MNGEMTRF	Multiservice Node Gigabit Ethernet Module Traffic Engineering provides statistics of Nodal traffic usage		IW-SPM
	TOTCONN	Provides count for total number connections handled by a particular MG4K-IP/IW-IP node.	
	TXRTPOCT	Provides count for total number of RTP bytes transmitted from a MG4K-IP/IW-IP node. Register TXRTPOC2 is an extension register for TXRTPOCT.	
	TXRTPOCT2	Extension of TXRTPOCT.	
	RXRTPOCT	Provides count for total number of RTP bytes received for a MG4K-IP/IW-IP node.	
	RXRTPOCT2	Extension of RXRTPOCT.	
	G711MUCN	Provides count for total number of G.711 MuLaw codec connections handled by a particular MG4K-IP/IW-IP node.	
	G711ACN	Provides count for total number of G.711 A-Law codec connections handled by a particular MG4K-IP/IW-IP node.	
	TXG711PK	Provides count for total number of RTP packets transmitted for G.711 connections handled by a particular MG4K-IP/IW-IP node.	
	TXG711PK2	Extension of TXG711PK.	
	RXG711PK	Provides count for total number of RTP packets received for G.711 connections handled by a particular MG4K-IP/IW-IP node.	
	RXG711PK	Extension of RXG711PK.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	G729CN	Provides count for total number of G.729 connections handled by a particular MG4K-IP/IW-IP node.	
	TXG729PK	Provides count for total number of RTP packets transmitted for G.729 connections handled by a particular MG4K-IP/IW-IP node.	
	TXG729PK	Extension of TXG729PK	
	RXG729PK	Provides count for total number of RTP packets received for G.729 connections handled by a particular MG4K-IP/IW-IP node.	
	RXG729PK	Extension of RXG729PK	
	CCDCN	Provides count for total number of 64K Clear Channel Data (CCD) Connections handled by a particular MG4K-IP/IW-IP node.	
	TXCCDPK	Provides count for total number of RTP packets transmitted for Clear Channel Data connections handled by a particular MG4K-IP/IW-IP node.	
	RXCCDPK	Provides count for total number of RTP packets received for Clear Channel Data connections handled by a particular MG4K-IP/IW-IP node.	
	VBDCN	Provides count for total number of Voice Band Data (VBD) Connections handled by a particular MG4K-IP/IW-IP node.	
	TXVBDPK	Provides count for total number of packets transmitted for Voice Band Data connections handled by a particular MG4K-IP/IW-IP node.	
	RXVBDPK	Provides count for total number of packets received for Voice Band Data connections handled by a particular MG4K-IP/IW-IP node.	
	T38CN	Provides count for total number of T.38 connections handled by a particular MG4K-IP/IW-IP node.	
	TXT38PK	Provides count for total number of packets transmitted for T.38 connections handled by a particular MG4K-IP/IW-IP node.	
	RXT38PK	Provides count for total number of packets received for T.38 connections handled by a particular MG4K-IP/IW-IP node.	
	RF2833CN	Provides count for total number of RFC2833 connections handled by a particular MG4K-IP/IW-IP node.	
	SLSUPCN	Provides count for total number of Silence Suppression connections handled by a particular MG4K-IP/IW-IP node.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
NCAS_LINK	Non-call Associated Signaling (NCAS) Link OM group		NGSS
	NUM_LINK_UP	Number of times the NCAS Link is brought up.	
	NUM_LINK_DOWN	Number of times the link goes down.	
	NUM_MSG_SENT	Number of messages sent over the NCAS Link.	
	NUM_MSG_RCVD	Number of times a response is received over the NCAS Link	
	NUM_MSG_SEND_FAIL	Number of times the message send fails	
	NUM_MSG_RCV_FAIL	Number of times the message receive fails.	
NGSSOM	Next Generation Session Server OM group		NGSS
	CS2ASOVF	Pegged when a CS2AS NGSS call is deflected because allowing the call would have caused the current CS2AS call count to exceed the SOC limit.	
	CS2ASHWM	Keeps track of the maximum value reached for the CS2AS call counter.	
	CS2CSOVF	Pegged when a CS2CS NGSS call is deflected because allowing the call would have caused the current CS2CS call count to exceed the SOC limit.	
	CS2CSHWM	Keeps track of the maximum value reached for the CS2CS call counter.	
NMSNCAS	Network Message Waiting (NMS) Non-call Associated Signaling (NCAS) OM group		NGSS
	SCTPNMSS	NMS TCAP messages sent successfully over SCTP	
	SCTPNMSR	NMS TCAP messages received successfully over SCTP	
	SCTPREJS	NMS REJ messages sent successfully over SCTP	
	SCTPREJR	NMS REJ messages receievd successfully over SCTP	
NMTCUNIT	Node Maintenance Unit Measurements group. The registers listed here are the only ones supported for SPM and MG4K applications.		DPT-SPM
	NDUERR	NOTE: This is an existing OM group. For details on the	
	NDUFLT	registers, see NTP 297-2621-814, available on Helmsman	
	NDUMBP	Express.	
	NDUMBU		

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	NDUMCRST		
	NDUMRRST		
	NDUNAP		
	NDUSBP		
	NDUSBU		
	NDUNAU		
	NDUSWERR		
	NDUTRAP		
NWMFRRCT Network Management Flexivle Reroute group			CS2K Core
	FRRATTCT	Counts calls that are rerouted to a Virtual Interworking Agent (VIA) route list. Required for ACC (Automatic Congestion Control).	
	FRRFLCT	Counts rerouted calls that fail to find an idle VIA route list. Required for ACC (automatic congestion control).	
PCEM Performance Measurements			CS2K Core
	EMSENT	Event message successfully generated.	
	EMFAIL	Failed to build event message.	
	EMSYSFL	System unable to send event message.	
	EMSENT2	Overflow register for EMSENT	
	EMFAIL2	Overflow register for EMFAIL	
	EMSYSFL2	Overflow register for EMSYSFL	
PKTMA Packet Media Anchor group			GWC
	PMAREQST	A peg register to indicate the number of anchored call attempts..	
	PMAFLNR	A peg register to indicate the number of failed anchored call attempts due to the unavailability of resources.	
	PMAHWM	A high water mark register to indicate the maximum number of simultaneous anchored calls.	
PM Peripheral Module group. The registers listed here are the only ones supported for SPM and MG4K applications.			DPT-SPM
	PMERR	NOTE: This is an existing OM group. For details on the	
	PMFLT	registers, see NTP 297-2621-814, available on Helmsman	
	PMMSBU	Express.	
	PMUMBU		
	PMSBP		

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	PMMBP		
	PMMWXFR		
	PMMCXFR		
	PMINTEG		
PMTYP Peripheral Module Type group. The registers listed here are the only ones supported for SPM and MG4K applications.			DPT-SPM
	PMTERR	NOTE: This is an existing OM group. For details on the registers, see NTP 297-2621-814, available on Helmsman Express.	
	PMTFLT		
	PMTMSBU		
	PMTUSBU		
	PMTMMBU		
	PMTSBP		
	PMTMBP		
	PMTMWXFR		
	PMTMCXFR		
	PMTINTEG		
SCMP	SCMPTRF	If an SCMP line is found Callp busy, the SCMPTRF register will be pegged for that line.	Line Provisioning
	SCMPMNT	If an SCMP line is found maintenance busy or unavailable, the SCMPTRF register will be pegged for that line.	
SIPGW_OVERLOAD OM group SIPGW_OVERLOAD is added to the Session Server to provide statistics related to the resources that are monitored to determine whether the SIP Gateway application is in overload.			
	CPU_OCCUPANCY	The value calculated for the amount of time the CPU spent performing work as a percentage to its total running time over the last sampling period (10 seconds)	
	CPU_OCCUPANCY_HWM	The maximum value calculated for the amount of time the CPU spent performing work as a percentage to its total running time over a 30 minute period. Reset to 0 every 30 minutes.	
	GCP_QUEUE_SIZE	The size of the GCP queue at the time the last sample was collected.	
	GCP_QUEUE_SIZE_HWM	The maximum sampled size of the GCP queue over a 30 minute period. Reset to 0 every 30 minutes.	
	SIP_QUEUE_SIZE	The size of the SIP queue at the time the last sample was collected.	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	SIP_QUEUE_SIZE_HWM	The maximum sampled size of the SIP queue over a 30 minute period. Reset to 0 every 30 minutes.	
SMSTOPS. This OM group records application-level events for the TOPS short message service.			TOPS
	SMSSENT, SMSSENT2	SMS sent	
	SMSSUCC, SMSSUCC2	SMS success	
	SMSFAIL, SMSFAIL2	SMS failure	
	SMSTIME, SMSTIME2	SMS time-out	
	SMSNETWK	SMS failure due to network problems	
	SMSTERM	SMS failure due to terminal (cell phone) problems	
	SMSRADIO	SMS failure due to radio interface problems	
	SMSMISC	Miscellaneous SMS failure	
SPMOVLD Specturm Overload Statistics group			SPM
	The new SPMOVLD group will have 18 OMs that give metrics on the SPM flow control system and the system overload control component. All OMs that apply to the system overload control component start with an ‘S’, all others apply to the flow control system. The actual peg counts and usage counts (accurate to one second) are accumulated on the peripheral and then uploaded to the OM group using the Spectrum OM Transfer System (SOTS).		
TC7WRLSS. This OM group records transport-level events such as types of TCAP messages sent and received, SS7 errors, etc. on TOPS wireless calls (SMS and WIN, as well as IS-41 and GSM).			TOPS
	INVOKES, INVOKES2	TCAP INVOKE sent	
	INVOKER, INVOKER2	TCAP INVOKE receives	
	RETRESS, RETRESS2	TCAP RETURN RESULT sent	
	RETRESR, RETRESR2	TCAP RETURN RESULT received	
	RETERRS	TCAP RETURN ERROR sent	
	RETERRR	TCAP RETURN ERROR received	
	REJECTS	TCAP REJECT sent	
	REJECTR	TCAP REJECT received	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	ABORTS	TCAP ABORT sent	
	ABORTR	TCAP ABORT received	
	NOTRIDS	No transaction identifiers	
	MBFULL	Incoming message from MSC ignored due to heavy traffic	
	RTFNOXLA	SCCP routing failure: No translation of such nature	
	RTFNOXLS	SCCP routing failure: No translation for this specific address	
	RTFSUBCG	SCCP routing failure: Subsystem congestion	
	RTFSUBFL	SCCP routing failure: Subsystem failure	
	RTFUNEQ	SCCP routing failure: Unequipped user	
	RTFNETFL	SCCP routing failure: Network failure	
	RTFNETCG	SCCP routing failure: Network congestion	
	RTFMISCE	SCCP routing failure: Failure other than the above seven	
	GTTFAIL	Global Title Translation failure	
TDGTHRU. TOPS Datagram Throughput. This OM group counts the number of UDP messages sent and received in each of several “buckets” or message size ranges. Each register in this group counts the number of messages in a specific size range that were sent by or received by a particular TOPS application, using a particular Ethernet interface. The group consists of 14 registers and 14 extension registers, counting message sizes ranging from <= 48 bytes up to > 368 bytes.			TOPS
TONES			CS2K Core
	TONEATT	Counts calls that the system routes to each tone generator.	
TRKQOS records instances in which QOS threshold values have been exceeded for calls handled by a particular GWC-based TDM trunk group.			GWC
	PKTLOSS	Packet Loss. Counts the number of times that the packet loss threshold has been exceeded.	
	JITTER	Jitter. Counts the number of times that the jitter threshold has been exceeded.	
	DELAY	Delay (latency). Counts the number of times that the delay threshold has been exceeded.	
N/A	Existing	As noted in the design document for 89007781 (PT-IP), the following data is reported by all gateways: packets sent; packets received; packet loss; octets sent; octets received; inter-arrival latency; jitter.	GWC

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
(Checking)		The OMs that feature 89008294 (UA-IP) will use already exist for the ATM solution, now extended to IP solutions. It includes the following OM counters: • Intra total number of channel allocation requests • Intra total number of failed channel allocation requests • Intra total number of failed channel allocation requests • Inter maxium simultaneous number of channels in use • Inter total number of channel allocation requests • Inter total number of failed channel allocation requests • Intra total number of channel allocation requests • Intra total number of failed channel allocation requests	GWC
TRNK2 OM group to hold extension registers from TRK OM group			CS2K Core
	TOTU2	Extension register of TOTU in TRK OM group	
	INCATOT2	Extension register of INCATOT in TRK OM group	
	TOTU2	Extension register of TOTU in TRK OM group	
	INCATOT2	Extension register of INCATOT in TRK OM group	
	NATTMPT2	Extension register of NATTMPT in TRK OM group	
	DEFLDCA	Extension register of DEFLD in TRK OM group	
	TRU2	Extension register of TRU in TRK OM group	
	SBU2	Extension register of SBU in TRK OM group	
	CONNECT2	Extension register of CONNECT in TRK OM group	
	TANDEM2	Extension register of TANDEM in TRK OM group	
	ANSWER2	Extension register of ANSWER in TRK OM group	
	NPQUERY2	Extension register of NPQUERY in TRK OM group	
	NPRESP2	Extension register of NPRESP in TRK OM group	
UTR Universal Tone Receiver group			UAS
	UTRSZRS	Counts each time that the system supplies a UTR to a call in response to a request.	
WINTOPS. This OM group records application-level events for wireless ADACC with release. This group uses WIN in the name since wireless intelligent network capabilities are used to provide ADACC with release for both IS-41 and GSM.			TOPS

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	WINBEGIN, WINBEGI2	IS-41 AnalyzedInformation or GSM InitialDP received.	
	REQCONN, REQCONN2	IS-41 ConnectResource or GSM EstablishTemporaryConnection sent	
	CONNECT, CONNECT2	IS-41 AnalyzedInformation or GSM Connect sent	
	DISCONN, DISCONN2	IS-41 AnalyzedInformation with action code of “disconnect call” or GSM DisconnectTemporaryConnection sent. This event is not part of the normal IS-41 call flow, but it is part of the normal GSM call flow. If this is pegged for IS-41, it means ADACC with release was not provided.	
	WINEND, WINEND2	GSM Application End received; no equivalent IS-41 message.	
	ERRCONN	MSC could not connect to TOPS using TLDN	
	ERRDISC	TOPS disconnected unexpectedly while providing operator assistance. IS-41 only; when this occurs in a GSM call, WINEND is pegged but not DISCONN or CONNECT.	
	ERRSSFT	MSC’s service switching function timer expired. Should not happen if TOPS Reset TImer is datafilled properly in Table ISUPTRK.	
	ABANDON	Wireless caller disconnected prior to receiving ADACC with release.	
	RESTIMR, RESTIMR2	ResetTimer sent (IS-41 and GSM)	
	NOTLDNS	No TLDNs available in Table TOPSTLDN.	
	NODATA	TOPS could not find EXT block associated with incoming TLDN call from MSC.	
	RXLAFAIL	TOPS call could not obtain original called digits and defaulted to 411.	
	SANTIMR	MSC did not release trunk to TOPS, or MSC did not send Application End.	
	TLDNTIME	A TLDN was allocated for an MSC call which never arrived. The TLDN is allocated to a new call.	
XACORE XA-Core hardware-related OMs			CS2K Core
	XAPE	PE (processor element) faults	
	XARXPE	Routine exercise test (RXe) PE failures	
	XASM	Critical shared memory (SM) faults	
	XARXSM	Routine exercise test (RXe) SM failures	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	XAIOP	Critical IOP (input/output processor) faults	
	XARXIO	Routine exercise test (RXe) IOP failures	
	XADISK	Disk faults	
	XATAPE	Critical tape faults	
	XARTIF	RTIF (reset terminal interface) packlet faults	
	XALOCP	Critical faults on a RTIF local port	
	XAREMP	Critical faults on a RTIF remote port	
	XACMIC	CMIC packlet faults	
	XACXABRT	Routine exercise (REx) test aborts	
	XARXBASE	Routine exercise test on base hardware failures	
	XARXFULL	Routine exercise test on all hardware failures	
	XARXALL	Routine exercise test on all hardware failures	
	XAMDI	Number of critical AMDI packlet faults detected	
	XAMDILNK	Number of critical AMDI link faults detected	
	XETHR	Hardware faults on Ethernet packlet	
	XETHRPRT	Hardware faults on an Ethernet port	
	XETHRLNK	Hardware faults on an Ethernet link	
XACSRVC	XA-Core service-related OMs		CS2K Core
	XAMDMAJU	Length of time (in 100 second increments) that an AMDI major alarm condition has existed	
	XAMDCRIU	Length of time (in 100 second increments) that an AMDI critical alarm condition has existed	
	XASSMPXU	Length of time (in 100 second increments) that a simplex SM condition has existed as a result of a system action	
	XAMSMPXU	Length of time (in 100 second increments) that a simplex SM condition has existed as a result of a manual action	
	XARXMPXU	Length of time (in 100 second increments) that a SM condition has existed as the result of a REx test	
	XASMCRIU	Length of time (in 100 second increments) that a low SM critical alarm has existed	
	XALKMAJU	Length of time (in 100 second increments) that an MScomm (message switch communication) major alarm has existed	
	XETHRMJU	Major alarms on an Ethernet RM	
	XETHRCRU	Minor alarms on an Ethernet RM	
	XATRAP	Trap interrupts	
	XASWINI	Warm restarts as a result of a system action	

CS 2000 Core OMs/PMs

OM Group or PM name	Registers	Description	Applicability
	XAMWINI	Warm restarts as a result of a manual action	
	XASCINI	Cold restarts as a result of a system action	
	XAMCINI	Cold restarts as a result of a manual action	
	XAPEMAJU	XACORE period of major alarm	
	XAPECRIU	XACORE period of low processing power	
XPMOVLD Collects statistics on XPM overload conditions. This is an existing OM group that functions the same as in TDM switches.			GWC
XPMOCC Collects statistics on CPU occupancy ini the GWC. This is an existing OM group that functions the same as in TDM switches.			GWC

Performance Measurements

The following section describes performance measurements collected and reported by the Integrated EMS for the various network elements. Pre-IEMS Performance interfaces for Network Elements, if integrated by the customer in SN07, are still supported in SN09, but are subject to the MD process that will be published for all FCAPS interfaces.

Audio codes Media Servers (AMS) Performance Measurements

Performance Measurements for the AudioCodes media servers are available through the Integrated EMS, and also through an SNMP interface. The media server will provide performance measurements in the form of two types:

- **Gauges:** Gauges represent the current state of activities on the media server. Gauges unlike counters can decrease in value and like counters, can increase. The value of a gauge is the current value or a snapshot of the current activity on the media server at that moment.
- **Counters:** Counters always increase in value and are cumulative. Counters, unlike gauges, never decrease in value unless the server is reset and then the counters are zeroed.

The media server performance measurements will be provided by two AudioCodes MIBs (acPerfMediaGateway and acPerfMediaServices). The first mib is generic-type of PM mib. The second PM mib is media server specific.

The generic PM mib covers the control protocol, the RTP stream, and the system packets statistics. This AC PM enterprise mibs supports statistics which apply to the media server and other AC products like gateways.

AudioCodes media servers PMs

The media server performance measurements will be provided by two AudioCodes MIBs (acPerfMediaGateway and acPerfMediaServices). The first mib is generic-type of PM mib. The second PM mib is media server

specific. The first table shows performance measurements related to control protocol, RTP stream, and system packet statistics mibs.

AMS Control Protocol, RTP, packet statistics PMs

OM Group or PM Name	Name	Description
Network Element: AMS		
acPerfMediaGateway (new in SN08	acPerfCpNumDupsForCompletedTransactions	**Number of Duplicated Completed Transactions:** The number of times a duplicate transaction request was received after the initial transaction had already been completed. In this case, the gateway resends the response for this transaction.
	acPerfCpNumDupsForOutstandingTransactions	**Number of Duplicated Transactions Outstanding:** The number of times a duplicate transaction request was received while the initial transaction was outstanding, that is, still in progress. In this case, the gateway ignores the duplicate request.
	acPerfCpMessageSendSuccesses	**Messages Send Successes:** Number of times there was a success in sending a call control (H.248) message. Call control messages are sent using the system's socket library. This counter tracks successes in using the local socket services. It does not track successes in end-to-end message transfer between the gateway and the call agent.
	acPerfCpMessageSendErrors	**Message Send Errors:** Number of times there was a failure in sending a call control (H.248) message. The message is sent via a datagram using the system's socket library. Normally a failure on a socket send operation would be attributed to an internal system problem.
	acPerfCpMessageReceiveSuccesses	**Message Receive Successes:** Number of times there was a success in receiving a call control (H.248) message. Call control messages are received using the system's socket library. This counter tracks successes in using the local socket services. It does not track successes in end-to-end message transfer between the gateway and the call agent.
	acPerfCpMessageReceiveErrors	**Message Receive Errors:** Number of times there was a failure in receiving a call control(H.248) message. Call control messages are received using the system's socket library. A failure on the socket receive operation can be attributed to an internal system problem or with the call agent sending a message larger than what is supported by the gateway.
	acPerfCpProtocolSyntaxErrors	**Protocol Syntax Errors:**: Number of syntax errors detected in incoming call control (H.248) messages.

AMS Control Protocol, RTP, packet statistics PMs

OM Group or PM Name	Name	Description
	acPerfCpMessageRetransmissions	**Message Retransmissions:** Each time the call engine times out waiting for an acknowledgement it retransmits the control protocol message, unless the number of max retransmissions is exceeded. This counter is incremented each time a message is retransmitted due to a timeout.
	acPerfCpMessageMaxRetransmissionsExceeded	**Message Max Re-transmissions Exceeded:** Number of times the call control message maximum retransmission count was exceeded. The gateway attempted several times to send a message to the call agent, but each time, an ack was not received. A failure of this type results in a failed call and is usually an indication that subsequent calls will fail. This problem is typically a result of the call agent being down or a result of a network problem
	acPerfCpMessagesFromUntrustedSources	**Messages From Untrusted Sources:** Number of messages received from untrusted sources, that is from network nodes other than the node on which the call agent is running.
	acPerfRtpSenderPackets	**RTP Sender Packets (Card):** Total number of RTP packets sent by the system for this card.
	acPerfRtpSenderOctets	**RTP Sending Octets (Card):** Total number of non-header RTP octets sent by this card.
	acPerfRtpReceiverPackets	**RTP Receiver Packets (Card):** Total number of RTP packets received by the system for this card.
	acPerfRtpReceiverOctets	**RTP Receiver Octets (Card):** Total number of non-header RTP octets received by this card.
	acPerfRtpRcvrLostPackets	**RTP Receiver Lost Packets (Card):** Total number of RTP packets lost as observed by this card.
	acPerfRtpFailedDueToLackOfResources	**RTP Failed Due to Lack of Resources**: The number of times a rtp request was rejected due to lack of resources since the last application restart.
	acPerfRtpSimplexInSessionsCurrent	**RTP Simplex In Sessions:** Current number of simplex input RTP sessions.
	acPerfRtpSimplexOutSessionsTotal	**RTP Simplex Out Session Total:** Total number of simplex output RTP sessions.
	acPerfRtpSimplexOutSessionsCurrent	**RTP Simplex Out Session Current:** Current number of simplex output RTP sessions
	acPerfRtpDuplexSessionsTotal	**RTP Duplex Sessions Total:** Total number of duplex RTP sessions.

AMS Control Protocol, RTP, packet statistics PMs

OM Group or PM Name	Name	Description
	acPerfRtpDuplexSessionsCurrent	**RTP Duplex Sessions Current**: Current number of duplex RTP sessions.
	acPerfSystemPacketEndpoints	**System Packet Endpoints:** Number of endpoints reserved for all packet network-related functions (conferencing, plays, etc.).

The second performance measurement mib is media server specific mib and contains statistics for these major categories:

- IVR – interactive voice response
- BCT – bearer channel tandeming
- CONF – Conferencing
- TT – Test Trunks

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
Network Element: AMS		
acPerfMediaServices (new in SN08	acPerfIvrPlayRequests	**Play Requests:** The total number of announcement requests received from the call agent
	acPerfIvrPlaySuccessful	**Play Successes:** Number of announcement requests processed successfully.
	acPerfIvrPlayFailedDueToLackOfResources	**Play Failures Due to Lack of Resources:** Number of announcement requests which failed to be played because some resource was not available.
	acPerfIvrPlayFailedDueToLackOfResources	**Play In Progress:** The number of announcement operations that are currently in progress.
	acPerfIvrPlayDuration	**Play Duration:** The duration, in seconds, of all successful announcement requests. The average duration of all requests (average hold time) can be computed by dividing acPerfPlayDuration by acPerfPlaySuccessful.
	acPerfIvrPlayFailedDueToProvMismatch	**Play Failed Due to Provisioning Mismatch:** Number of audio segments which failed to be played because of a provisioning mismatch.
	acPerfIvrPlayCollectRequests	**Play Collect Requests:** The number of play collect requests.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	acPerfIvrPlayCollectSuccessful	**Play Collect Successful:** Number of play collects completed successfully. A request is considered successful if the entire sequence, from initial prompt to success/failure prompt, is played out without a failure due to lack of resources, provisioning mismatch, or any other media server failure. The failure of the user to enter the proper digits is not a reason for failure of the request.
	acPerfIvrPlayCollectFailedDueToLackOfResources	**Play Collect Failure due to Lack of Resources:** The number of play collect requests that failed due to lack of resources.
	acPerfIvrPlayCollectFailedDueToProvMismatch	**Play Collect Failed Due to Provisioning Mismatches:** The number of play collect requests that failed due a provisioning mismatch.
	acPerfIvrPlayCollectInProgress	**Play Collect In Progress:** The number of play collect operations that are currently in progress.
	acPerfIvrPlayCollectDuration	**Play Collect Duration in Seconds:** The duration, in seconds, of all successful play collect requests. The average duration of all requests can be computed by dividing acPlayCollectDuration by acPlayCollectSuccessful.
	acPerfIvrContDigitCollectRequests	**Number of Continuous Digit Collection Requests:** The number of continuous digit collect requests.
	acPerfIvrContDigitCollectSuccessful	**Number of Continuous Digit Collect Requests Successful:** Number of continuous digit collects completed successfully.
	acPerfIvrContDigitCollectFailedDueToLackOfResources	**Number of Continuous Digit Collection request failed (no resources):** The number of continuous digit collect requests that failed due to lack of resources.
	acPerfIvrContDigitCollectInProgress	**In Progress Continuous Digit Collection requests:** The number of continuous digit collect operations that are currently in progress.
	acPerfIvrContDigitCollectDuration	**Successful Continuous Digit Collect Requests:** The duration, in seconds, of all successful continuous digit collect requests. The average duration of all requests can be computed by dividing acDCCollectDuration by acDCCollectSuccessful.
	acPerfBctRequests	**Total BCT Requests:** The total number of BCT contexts opened since the media server initialized.
	acPerfBctSuccessful	**Successful BCT requests:** Number of BCT requests processed successfully.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	acPerfBctFailedDueToLackOfResources	**Failed BCT requests:** Number of BCT requests which failed to be played because a resource was not available.
	acPerfBctInProgress	**In progress BCT requests:** The number of BCT calls that are currently in progress.
	acPerfBctDuration	**Duration of BCT contexts:** The duration, in seconds, of all successful BCT contexts. The average duration of all contexts can be computed by dividing acPerfBCTDuration by acPerfBCTSuccessful.
	cPerfBctTotalParticipants	**Total of BCT participants**: The total number of BCT participants since the media server initialized.
	acPerfBctCurrentNumberOfParticipants	**In progress BCT participants:** The number of participants in all BCT calls that are currently in progress.
	acPerfConfRequests	**Total number of conferences processed:** The total number of conferences processed since the last application restart. This is the number of conferences created and not the number of members.
	acPerfConfSuccessful	**Successful Conferences:** Number of conference requests processed successfully.
	acPerfConfInProgress	**In-progress Conferences:** The number of conferences currently in progress.
	acPerfConfDuration	**Conference Duration:** The duration, in seconds, of all successful conference requests. The average duration of all requests can be computed by dividing acPerfConfDuration by acPerfConfSuccessful.
	acPerfConfFailedDueToLackOfResources	**Conference Failures due to lack of resources:** The number of times a conference request was rejected due to lack of resources since the last application restart.
	acPerfConfAddRequests	**Requests to add a conferee:** The number of requests to add a conferee to an existing conference.
	acPerfConfAddSuccessful	**Conferee adds successful:** The number of times a conferee was added successfuly to an existing conference.
	acPerfConfAddFailedDueToLackOfResources	**Conferee Add Failures due to lack of resources:** The number of times a conferee could not be added to an existing conference due to a lack of resources.

AMS IVR, BCT, CONF, and IT PMs

OM Group or PM Name	Name	Description
	acPerfConfPlays	**Plays into Conference:** The total number of plays made into conferences since the last application restart.
	acPerfConfPlayCollects	**Play Collects in Conference:** The total number of play collects made into conferences since the last application restart.
	acPerfConfTones	**Play Tones into conference:** The total number of Tones played into conferences since the last application restart.
	acPerfConfPortsUsed	**Conference Ports Reserved:** The total number of ports that were reserved for conferences since the last application restart.
	acPerfConfPortsReserved	**Conference Port Reserved for monitor:** A monitor port may be reserved by the call agent when setting up a conference. The monitor port can then be used by one or more listen-only conferees.
	acPerfTtRequests	**Test Trunk Test Requests:** The number of test trunk tests requested.
	acPerfTtSuccessful	**Test Trunk Test Request Successes:** The number of test trunk tests that were successfully setup and torn down. This PM is not a reflection on whether the test actually passed or failed.
	acPerfTtInProgress	**In-Progress Test Trunk Tests:** The number of test trunk tests that are currently in progress
	acPerfTtDuration	**Test Trunk Test Duration:** The duration, in seconds, of all successful test trunk requests. This number is the time between a test trunk test being initiated and completed. The average duration of all requests can be computed by dividing acPerfTtDuration by acPerfTtSuccessful.
	acPerfTtFailedDueToLackOfResources	**Test Trunk failures due to lack of resources:** The number of times a test trunk request was rejected due to lack of resources since the last application restart.

Ethernet Routing Switch 8600 (formerly Passport 8600) PMs

For information on performance measurements (PMs) available for the Media Gateway 15000 (previously PVG) network element, refer to Appendix G in this document, *Ethernet Routing Switch 8600 Trap List.*

GWC Performance Measurements

Performance Measurements for the Gatewqy Controller are available through the Integrated EMS. For more detailed information, refer to NN10208-711,Gateway Controller Performance Management. The following table lists the GWC performance measurements.

GWC Performance Measurements

OIDs	Description
The GWC supports collection of a subset of several MIBs. The following table entries show the OIDs that are collected in various categories.	
Host-Resources-MIB	
host(25).hrSystem(1)	
25.1.hrSystemUptime(1)	System Uptime (distinct from sysUpTime)
25.1.hrSystemDate(2)	System local DateAndTime
25.1.hrSystemInitialLoadParameters(4)	Load path/parameters used
25.1.hrSystemNumUsers(5)	Current number of “user sessions”
25.1.hrSystemProcesses(6)	Number of tasks
25.1.hrSystemMaxProcesses(7)	Maximum number of tasks
host(25).hrStorage(2)	
25.2.hrMemorySize(2)	Main memory DRAM size (KBytes)
25.2.hr.StorageTable(3)	Table describing storage and resource areas, including for each: Type, Description, AllocationUnits, Size, Used, and AllocationFailures. An entry in this table is planned for each of the resources currently registered in the Base Resource Monitor: - System Heap - VRTX Workspace - Segment Descriptors - IPC Buffers - Ethernet DCU Buffers
host(25).hrDevice(3)	
25.3.hrDeviceTable(2)	Table of hardware devices contained in host, including for each: Type, Description, “ID”, Status, and Error counts. An entry is planned in this table for each of the devices listed on the PCI bus, plus the CPU.

GWC Performance Measurements

OIDs	Description
25.3.hrProcessorTable(3)	Table of info on processors for this host, including a FirmwareID and CPU-Load (1min). There will be an entry for each processor in the hrDeviceTable (just 1 for now).
25.hrSWRun(4)	
25.4.hrSWOSIndex(1)	Index of the entry in the following table for the OS.
25.4.hrSWRunTable(2)	Table of software running on the host, and for each host, a Name, ProductID, Run Path and Parameters, Type, and Status. Status is implemented as READ-ONLY.
25.hrSWRunPerf(5)	
25.5.hrSWRunPerfTable(1)	Table of performance data for software in the hrSWRun table, which includes for each task the CPU and memory usage CPU and memory usage for each task that is available.
RFC1213-MIB	
sysDescr	
snmpInPkts	
snmpOutPkts	
snmpInBadVersions	
snmpInBadCommunityNames	
snmpInBadCommunityUses	
snmpInASNParseErrs snmpInTotalReqVars	
snmpInTotalSetVars	
snmpOutTraps	
snmpSilentDrops	
Unit Status-MIB	
norUnitAdminStatus	
norUnitOperStatus	
norUnitActivity	
DPT Services PM-MIB	
dptCallAttempts	
GWC Performance Statistics	

GWC Performance Measurements

OIDs	Description
	The following are reported through the GWC Performance MIB: • Small GWs in Disabled State • Large GWs in Disabled State • Trunk GWs in Disabled State • Audio GWs in Disabled State • Total Gateways Provisioned • DNS failed GW discovery • DNS good GW discovery • RSIP used in GW discovery • Total DNS GWs to discover • USP SS7 paths disabled • USP SS7 path not Active • Peer connections failed during interval • Peer connections completed during interval • Peer connections attempted during interval

GWC Performance Measurements

OIDs	Description
GWC Performance Statistics	
Media Proxy OMs	The following are reported through the GWC Performance MIB: • Number of provisioned Media Proxies counts the number of currently provisioned media proxies on the GWC each 5-minute period. • Media Proxy 5 minute successful calls counts the number of calls that were successfully setup using this Media Proxy on this GWC in the last 5 minute OM period. • Media Proxy 30 minute successful calls counts the number of calls that were successfully setup using this Media Proxy on this GWC in the last 30 minute period. • Media Proxy 5 minute failed calls counts the number of failed attempts to setup a call using this Media Proxy on this GWC in the last 5 minute OM period. • Media Proxy 30 minute failed calls counts the number of failed attempts to setup a call using this Media Proxy on this GWC in the last 30 minute period. • GWC 5 minute successful calls counts the number of calls that were successfully setup using any available Media Proxy on this GWC in the last 5 minute OM period. • GWC 30 minute successful calls counts the number of calls that were successfully setup using any available Media Proxy on this GWC in the last 30 minute period. • GWC 5 minute failed calls counts the number of failed attempts to setup a call on any available Media Proxy on this GWC in the last 5 minute OM period. • GWC 30 minute failed calls counts the number of failed attempts to setup a call on any available Media Proxy on this GWC in the last 30 minute period.

IEMS Performance Measurements

The following table lists the performance measurements (PMs) collected by the Integrated Element Management System.

Collection Attribute Name	Description
Network Element: IEMS	
database	usedTableSpaceInBytes
	usedTableSpaceInPercent
	numOfTableCleanUpPolicyExecutions
fault/events	numOfEvents
	numOfEventsFromUnknownCustlogDevices
	numOfEventsFromUnknownDevices
	numOfDiscardedEvents
	numOfEventsAdded
	eventQueueSize
	avgEventThroughputRate
	maxEventThroughputRate
	DeviceEventRateTable This table will have the following columns: - ID - DeviceName - EventRate per Second
fault/alarms	numOfActiveAlarms
	numOfCriticalAlarms
	numOfMajorAlarms
	numOfMinorAlarms
	nmOfWarningAlarms
	numOfAlarmsCleared
	numOfAlarmsAdded
MG3200	Call Processing Performance Management (10 measurements)
	RTP Performance Measurements (12 measurements)
	System Performance Measurements (2 measurements)
performanc e	numOfCollectionJobsProvisioned
	numOfReportJobsProvisioned
	numOfFailedReportJobs
	numOfTransferJobProvisioned
	numOfAttributesCollected
	numOfAttributesCollectedOverPreviousInterval
performance/Successful Collection Jobs	numOf5MinSuccessfulJobs
	numOf15MinSuccessfulJobs
	numOf30MinSuccessfulJobs

Collection Attribute Name	Description
	numOf60MinSuccessfulJobs
	numOf12HrSuccessfulJobs
	numOf24HrSuccessfulJobs
performance/Partial Successful Collection Jobs	numOf5MinPartialSuccessfulJobs
	numOf15MinPartialSuccessfulJobs
	numOf30MinPartialSuccessfulJobs
	numOf60MinPartialSuccessfulJobs
	numOf12HrPartialSuccessfulJobs
	numOf24HrPartialSuccessfulJobs
performance/Failed Collection Jobs	numOf5MinFailedJobs
	numOf15MinFailedJobs
	numOf30MinFailedJobs
	numOf60MinFailedJobs
	numOf12HrFailedJobs
	numOf24HrFailedJobs
performance/Collection Job Table	5MinCollectionJobTable This table will have the followingcolumns - ID - JobName - Start Time - Execution Time
	15MinCollectionJobTable
	30MinCollectionJobTable
	60MinCollectionJobTable
performance/report Job Table	5MinReportJobTable
	15MinReportJobTable
	30MinReportJobTable
	60MinReportJobTable
performance/failedTransfer Jobs	numOf5MinFailedJobs
	numOf15MinFailedJobs
	numOf30MinFailedJobs
	numOf60MinFailedJobs
	numOf12HrFailedJobs
	numOf24HrFailedJobs
performance/transfer Job Table	5MinTransferJobTable
	15MinTransferJobTable
	30MinTransferJobTable
	60MinTransferJobTable

Collection Attribute Name	Description
	30MinReportJobTable
	60MinReportJobTable
topology	numOfManagedObjects
	numOfAddedManagedObjects
	numOfDeletedManagedObjects
	numOfThrottledDevices
	numOfUnManagedDevices
	numOfUnknownDevices
client	numOfActiveClients
	numOfSuccessfulLogins
	numOfFailedLoginAttempts
application memory	applicationHeapSize
	maxApplicationHeapSizeInAGivenInterval
system	systemRestartCount

MCS, RTP Media Portal, and MAS Performance Measurements

For information on performance measurements (PMs) available for these network elements, refer to the following documents:

- NN10384-700, *MCS 5200 Performance Management*
- NN10367-111, *CVoIP RTP Media Portal Basics*
- NN10303-111, *MAS Meetme Basics*

The following MCS performance measurements are new for SN09.

MCS Performance Measurements

OM Group or PM Name Registers	Description
Network Element: MCS	
StableCallCheckpointGenerated	Increments for each checkpoint generation corresponding to a new stable call on the active instance.
EndCallCheckpointGenerated	Increments when the Call terminates on the active instance and gets checkpointed for deletion.
StableCallCheckpointProcessed	Increments on the standby instance when a checkpoint indicating a new stable call or the end of an existing call is processed.
EndCallCheckpointProcessed	Increments on the standby instance when a checkpoint indicating a new stable call or the end of an existing call is processed.
CheckpointedCalls	Used on the standby instance to monitor the number of calls that would be preserved in a case of a failover.

MCS Performance Measurements

OM Group or PM Name	Registers	Description
Presence Event Report		Tracks the behavior of the various presence events that are processed by the server. For the 8 presence event types, OM registers count events Created, Processed, Optimized, Queued, and Parked.
EndCallCheckpointProcessed		Increments on the standby instance when a checkpoint indicating a new stable call or the end of an existing call is processed.
throttleNotifySelfOnly, added to the existing "Pesence" OM group		Pegged every time the system does not send out a notifications to non-self subscriptions because of a presence state change during minor overload. This is pegged once for the entire state change, and does not reflect the actual number of notify messages that were not sent out
throttleNotifyAll, added to the existing "Pesence" OM group		Pegged every time the system does not send out any notifications, including self-subscriptions because of a presence state change during major or severe overload. This is pegged once for the entire state change, and does not reflect the actual number of notify messages that were not sent out
PCMM Aggregate OMs		
	incomingMsgQHighWater - This OM indicates thehighest percentage used for the incoming PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported.	
	transactionQHighWater - This OM indicates the highest percentage used for the outgoing PCMM message queue. This value represents the high water mark since the system was started. It is not reset each time the OMs are reported.	
	voiceGateAttempts - Total number of PCMM voice half calls processed across all policy servers connected to this session server.	
	unsVoiceGateAttempts - Total number of unsuccessful PCMM voice half calls processed.	
	unsupCodecVoiceGateAttempts - Total number of PCMM voice half calls with an SDP containing at least one codec for which bandwidth could not be calculated.	
	videoGateAttempts - Total number of PCMM video half calls processed across all policy servers connected to this session server.	
	unsVideoGateAttempts - otal number of unsuccessful PCMM video half calls processed.	
	unsupCodecVideoGateAttempts - Total number of PCMM video half calls with an SDP containing at least one codec for which bandwidth could not be calculated.	
	outstandingDiscStale - The number of transactions that were discarded because no response was received from the policy server or because the outstanding transaction queue was full and the oldest transaction waiting for a response was removed to make room for a new transaction.	

MCS Performance Measurements

OM Group or PM Name	Registers	Description
		unkMediaGateAttempts - The number of PCMM gate attempts that could not be processed because the media type was unknown (i.e. not voice, video, or image).
PCMM Per-Policy Server OMs		
		numInitializations - Number of times the policy server COPS connection successfully completed the PCMM initialization sequence.
		cnxPSDrop - Number of times the policy server gracefully closed the COPS TCP connection (i.e. in a way that caused a TCP FIN message to be sent from the policy server to the session server).
		cnxDropProtTimeout - Number of times the connection was dropped by the session server due to lack of PCMM response from the policy server.
		tcpSendFail - Number of times that PCMM messages had to be discarded due to the outgoing TCP buffer being full.
		transDiscLinkDown - Number of PCMM transactions that were discarded due to the PCMM signaling link being down.
		transDiscStale - Number of PCMM transactions that were discarded because no response was received from the policy server for more than seven seconds. Or, if the outstanding transaction queue is full, the number of oldest transactions that were discarded to make room for new outstanding transactions.
		voiceGateAttempts - Total number of PCMM voice half calls processed for this policy server.
		unsVoiceGateAttempts- Total number of unsuccessful PCMM voice half calls processed.
		videoGateAttempts - Total number of PCMM voice half calls processed for this policy server.
		unsVideoGateAttempts - Total number of unsuccessful PCMM video half calls processed.
		gsaReceived - Total number of Gate-Set-Ack messages received from the policy server.
		gdSent - Total number of Gate-Delete messages sent to the policy server.
		upVoiceGSEReceived - Total number of Gate-Set-Err messages received from the policy server for upstream voice gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
		upVoiceGSENoResources - Number of Gate-Set-Err messages for upstream voice gates with error code 1 - Insufficient Resources.
		upVoiceGSEUnkGateId - Number of Gate-Set-Err messages for upstream voice gates with error code 2 - Unknown GateID.
		upVoiceGSEOther - Number of Gate-Set-Err messages for upstream voice gates with error code 127 - Other, Unspecified Error.
		dnVoiceGSEReceived - Total number of Gate-Set-Err messages received from the policy server for downstream voice gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.

MCS Performance Measurements

OM Group or PM Name	Registers	Description
		dnVoiceGSENoResources - Number of Gate-Set-Err messages for downstream voice gates with error code 1 - Insufficient Resources.
		dnVoiceGSEUnkGateId - Number of Gate-Set-Err messages for downstream voice gates with error code 2 - Unknown GateID.
		dnVoiceGSEOther - Number of Gate-Set-Err messages for downstream voice gates with error code 127 - Other, Unspecified Error.
		gseInvSubscr - Number of Gate-Set-Err messages for voice and video, upstream and downstream gates with error code 13 - Invalid Subscriber ID.
		gseInvAMID - Number of Gate-Set-Err messages for voice and video, upstream and downstream gates with error code 14 - Unauthorized AMID.
		upVideoGSEReceived - Total number of Gate-Set-Err messages received from the policy server for upstream video gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
		upVideoGSENoResources - Number of Gate-Set-Err messages for upstream video gates with error code 1 - Insufficient Resources.
		upVideoGSEUnkGateId - Number of Gate-Set-Err messages for upstream video gates with error code 2 - Unknown GateID.
		upVideoGSEOther - Number of Gate-Set-Err messages for upstream video gates with error code 127 - Other, Unspecified Error.
		dnVideoGSEReceived - Total number of Gate-Set-Err messages received from the policy server for downstream video gates. This OM is incremented for all Gate-Set-Error messages regardless of the failure reason.
		dnVideoGSENoResources - Number of Gate-Set-Err messages for downstream video gates with error code 1 - Insufficient Resources.
		dnVideoGSEUnkGateId - Number of Gate-Set-Err messages for downstream video gates with error code 2 - Unknown GateID.
		dnVideoGSEOther - Number of Gate-Set-Err messages for downstream video gates with error code 127 - Other, Unspecified Error.
		grsClose - otal number of Gate-Report-State messages received indicating that a gate was closed by the CMTS for all reasons.
		grsCloseResReassign - Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 1 - reservation reassignment.
		grsCloseMacLayer - Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 2 - lack of DOCSIS MAC-Layer responses.
		grsCloseT1 - PCMM timer T1 specifies the number of seconds a PCMM gate can be authorized but not reserved. This OM indicates the number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 3 - timer T1 expiration.

MCS Performance Measurements

OM Group or PM Name	Registers	Description
	grsCloseT2 - PCMM timer T2 specifies the number of seconds a PCMM gate must hold bandwidth reserved in excess of what was committed. Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 4 - timer T2 expiration.	
	grsCloseResMaint - Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 6 - lack of reservation maintenance.	
	grsCloseT4 - Number of Gate-Report-State messages received indicating that a gate was closed by the CMTS due to reason 8 - timer T4 expiration.	
	grsNotif - Total number of Gate-Report-State messages received indicating a change of gate state (for any reason) that did not result in the gate being closed.	
	grsNotifT3 - Number of Gate-Report-State messages received indicating that a gate was transitioned to the Committed-Recovery state by the CMTS due to the T3 timer expiring.	

MG 3200 Performance Measurements

Performance Measurements for the MG 3200 are available through the Integrated EMS via SNMP. For more information on MG 3200 PMs, refer to LTRT-72704, *Nortel Media Gateway MG3200 H.248 User's Manual.*

MG 3200 Performance Measurements

OM Group or PM Name	Registers	Description
Network Element: MG 3200		
	Call Processing Performance Management	
	acPerfCpNumDupsForCompletedTransactions	
	acPerfCpNumDupsForOutstandingTransactions	
	acPerfCpMessageSendSuccesses	
	acPerfCpMessageSendErrors	
	acPerfCpMessageReceiveSuccesses	
	acPerfCpMessageReceiveErrors	
	acPerfCpProtocolSyntaxErrors	
	acPerfCpMessageRetransmissions	
	acPerfCpMessageMaxRetransmissionsExceeded	
	acPerfCpMessagesFromUntrustedSources	
	RTP Performance Measurements	
	acPerfRtpSenderPackets	
	acPerfRtpSenderOctets	
	acPerfRtpReceiverPackets	

MG 3200 Performance Measurements

OM Group or PM Name	Registers	Description
	acPerfRtpReceiverOctets	
	acPerfRtpRcvrLostPackets	
	acPerfRtpFailedDueToLackOfResources	
	acPerfRtpSimplexInSessionsTotal	
	acPerfRtpSimplexInSessionsCurrent	
	acPerfRtpSimplexOutSessionsTotal	
	acPerfRtpSimplexOutSessionsCurrent	
	acPerfRtpDuplexSessionsTotal	
	acPerfRtpDuplexSessionsCurrent	
	System Performance Measurements	
	acPerfSystemPacketEndpoints	
	acPerfSystemPacketEndpointsInUse	

MG 9000 Performance Measurements

Performance Measurements for the MG 9000 are available through the Integrated EMS. For more information on MG9000 PMs, refer to NN10140-711, *MG 9000 Performance Management* and Appendix B of this document, *MG 9000 MIB OMs/PMs*. That appendix, together with the following table, list the MG 9000 performance measurements.

MG 9000 Performance Measurements

OM Group or PM Name	Registers	Description
Network Element: MG 9000		
Ethernet OMs		
	Number of Alignment Errors	
	Number of FCS Errors	
	Number of Internal MAC Receive Errors	
	Number of Frame Too Longs	
	Number of Internal MAC TX Errors	
	Number of Symbol Errors	
	Number of Inpause Frames	
	Number of Outpause Frames	
	Number of Drop Events	
	Number of Broadcast Packets	

MG 9000 Performance Measurements

OM Group or PM Name	Registers	Description
	Number of Multicast Packets	
	Number of CRC Alignment Errors	
	Number of Undersize Packets	
	Number of Oversize Packets	
	Number of Fragments	
	Number of Jabbers	
	Number of Collisions	
GWOVLOM This OM group will be incremented for every call connection request that is denied.		
	OVERLOAD	This register is incremented when a Media Gateway 9000 reaches an overload threshold and call connections are denied.
MG9K Performance Statistics		
	Errored Seconds	
	Severely Errored Seconds	
	Unavailable Seconds	
	Optical Power Transmit	
	Optical Power Receive	
	Transmit Bias Current	
	Termperature	
	Voltage	
MG9K GIGE OM Statistics MG9K EM performance strategy where the data is collected in 15 or 5/30 minutes for 96 intervals.		
	Errored Seconds	Counter for Errored Seconds
	Severely Errored Seconds	Counter for Severely Errored Seconds
	Unavailable Seconds	Counter for Unavailable Seconds
	Optical Power Transmit	Optical Power Transmit
	Optical Power Receive	Counter for Optical Power Receive
	Transmit Bias Current	Counter for Transmit Bias Current
	Temperature	Counter for Temperature
RMON Performance Measurements		
	Drop Events	The current data associated with etherStatsDropEvents.
	Broadcast Packets	The counter data associated with etherStatsBroadcastPkts.
	Multicast Packets	The counter associated with etherStatsMulticastPkts.
	CRC Alignment Errors	The counter associated with etherStatsCRCAlignErrors.
	Undersize Packets	The counter associated with etherStatsUndersizePkts.

MG 9000 Performance Measurements

OM Group or PM Name	Registers	Description
	Oversize Packets	The counter associated with etherStatsOversizePkts.
	Fragments	The counter associated with etherStatsFragments.
	Jabbers	The counter associated with etherStatsJabbers.
	Collisions	The counter associated with etherStatsCollisions.
RMON HC Performance Measurements		
	HC overflow packets	The counter associated with HC Overflow Packets.
	Packets received	The counter associated with number of packets received.
	Overflow octets	The counter associated with HC number of Overflow octets.
	Octets of data received	The counter associated with number of octets of data received.
	Total HC Octets	The counter associated with Total Number of HC Octets.
	Total non unicast packets	The counter associated with Total number of non unicast packets.
	Total non unicast HC octets	The counter associated with Total number of non unicast HC octets.
	Total non unicast octets	The counter associated with Total number of non unicast octets.
	Total non unicast over flow octets	The counter associated with Total number of non unicast over flow octets.
	Total non unicast HC octets	The counter associated with Total number of non unicast HC octets.
SMON MIB table		
	smonVlanIdStatsTotal Pkts	Total incoming packets.
	smonVlanIdStatsTotal HCPkts	Total outgoing packets.
	smonVlanIdStatsTotal Octets	Ttotal incoming octets.
	smonVlanIdStatsTotal HCOctets	Total outgoing octets.
SMON Performance Measurements		
	VLAN ID	The VLAN ID.
	Total Packets	The counter associated with Total number Packets.
	Total HC Packets	The counter associated with Total Number of HC Packets.
	Create time	The Create time.
	Total Octets	The counter associated with Total Number of Octets.
	Total HC octets	Displays the total number of HC octets.
	Total overflow packets	Displays the total number of overflow packets.

MG 9000 Performance Measurements

OM Group or PM Name	Registers	Description
	Total overflow octets	Displays the total number of overflow octets.
	Total non unicast packets	The counter associated with Total number of non unicast packets.
	Total non unicast HC octets	The counter associated with Total number of non unicast HC octets.
	Total non unicast octets	The counter associated with Total number of non unicast octets.
	Total non unicast over flow octets	The counter associated with Total number of non unicast over flow octets.
	Total non unicast HC octets	The counter associated with Total number of non unicast HC octets.
SMON Performance		
	smonVlanIdStatsTotalPkts - total incoming packets	
	smonVlanIdStatsTotalHCPkts - total outgoing packets	
	smonVlanIdStatsTotalOctets - total incoming octets	
	smonVlanIdStatsTotalHCOctets - total outgoing octets	

Media Gateway 15000 OMs/PMs and Passport 15000/Multiservice Switch OMs/PMs

Note: Starting in SN08, the terms Packet Voice Gateway (PVG) and Passport 15000 were rebranded as part of Nortel Networks' brand simplified naming format. The PVG is now referred to as Nortel Networks Media Gateway 15000. The Passport 15000 is now referred to as the Nortel Networks Multiservice Switch 15000.

For details on Media Gateway 15000 and Multiservice Switch 15000 performance measurements, refer to NTP NN10158-711, *MSS 15000, MG 15000 & MDM Performance.*

Starting in SN08, the the 5- and 30-minute performance measurements (PMs) provided Internet protocol (IP) statistics. The IP statistics are available at a physical interface level. You can use IP statistics for operational monitoring and for network planning and engineering. Also, you can obtain performance information from IP statistics, such as link bandwidth utilization, voice call volumes, and error conditions. These are key for monitoring the network using PMs. Within the Multiservice Switch, performance measurements (PMs) are referred to as network traffic management (NTM) statistics.

IP interface statistics apply to all physical interfaces on Nortel Networks Multiservice Switch 15000 nodes that process layer 3 IP. This includes ports on the Ethernet-based Gigabit Ethernet (GE) function processors (FPs), the control processor (CP) operations, administration, and maintenance (OAM) Ethernet port, and the asynchronous transfer mode (ATM)-based OC-3, OC-12 and DS3 ports. PMs for these nodes now include an expanded range of values.

Statistics collection and data flow

The data collection system (DCS) on the node collects NTM statistics from the control and function processors, and ATM and IP interfaces, at 5-minute intervals. To collect the statistics, the DCS uses a real-time statistics stream (rtstats). Each node forwards these records to Nortel Networks Multiservice Data Manager (MDM) servers.

On Nortel Networks Multiservice Data Manager (MDM) servers, the Performance Measurements Stream Processor (PMSP) server application manages performance. NTM statistics originating from node processors flow to the PMSP server application. The PMSP server application converts the statistics into ASCII comma separated value (CSV) formatted 5-minute records. It also creates 30-minute data records by aggregating six 5-minute data records. These are referred to as 5-minute and 30-minute performance measurements (PMs).

The MDM servers transfer the NTM data directly to the OSS applications, or to the CS2000 Core Manager running on the SDM, depending on the network configuration.

Accessing files through the SDM or MDM

Note: Access via SDM is not generally available for Media Gateway 15000 (previously PVG) performance measurements.

NTM statistics data can be configured to be obtained from the SuperNode Data Manager (SDM).The PM file follows the file naming conventions of the Operational Measurement Delivery (OMD) application. The format of the file name is:

```
<name>.<date>.<time>.PP.<type>.CSV
```

The collected NTM statistics files are stored in the /omdata/closedNotSent directory. They are now available to the OSS application. The OSS application retrieves the files and moves them to the /omdata/closedSent directory. Upon the transfer of the files, the OMD automatically sets the retention period for the files. The retention period for a file can be configured using the OMUI. It can range from one to fourteen days.

When NTM statistics data is configured to be obtained from Nortel Networks Multiservice Data Manager (MDM) servers, the name of the file is similar to that used by SDM. However, the Host Group Directory Server (HGDS) group name or shelf name indicating the source of the NTM statistics data replaces the "PP" string found after the time stamp in the SDM file name. The format for the file name appears below.

```
<name>.<date>.<time>.<HGDS group or shelf name>.<type>.CSV
```

PMs for Media Gateway 15000

For information on performance measurements (PMs) available for the Media Gateway 15000 (previously PVG) network element, refer to NN10158-711, *MSS 15000, MG 15000 & MDM Performance*.

MS 2000 Series Node OMs/PMs

Refer to NN10320-100, *ATM Solutions Basics,* and NN10300-100, *IP Solutions Basics*.

Session Server Manager OMs/PMs

Refer to NN10342-711, *Session Server Manager Performance Management*.

SAM21 OMs/PMs

The SAM21 EM has no operational or performance measurements.

STORM OMs/PMs

Refer to NN10054-711, *STORM Performance Management*.

UAS OMs/PMs

The following table lists the operational measurements (OMs) and performance measurements (PMs) available for the UAS network element.

UAS supports CSV and XML format. For details, refer to NN10139-001, *UAS Performance*.

OM group or PM name	Description
Network Element: UAS	
CRC Count	A Minor alarm is raised when the CRC error count threshold is exceeded.
Plane Msg Count	A Minor alarm is raised when the plane message count threshold is exceeded.
norUasProtocolSyntaxErrors	Number of syntax errors detected in incoming call control (MGCP, H.248) messages.
norUasProtocolMessageValidationErrors	Number of times an incoming call control (MGCP, H.248) message had valid syntax, but failed validation
norUasUdpSendErrors	Number of times there was a failure in sending a call control (MGCP, H.248) message. The message is sent via a datagram using the system's socket library. Normally a failure on a socket send operation would be attributed to an internal system problem.
norUasUdpReceiveErrors	Number of times there was a failure in receiving a call control (MGCP, H.248) message. Call control messages are received using the system's socket library. A failure on the socket receive operation can be attributed to an internal system problem or with the call agent sending a message larger than what is supported by the gateway.
norUasMgcpMessageRetransmissions	Number of retransmissions of media gateway control protocol messages. Media gateway control protocol is used in here in a generic sense to include both MGCP and H.248
norUasMgcpMessageRetransmissionFailures	Number of times a retransmitted media gateway control protocol message was not acknowledged. Media gateway control protocol is used in here in a generic sense to include both MGCP and H.248.
norUasAudioSegmentPlayed	Number of successful attempts to play audio. For the current number of play attempts, see norUasCurrentNumberOfPlays.
norUasAudioSegmentFailed	Number of failed attempts to play audio. Failures can occur for the following reasons: - call agent sent a bad audio segment id - the audio segment is not provisioned - there was an internal program error Examine the logs to determine the exact nature of the failure.
norUasAckfail	Number of negative acknowledgements (nacks) received. Nacks can be sent by the call agent in response to RSIP or NTFY messages.

OM group or PM name	Description
norUasTimeout	Number of times the call engine timed out waiting for an acknowledgement.
norUasProterror	Number of call control protocol errors detected. Typical reasons for these errors are: - duplicate parameter - invalid range of parameter - mandatory parameter missing Examine the logs to determine the exact nature of the failure.
norUasRestart	Number of abnormal restarts of one of two critical threads in the call processing process. The two threads are the event state machine thread and the maintenance state machine thread. Examine the logs to determine which thread failed.
norUasComperror	The number of times the call engine failed to build a response to a call agent message. Examine the logs to determine the exact nature of the failure.
norUasConndeleted	Number of times that the call engine receives a bad connection id from the call agent. This is normally a result of the call agent sending a message for a connection that has already been deleted.
norUasCallControlMessageSendFailures	Number of times the call control message maximum retransmission count was exceeded. The UAS attempted several times to send a message to the call agent, but each time, an ack was not received. A failure of this type results in a failed call and is usually an indication that subsequent calls will fail. This problem is typically a result of the call agent being down or a result of a network problem.
norUasEndpointsInUse	Number of endpoints that the call engine is currently using for all packet network-related functions (conferencing, plays, etc.).
norUasNumDupsForCompletedTransactions	The number of times a duplicate transaction request was received after the initial transaction had already been completed. In this case, the gateway resends the response for this transaction.
norUasNumDupsForOutstandingTransactions	The number of times a duplicate transaction request was received while the initial transaction was outstanding, that is, still in progress. In this case, the gateway ignores the duplicate request.
norUasConfTotal	The total number of conferences processed since the last application restart.
norUasConfLackOfResourceRejections	The number of times a conference request was rejected due to lack of resources since the last application restart.

OM group or PM name	Description
norUasConfPlays	The total number of plays made into conferences since the last application restart.
norUasRequestsFailed	The number of resource requests for endpoints on this pool that failed.
norUasNumberOfPlayRecords	The total number of play record operations.
norUasNumberOfPlayRecordErrors	The total number of failed play record operations.

USP OMs/PMs

See Appendix D

Refer to Appendix D for a complete list of the operational measurements (OMs) and performance measurements (PMs) available for the USP network element. You may also refer to NN10137-711, *USP Performance Management* and NN1038-711, *USP-Compact Performance Management*.

USP supports SSV format. For details on this format, refer to the Performance section of the FCAPS documentation on USP, NN10137-711.

Appendix A: Ethernet Routing Switch 8600 Performance Metrics

Performance Metric Identifier	MIB Name	Description	Default Succession IEMS Collection Interval
RFC1213-MIB			
sysDescr	RFC1213-MIB	A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.	Every 30 mins
sysObjectID	RFC1213-MIB	The vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining `what kind of box' is being managed. For example, if vendor `Flintstones, Inc.' was assigned the subtree 1.3.6.1.4.1.4242, it could assign the identifier 1.3.6.1.4.1.4242.1.1 to its `Fred Router'.	Every 30 mins
sysUpTime	RFC1213-MIB	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.	Every 30 mins
sysName	RFC1213-MIB	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.	Every 30 mins
sysLocation	RFC1213-MIB	The physical location of this node (e.g., `telephone closet, 3rd floor').	Every 30 mins
ifIndex	RFC1213-MIB	A list of the following PM ID labels contained in this table.	Every 5 and 30 mins
ifDescr	RFC1213-MIB	DisplayString. A textual string containing information about the interface. This string should include the name of the manufacturer, the product name and the version of the hardware interface."	Every 5 and 30 mins
ifInOctets	RFC1213-MIB	The total number of octets received on the interface, including framing characters.	Every 5 and 30 mins
ifInDiscards	RFC1213-MIB	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.	Every 30 mins
ifInErrors	RFC1213-MIB	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.	Every 30 mins
ifOutOctets	RFC1213-MIB	The total number of octets transmitted out of the interface, including framing characters.	Every 5 and 30 mins
ifOutDiscards	RFC1213-MIB	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.	Every 30 mins
ifOutErrors	RFC1213-MIB	The number of outbound packets that could not be transmitted because of errors.	Every 30 mins
ipInReceives	RFC1213-MIB	The total number of input datagrams received from interfaces, including those received in error.	Every 5 and 30 mins
ipInDiscards	RFC1213-MIB	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.	Every 30 mins
ipOutRequests	RFC1213-MIB	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. Note that this counter does not include any datagrams counted in ipForwDatagrams.	Every 5 and 30 mins
ipOutDiscards	RFC1213-MIB	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.	Every 30 mins
RFC1271-MIB			
etherStatusDataSource	RFC1271-MIB	A list of the following PM ID labels contained in this table.	Every 30 mins
etherStatsCRCAlignErrors	RFC1271-MIB	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).	Every 30 mins
etherStatsUndersizePkts	RFC1271-MIB	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.	Every 30 mins
etherStatsOversizePkts	RFC1271-MIB	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.	Every 30 mins

Performance Metric Identifier	MIB Name	Description	Default Succession IEMS Collection Interval
etherStatsFragments	RFC1271-MIB	The total number of packets received that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits but including FCS octets).	Every 30 mins
etherStatsJabbers	RFC1271-MIB	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).	Every 30 mins
etherStatsCollisions	RFC1271-MIB	The best estimate of the total number of collisions on this Ethernet segment.	Every 30 mins
etherHistoryIndex	RFC1271-MIB	A list of the following PM ID labels contained in this table.	Every 30 mins
etherHistoryCRCAlignErrors	RFC1271-MIB	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).	Every 30 mins
etherHistoryUndersizePkts	RFC1271-MIB	The number of packets received during this interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.	Every 30 mins
etherHistoryOversizePkts	RFC1271-MIB	The number of packets received during this interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.	Every 30 mins
etherHistoryFragments	RFC1271-MIB	The total number of packets received during this sampling interval that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits but including FCS octets).	Every 30 mins
etherHistoryJabbers	RFC1271-MIB	The number of packets received during this interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and were not an integral number of octets in length or had a bad Frame Check Sequence (FCS).	Every 30 mins
etherHistoryCollisions	RFC1271-MIB	The best estimate of the total number of collisions on this Ethernet segment during this interval.	Every 30 mins
historyControlDataSource	RFC1271-MIB	This object identifies the source of the data for which historical data was collected and placed in a media-specific table on behalf of this historyControlEntry. This source can be any interface on this device. In order to identify a particular interface, this object shall identify the instance of the ifIndex object, defined in [4,6], for the desired interface.	Every 30 mins
OSPF-MIB			
ospfIfIpAddress	OSPF-MIB	A list of the following PM ID labels contained in this table.	Every 30 mins
ospfAddressLessIf	OSPF-MIB	Integer32. For the purpose of easing the instancing of addressed and addressless interfaces; This variable takes the value 0 on interfaces with IP Addresses, and the corresponding value of ifIndex for interfaces having no IP Address.	Every 30 mins
ospfIfEvents	OSPF-MIB	The number of times this OSPF interface has changed its state, or an error has occurred.	Every 30 mins
OSPF-MIB			
ospfNbrAddressLessIndex	OSPF-MIB	A list of the following PM ID labels.	Every 30 mins
ospfNbrIpAddr	OSPF-MIB	The IP address this neighbor is using in its IP Source Address. Note that, on addressless links, this will not be 0.0.0.0, but the address of another of the neighbor's interfaces.	Every 30 mins
ospfNbrEvents	OSPF-MIB	The number of times this neighbor relationship has changed state, or an error has occurred.	Every 30 mins
SNMP-FRAMEWORK-MIB			
snmpInvalidMsgs	SNMP-FRAMEWORK-MIB	The total number of packets received by the SNMP engine which were dropped because there were invalid or inconsistent components in the SNMP message.	Every 30 mins
SNMP-FRAMEWORK-MIB			
snmpInPkts	SNMP-FRAMEWORK-MIB	The total number of Messages delivered to the SNMP entity from the transport service.	Every 30 mins
snmpOutPkts	SNMP-FRAMEWORK-MIB	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.	Every 30 mins
snmpInBadVersions	SNMP-FRAMEWORK-MIB	The total number of SNMP Messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.	Every 30 mins
snmpInBadCommunityUses	SNMP-FRAMEWORK-MIB	The total number of SNMP Messages delivered to the SNMP protocol entity which represented an SNMP operation which was not allowed by the SNMP community named in the Message.	Every 30 mins
snmpInASNParseErrs	SNMP-FRAMEWORK-MIB	The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP Messages.	Every 30 mins
snmpInTotalReqVars	SNMP-FRAMEWORK-MIB	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.	Every 30 mins

Performance Metric Identifier	MIB Name	Description	Default Succession IEMS Collection Interval
snmpInTotalSetVars	SNMP-FRAMEWORK-MIB	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.	Every 30 mins
snmpOutTraps	SNMP-FRAMEWORK-MIB	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.	Every 30 mins
VRRP-MIB			
vrrpStatusIfIndex	VRRP-MIB	INTEGER. A list of the following PM ID labels contained in this table.	Every 30 mins
vrrpStatsVrId	VRRP-MIB	Integer32 (1..255). This object contains the Virtual Router Identifier (VRID).	Every 30 mins
vrrpStatsBecomeMaster	VRRP-MIB	The total number of times that this virtual router's state has transitioned from BACKUP to MASTER.	Every 30 mins
RAPID-CITY (rcStat)			
rcSysBufferUtil	RAPID-CITY	Buffer utilization as a percentage of the total amount of buffer space in the system. A high value indicates congestion.	Every 30 mins
rcSysBufferUtilPeak	RAPID-CITY	The largest buffer utilization since sysUpTime.	Every 30 mins
rcSysBufferUtilPeakTime	RAPID-CITY	Timestamp for rcSysPeakBandwidth.	Every 30 mins
rcSysNVRamUsed	RAPID-CITY	Non-volatile RAM in use in Kbytes.	Every 30 mins
rcSysCpuUtil	RAPID-CITY	Percentage of CPU utilization.	Every 30 mins
rcSysSwitchFabricUtil	RAPID-CITY	Percentage of Switching Fabric utilization.	Every 30 mins
rcStatPortIndex	RAPID-CITY	Integer32. A list of the following PM ID labels contained in this table.	Every 30 mins
rcStatFrameTooShorts	RAPID-CITY	The total number of frames that are too short that were encountered on this interface.	Every 30 mins
rcStatBridgeInDiscards	RAPID-CITY	The total number of frames that were discarded by the bridging entity.	Every 30 mins
rcStatRouteInDiscards	RAPID-CITY	The total number of frames that were discarded by the bridging entity.	Every 30 mins
rcStatStgForwardTransitions	RAPID-CITY	The number of times this port has transitioned from the Learning state to the Forwarding state.	Every 30 mins
rcStatGigPortIndex	RAPID-CITY	Integer32. A list of the following PM ID labels contained in this table.	Every 30 mins
rcStatGigLinkFailures	RAPID-CITY	The total number of link failures encountered on this interface.	Every 30 mins
rcStatGigPacketErrors	RAPID-CITY	The total number of packet errors encountered on this interface.	Every 30 mins
rcStatGigCarrierErrors	RAPID-CITY	The total number of carrier errors encountered on this interface.	Every 30 mins
rcStatGigLinkInactiveErrors	RAPID-CITY	The total number of link inactive errors encountered on this interface.	Every 30 mins
rcStatSmltIstDownCnt	RAPID-CITY	Counters that counts how the session between the two peering switches has done down since last boot.	Every 30 mins
rcStatSmltSmltDownTxMsgCnt	RAPID-CITY	Counters that counts the tx Smlt Down msg.	Every 30 mins
rcStatSmltSmltDownRxMsgCnt	RAPID-CITY	Counters that counts the rx Smlt Down msg.	Every 30 mins
rcStatSmltSmltUpTxMsgCnt	RAPID-CITY	Counters that counts the tx Smlt Up msg.	Every 30 mins
rcStatSmltSmltUpRxMsgCnt	RAPID-CITY	Counters that counts the rx Smlt Up msg.	Every 30 mins
RAPID-CITY (rc2kAtm)			
rc2kAtmPortStatsIndex	RAPID-CITY	Integer32. A list of the following PM ID labels contained in this table.	Every 30 mins
rc2kAtmPortStatsInDroppedPkts	RAPID-CITY	Number of AAL5 CPCS PDUs dropped due to resource exhaustion.	Every 30 mins
rc2kAtmPortStatsOutDroppedPkts	RAPID-CITY	Number of AAL5 CPCS PDUs dropped because the transmitter closed the channel.	Every 30 mins
rc2kAtmVportStatsIfIndex	RAPID-CITY	Integer32. A list of the following PM ID labels contained in this table. Port number.	Every 5 and 30 mins
rc2kAtmVPortStatsInOctets	RAPID-CITY	AAL5 CPCS PDU octects received from ATM interface	Every 5 and 30 mins
rc2kAtmVPortStatsOutOctets	RAPID-CITY	AAL5 CPCS PDU octects transmitted out of ATM interface	Every 5 and 30 mins
rc2kAtmVPortStatsInErrors	RAPID-CITY	AAL5 CPCS PDUs received with errors from ATM interface. These errors include CRC-32 errors,SAR time-out errors and oversized SDU errors.	Every 30 mins
rc2kAtmVPortStatsOutErrors	RAPID-CITY	Number of AAL5 CPCS PDUs that couldn't be transmitted due to errors.	Every 30 mins
rc2kAtmVPortStatsInDiscards	RAPID-CITY	Number of received AAL5 CPCS PDUs discarded.	Every 30 mins
rc2kAtmVPortStatsOutDiscards	RAPID-CITY	Number of AAL5 CPCS PDUs which are to be transmitted but discarded.	Every 30 mins
rcStgPort	RAPID-CITY	Integer32. The port number of the port for which this entry contains Spanning Tree Protocol management information	Every 30 mins
rcStgPortForwardTransitions	RAPID-CITY	The number of times this port has transitioned from the Learning state to the Forwarding state.	Every 30 mins

OMs collected via CSV for OSS
Not supported at Performance Browser
New in SN09

Appendix B: MG 9000 MIB OMs/PMs

OM Name	Type	Description
norCarrSonetMedCurrentOpt	Unsigned32	Optical Power Transmitted. This is interpreted as a Percentage
norCarrSonetMedIntervalLBC	Unsigned32	Laser Bias Current.
nnMegacoOMDSPIntervalTable		
nnMegacoOMDSPnumToneRcvrReq	Unsigned32	The number of tone receiver requests during this interval.
nnMegacoOMDSPnumToneRcvrReqFail	Unsigned32	The number of tone receiver requests that failed during this interval.
nnMegacoOMDSPnumToneGenReq	Unsigned32	The number of tone generator requests during this interval.
nnMegacoOMDSPnumToneGenReqFail	Unsigned32	The number of tone generator requests that failed during this interval.
nnMegacoOMDSPnumCMRmodemReq	Unsigned32	The number of CMR modem requests during this interval.
nnMegacoOMDSPnumCMRmodemReqFail	Unsigned32	The number of CMR modem requests that failed during this interval.
nnMegacoOMDSPCurrentDayTotalTable		
nnMegacoOMCESnumChnlAllocIntra	Unsigned32	The total number of channel allocation requests for intra-switched calls during this interval.
nnMegacoOMCESnumChnlAllocIntraFail	Unsigned32	The total number of channel allocation requests for intra-switched calls that failed during this interval.
nnMegacoOMCESnumChnlAllocInter	Unsigned32	The total number of channel allocation requests for inter-switched calls during this interval.
nnMegacoOMCESnumChnlAllocInterFail	Unsigned32	The total number of channel allocation requests for inter-switched calls that failed during this interval.
nnMegacoOMECANIntervalTable		
nnMegacoOMECANnumResrceReq	Unsigned32	The total number of ECAN resource request attempts during this interval.
nnMegacoOMECANnumResrceReqFail	Unsigned32	The total number of ECAN resource request attempts that failed during this interval.
nnMegacoQoSIntervalTable		
nnMegacoQoSIntervalCalls	Unsigned32	total number of calls (in this 15-min interval)."
nnMegacoQoSIntervalBadCalls	Unsigned32	total number of bad calls (in this 15-min interval)."
nnMegacoQoSIntervalPktsSent	Unsigned32	number of packets sent (in this 15-min interval)."
nnMegacoQoSIntervalPktsLost	Unsigned32	number of packets lost (in this 15-min interval)."
nnMegacoQoSIntervalPktLossPct	Interger	% of packets lost (in this 15-min interval)."
nnMegacoQoSIntervalJitter	Unsigned32	average jitter (in a 15-min interval)."
nnMegacoQoSIntervalLatency	Unsigned32	average latency (in a 15-min interval)."
nnMegacoOMMedGwyIntervalTable		
nnMegacoOMMedGwyNumInMessages	Unsigned32	Number of messages received from the Gateway Controller (GWC) during this interval.
nnMegacoOMMedGwyNumInOctets	Unsigned32	Number of octets received from the Gateway Controller (GWC) during this interval.
nnMegacoOMMedGwyAvrgInMsgRate	Unsigned32	Average message rate (per minute) for messages received from the GWC during this interval.
nnMegacoOMMedGwyMaxInMsgRate	Unsigned32	Maximum message rate (per minute) for messages received from the GWC during this interval.
nnMegacoOMMedGwyNumOutMessages	Unsigned32	Number of messages sent to the Gateway Controller (GWC) during this interval.
nnMegacoOMMedGwyNumOutOctets	Unsigned32	Number of octets sent to the Gateway Controller (GWC) during this interval.
nnMegacoOMMedGwyAvrgOutMsgRate	Unsigned32	Average message rate (per minute) for messages sent to the GWC during this interval.
nnMegacoOMMedGwyMaxOutMsgRate	Unsigned32	Maximum message rate (per minute) for messages sent to the GWC during this interval.
NORTEL-UEMG-BANDWIDTH-MIB		
nnBwShelfCurrentSloaBandwResrvdTable		

nnBwShelfCapacitySloaBandwReserved	NnBwCellsPerSec	Current amount of reserved bandwidth Capacity for the aggregate of all Switched Lines over ATM VCs on This UEMG shelf.
nnBwShelfIntervalSloaBandwResrvdTable		
nnBwShelfIntervalSloaBandwReserved	NnBwCellsPerSec	ith 15-minute measure amount of reserved band width allocated for the aggregate of all Switched Lines over ATM VCs on This UEMG shelf."
nnBwIntervalBandwUtilTable		
nnBwBandwUtilIntervalInCellRate	NnBwCellsPerSec	The ith 15min measure of the inbound bandwidth utilization.
nnBwBandwUtilIntervalOutCellRate	NnBwCellsPerSec	The ith 15min measure of the outbound bandwidth utilization.
nnBwBandwUtilIntervalInDslCellRate	NnBwCellsPerSec	The ith 15min measure of the inbound dsl band width utilization.
nnBwBandwUtilIntervalOutDslCellRate	NnBwCellsPerSec	The ith 15min measure of the outbound dsl band width utilization.
nnBwIntervalQueueFillTable		
nnBwQueueFillIntervalTotal	NnBwPercent	ith 15-minute value % fill of the entire input cell queue associated with the central switching fabric.
nnBwQueueFillIntervalCbr	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all CBR VCs.
nnBwQueueFillIntervalRtVbr	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all rt-VBR VCs.
nnBwQueueFillIntervalNrtVbr	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all nrt-VBR VCs.
nnBwQueueFillIntervalUbr	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all UBR VCs.
nnBwQueueFillIntervalUbrPlus	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all UBR+ VCs.
nnBwQueueFillIntervalControl	NnBwPercent	ith 15-minute value % fill of the entire input queue associated with the aggregate of all Control VCs.
nnBwAbiCurrentBandwResrvdTable		
nnBwAbiCapacityBandwReserved	NnBwCellsPerSec	Current amount of reserved bandwidth Capacity for the aggregate of all ABI VCs on this ABI interface.
nnBwAbiIntervalBandwResrvdEntry		
nnBwAbiIntervalBandwReserved	NnBwCellsPerSec	ith 15-minute measure amount of reserved bandwidth allocated for the aggregate of all VCs on this ABI interface."
SNMP-MPD-MIB		
SNMP Table		
snmpInvalidMsgs	Counter32	The total number of packets received by the SNMP engine which were dropped because there were invalid or inconsistent components in the SNMP message.
SNMPv2-MIB		
snmpInBadCommunityNames	Counter32	The total number of community-based SNMP messages (for example, SNMPv1) delivered to the SNMP entity which used an SNMP community name not known to said entity. Also, implementations which authenticate community-based SNMP messages using check(s) in addition to matching the community name (for example, by also checking whether the message originated from a transport address allowed to use a specified community name) MAY include in this value the number of messages which failed the additional check(s). It is to authenticate community-based SNMP messages specify the precise conditions that contribute to this value.
snmpInPkts	Counter32	The total number of messages delivered to the SNMP entity from the transport service.
NORTEL-UEMG-CLKSYNC-MIB		
NnClkSyncRefTable		This table provides status information for each of the sync reference inputs associated with the ITP card. There are six references per ITP card, two ITP cards on each shelf.
nnClkSyncRefId	interger	Reference Identification... Identifies the six possible clock synchronization references on the ITP card. This field along with entPhysicalIndex defines a unique row in the nnClkSyncRefTable. itx0 (1), -- reference coming from the left ITX (ITX 0) itx1 (2), -- reference coming from the right ITX (ITX 1)

		dcc0 (3), -- reference coming from the left DCC (DCC-0) dcc1 (4), -- reference coming from the right DCC (DCC-1) host0 (5), -- reference cabled into the ITP ATM25 phy0 host1 (6) -- reference cabled into the ITP ATM25 phy1 "
nnClkSyncRefLossOfSignalCount	Unsigned32	Contains the count of the number of onsets of timing reference signal loss. Range is from 0 - 255
nnClkSyncRefLossOfFrameCount	Unsigned32	Contains the count of the number of loss of frames. Range is from 0 - 255.
NnClkSyncSignalTable		This table provides status information on each of the six timing signals coming into the UE9KMG host shelf. There is one entry for each network timing signal (total of two), and one entry for each BITS signal (total of 4)
nnClkSyncSignalId	interger	Signal Identification... Identifies the six possible timing source signals which eventually are seen as references into the ITP card. This field defines a unique row in the nnClkSyncSignalTable. bitsA-0 (1), -- BITS A signal coming into the left ITX of -- the BITS ITX connected pair. bitsB-0 (2), -- BITS B signal coming into the left ITX of -- the BITS ITX connected pair. bitsA-1 (3), -- BITS A signal coming into the right ITX of -- the BITS ITX connected pair. bitsB-1 (4), -- BITS B signal coming into the right ITX of -- the BITS ITX connected pair. dcc-0 (5), -- Network Traffic signal coming into DCC-0 dcc-1 (6) -- Network Traffic signal coming into DCC-1"
nnClkSyncSignalLossOfFrameCount	Unsigned32	Contains the count of the number of loss of frames.
nnClkSyncSibnalLossOfSignalCount	Unsigned32	Contains the count of the number of onsets of timing source signal loss.
SONET-MIB		
sonetSectionIntervalTable		
sonetSectionIntervalESs	PerfIntervalCount	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Section in a particular 15-minute interval in the past 24 hours.
sonetSectionIntervalSESs	PerfIntervalCount	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Section in a particular 15-minute interval in the past 24 hours.
sonetSectionIntervalSEFSs	PerfIntervalCount	The counter associated with the number of Severely Errored Framing Seconds encountered by a SONET/SDH Section in a particular 15- minute interval in the past 24 hours.
sonetSectionIntervalCVs	PerfIntervalCount	The counter associated with the number of Coding Violations encountered by a SONET/SDH Section in a particular 15-minute interval in the past 24 hours.
sonetLineIntervalTable		
sonetLineIntervalESs	PerfIntervalCount	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Line in a particular 15-minute interval in the past 24 hours.
sonetLineIntervalSESs	PerfIntervalCount	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Line in a particular 15-minute interval in the past 24 hours.
sonetLineIntervalCVs	PerfIntervalCount	The counter associated with the number of Coding Violations encountered by a SONET/SDH Line in a particular 15-minute interval in the past 24 hours.
sonetLineIntervalUASs	PerfIntervalCount	The counter associated with the number of Unavailable Seconds encountered by a SONET/SDH Line in a particular 15-minute interval in the past 24 hours.
sonetPathIntervalTable		
sonetPathIntervalESs	PerfIntervalCount	The counter associated with the number of Errored Seconds encountered by a SONET/SDH Path in a particular 15-minute interval in the past 24 hours.
sonetPathIntervalSESs	PerfIntervalCount	The counter associated with the number of Severely Errored Seconds encountered by a SONET/SDH Path in a particular 15-minute interval in the past 24 hours.

sonetPathIntervalCVs	PerfIntervalCount	The counter associated with the number of Coding Violations encountered by a SONET/SDH Path in a particular 15-minute interval in the past 24 hours.
sonetPathIntervalUASs	PerfIntervalCount	The counter associated with the number of Unavailable Seconds encountered by a Path in a particular 15-minute interval in the past 24 hours.
APS-MIB		
apsChanStatusTable		
apsChanSignalDegrades	Counter32	A count of Signal Degrade conditions. This condition occurs when the line Bit Error Rate exceeds the currently configured threshold.
apsChanSignalFailures	Counter32	A count of Signal Failure conditions that have been detected on the incoming signal. This condition occurs when a loss of signal, loss of frame, AIS-L or a Line bit error rate exceeding 10^-3 is detected on an incoming line.
apsChanSwitchovers	Counter32	The number of times this channel has switched to the protection line. When queried with index value apsChanNumber set to 0, which is the protection line, this object will return 0.
IMA-MIB (new in SN05)		
imaGroupIntervalTable		
imaGroupIntervalUnavailSecs	Gauge32	Count of one second intervals where the IMA Group Traffic State Machine is Down in one of the previous 96, individual 15 minute, intervals
imaGroupIntervalNeNumFailures	Gauge32	The number of times a near-end group failure (Config-Aborted, Insufficient-Links) has been reported in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalTable		
imaLinkIntervalImaViolations	Gauge32	ICP violations: count of errored, invalid or missing ICP cells, except during SES-IMA or UAS-IMA conditions, in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalOifAnomalies	Gauge32	The number of OIF anomalies, except during SES-IMA or UAS-IMA conditions, at the near-end in one of the previous 96, individual 15 minute, intervals. This is an optional attribute
imaLinkIntervalNeSevErroredSecs	Gauge32	Count of one second intervals containing >= 30% of the ICP cells counted as IV-IMAs, or one or more link defects (e. g., LOS, OOF/ LOF, AIS, or LCD), LIF defects, or LODS defects, except during UAS-IMA condition, in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalNeUnavailSecs	Gauge32	Count of unavailable seconds at near-end in one of the previous 96, individual 15 minute, intervals: unavailability begins at the onset of 10 contiguous SES-IMA and ends at the onset of 10 contiguous seconds with no SES-IMA
imaLinkIntervalNeTxUnusableSecs	Gauge32	Tx Unusable seconds: count of Unusable seconds at the near-end Tx LSM in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalNeRxUnusableSecs	Gauge32	Rx Unusable seconds: count of Unusable seconds at the near-end Rx LSM in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalNeTxNumFailures	Gauge32	The number of times a near-end transmit failure alarm condition has been entered on this link (i.e., some form of implementation specific transmit fault) in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalNeRxNumFailures	Gauge32	The number of times a near-end receive failure alarm condition has been entered on this link (i.e., LIF, LODS, RFI-IMA, Mis-Connected, or some form of implementation specific receive fault) in one of the previous 96, individual 15 minute, intervals
imaLinkIntervalTxStuffs	Gauge32	Count of stuff events inserted in the transmit direction in one of the previous 96, individual 15 minute, intervals. This is an optional attribute
imaLinkIntervalRxStuffs	Gauge32	Count of stuff events detected in the receive direction in one of the previous 96, individual 15 minute, intervals. This is an optional attribute

UEMG-PERFMON-MIB		
nnPmUtilOmIntervTable		This table contains history measurements of CPU, Ram, Flash and Channel Usage. Measurements in this table are rolling (peak and average values) of each 15 minute interval up to 24 hours old.
nnPmUtilIntervCpuPeak	Integer	Peak CPU Occupancy (as a percentage of usage)
nnPmUtilIntervCpuAvg	Integer	Average CPU Occupancy (as a percentage of usage)
nnPmUtilIntervRamPeak	Integer	Peak RAM Usage (as a percentage of usage)
nnPmUtilIntervRamAvg	Integer	Average RAM Usage (as a percentage of usage)
nnPmUtilIntervFlashPeak	Integer	Peak Flash Memory Usage (as a percentage of usage)
nnPmUtilIntervFlashAvg	Integer	Average Flash Memory Usage (as a percentage of usage)
nnPmUtilIntervChanPeak	Integer	Peak Channel Usage (as a percentage of usage)
nnPmUtilIntervChanAvg	Integer	Average Channel Usage (as a percentage of usage)
nnPmSnmpOmIntervTable		This table contains measurements of SNMP requests and events. Measurements in this table are rolling (peak and average values) of each 15 minute interval up to 24 hours old.
nnPmSnmpIntervReqPeak	Interger32	The Peak number of SNMP Requests/PDUs in the most Recent 15 mins. These are accumulated on 1-minute cycles.
nnPmSnmpIntervReqAvg	Interger32	The Avg number of SNMP Requests/PDUs in the most Recent 15 mins. These are accumulated on 1-minute cycles. Thus, the avg is the avg of the last 15x 1-minute cycles. Precision is tenths, thus 816 is 81.6
nnPmSnmpIntervNotifPeak	Interger32	The Peak number of SNMP Notifications in the most Recent 15 mins. These are accumulated on 1-minute cycles.
nnPmSnmpIntervNotifAvg	Interger32	The Avg number of SNMP Notifications sent in the most Recent 15 mins. These are accumulated on 1-minute cycles. Thus, the avg is the avg of the last 15x 1-minute cycles. Precision is tenths, thus 816 is 81.6
nnPmOvldRscIntervTable		
nnPmOvldRscIntervPduRatePeak	Interger32	Peak # received AAl5 PDUs per sec for this 15 minute interval
nnPmOvldRscIntervPduRateAvg	Interger32	Avg num recvd AAL5 PDUs per sec for this 15 minute interval
nnPmOvldRscIntervCbvMsgRPeak	NnPerfMonHundredths	Peak recvd conn request msgs per sec for this 15 minute interval
nnPmOvldRscIntervCbvMsgRAvg	NnPerfMonHundredths	Avg conn request msgs per sec for this 15 minute interval
nnPmOvldRscIntervConQDelPeak	NnPerfMonHundredths	Milliseconds...peak time a connRequest is pending in its queue for this 15 minute interval
nnPmOvldRscIntervConQDelAvg	NnPerfMonHundredths	Milliseconds...Avg time a connRequest is pending in its queue for this 15 minute interval
nnPmOvldRscIntervCpuUtilPeak	NnPerfMonPercent	Peak cpu occupancy for this 15 minute interval
nnPmOvldRscIntervCpuUtilAvg	NnPerfMonPercent	Avg cpu occupancy this 15 minute interval
nnPmOvldConnDenyIntervTable		
nnPmOvldConnDenyIntervCount	Interger32	Count of the number of Connection requests Denied for this 15 minute interval
NORTEL-UEMG-RELMSGING-MIB		
nnRelMsgSctpAssocOmCurrTable		
nnRelMsgSctpAscCurrClosed	Unsigned32	number of times that this association closed (both aborts and shutdowns)
nnRelMsgSctpAscCurrAbort	Unsigned32	number of times that this association aborted.
nnRelMsgSctpAssocOmIntervTable		
nnRelMsgSctpAscIntervClosed	Unsigned32	number of times that this association closed (both aborts and shutdowns)
nnRelMsgSctpAscIntervAbort	Unsigned32	number of times that this association aborted.
nnRelMsgSctpAscIntervOutPacks	Unsigned32	number of packets transmitted
nnRelMsgSctpAscIntervInPacks	Unsigned32	number of packets received, this association
nnRelMsgSctpAscIntervDiscPacks	Unsigned32	number of packets discarded by this association.
nnRelMsgSctpAscIntervRetranPacks	Unsigned32	number of packets retransmitted by this association, this interval
nnRelMsgSctpAscIntervT1expires	Unsigned32	number of T1 Expires
nnRelMsgSctpAscIntervT2expires	Unsigned32	number of T2 expires.
nnRelMsgSctpAscIntervT3expires	Unsigned32	number of T3 expires
nnRelMsgSctpAscIntervCongCount	Unsigned32	number of times this assoc entered congestion.

nnRelMsgSctpAscIntervCongCleared	Unsigned32	number of times congestion cleared by audit.
NORTEL-UEMG-GIGE_mib		
nnGLinkOmIntervTable		
nnGLinkIntervESs	Unsigned32	history, nth interval Errored Seconds
nnGLinkIntervSESs	Unsigned32	history, nth interval Severely Errored Seconds
nnGLinkIntervUASs	Unsigned32	history, nth interval Unavailable Seconds
nnGLinkIntervOPT	Unsigned32	history, nth interval Optical Transmit Current
nnGLinkIntervOPR	Unsigned32	history, nth interval Optical Power Receive
nnGLinkIntervTBC	Unsigned32	history, nth interval Transmit Bus Current
nnGLinkIntervVCC	Unsigned32	history, nth interval Voltage
nnGLinkIntervTEMP	Unsigned32	history, nth interval Temperature
nnGLinkIntervTxFifoOverruns	Counter64	history, nth interval Transmit Fifo Overruns
nnGLinkIntervTxFifoUnderruns	Counter64	history, nth interval Transmit Fifo Underruns
nnGLinkIntervTxBytesOverflow	Unsigned32	history, nth interval Transmit Bytes, Overflow
nnGLinkIntervTxBytes	Counter64	history, nth interval Transmit Bytes
nnGLinkIntervRxFcsFail	Counter64	history, nth interval Receive Fcs Failures
nnGLinkIntervRxLenTypeFail	Counter64	history, nth interval Receive LEN Type Failures
nnGLinkIntervRxGoodPause	Counter64	history, nth interval Receive Good Pause
nnGLinkIntervRxBadOpCntlFrames	Counter64	history, nth interval Receive Bad Opcode Control Frames
nnGLinkIntervRxControlFrames	Counter64	history, nth interval Receive Control Frames
Remote Network Monitoring MIB		
etherHistoryTable		
etherHistoryDropEvents	Counter32	The total number of events in which packets were dropped by the probe due to lack of resources during this sampling interval. Note that this numbe is not necessarily the number of packets dropped, it is just the number of times this condition has been detected.
etherHistoryBroadcastPkts	Counter32	The number of good packets received during this sampling interval that were directed to the broadcast address.
etherHistoryMulticastPkts	Counter32	The number of good packets received during this sampling interval that were directed to a multicast address. Note that this number does not include packets addressed to the broadcast address.
etherHistoryCRCAlignErrors	Counter32	The number of packets received during this sampling interval that had a length (excluding framing bits but including FCS octets) between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherHistoryUndersizePkts	Counter32	The number of packets received during this sampling interval that were less than 64 octets long (excluding framing bits but including FCS octets) and were otherwise well formed.
etherHistoryOversizePkts	Counter32	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets) but were otherwise well formed.
etherHistoryFragments	Counter32	The total number of packets received during this sampling interval that were less than 64 octets in length (excluding framing bits but including FCS octets) had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
etherHistoryJabbers	Counter32	The number of packets received during this sampling interval that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)
etherHistoryCollisions	Counter32	The best estimate of the total number of collisions on this Ethernet segment during this sampling interval.
etherHistoryUtilization	Counter32	The best estimate of the mean physical layer network utilization on this interface during this sampling interval, in hundredths of a percent.
HC-RMON-MIB		
etherHistoryHighCapacityTable		

etherHistoryHighCapacityOverflowPkts	Gauge32	The number of times the associated etherHistoryPkts Gauge overflowed during this sampling interval.
etherHistoryHighCapacityPkts	CounterBasedGauge64	The total number of packets (including bad packets, broadcast packets, and multicast packets) received during this sampling interval.
etherHistoryHighCapacityOverflowOctets	Gauge32	The number of times the associated etherHistoryOctets counter has overflowed during this sampling interval.
etherHistoryHighCapacityOctets	CounterBasedGauge64	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets) during this sampling interval.
NORTEL-UEMG-IPSEC-MIB		
nnIpsecOmIntervalTable		
nnIpsecOmIntervalPacketsTx	Integer32	Number of Transmitted Packets this 15min interval
nnIpsecOmIntervalPacketsRx	Integer32	Number of Received Packets this 15min interval
nnIpsecOmIntervalPacketsDiscardedOut	Integer32	Number of Dropped Outbound Packets this 15min interval
nnIpsecOmIntervalPacketsDiscardedIn	Integer32	Number of Dropped Inbound Packets this 15min interval

Appendix C: VoA/IP MSS15000, MG15000 and MDM Alarm Log Summary

1. Introduction

This document provides a list of Multiservice Switch 15000 (MSS15000), Media Gateway 15000 (MG15000) (formerly known as PVG) and Multiservice Data Manager (MDM) alarm logs applicable to up to Succession SN08 for Voice over ATM (VOA) and Voice over IP (VOIP) solutions.

The purpose of this document includes:

- It provides a Carrier VOIP customer (and more specifically an OSS Fault application writer) a summarized subset of the possible alarms that can appear when MSS15000/MG15000 and MDM are configured for the Carrier VOIP application. The descriptions of the alarms are found in [6] and [3].
- When configured to receive MSS15000/MG15000/MDM Alarm logs in SCC2 format from the Supernode Data Manager (SDM), it also provides the mapping information needed to interpret the SCC2 format.
- It is also input to solution-level OSS Guide information which is in progress of being delivered to provide this information in the FCAPS-based solution documentation.

2. SCC2 Log Format

The SCC2 log report for MSS15000, MG15000, and MDM alarms comprises a one line header, followed by seven lines of body text, as per the following example:

```
 37 PPEM300 8169 TBL
      time: 2002 01 11 15 37 06
      event: clear
      compId: EM P15KF LP 7 SONET 3
      severity: cleared
      faultCode: 70115201
      alarmType: communications
      commentData: Loss of frame condition has been cleared.
```

The header is of format:

aabbcdddeeefgghhijjjj

Each field, as applicable for MSS15000/MG15000 and MDM alarms, is described in Table 1.

Table 1 MSS15000/MG15000 and MDM SCC2 Header Field Description

Field	Description	Applicable Log Values
aa	Alarm severity MSS15000/MG15000/MDM alarm log severity	"*C" = critical alarm "**" = major alarm "* " = minor and warning and indeterminate alarm " " = clear alarm Two characters, left justified, padded with blanks.

Field	Description	Applicable Log Values
bb	Minute indicator Two numeric character indicator representing the minutes after the hour. Generated by SDM at time SDM receives the alarm log from MDM.	Ranges from 00 to 59, right justified, padded with zeros.
c	single space	" "
dddd	Log Name Assigned by SDM. Based upon the first four digits ("Index Group") of the eight-digit MSS15000/MG15000 or MDM alarm identifier.	Four characters, left justified, padded with blanks. "CA " for index group 0000. "PPEM" for index groups beginning with 70xx and some fault codes in group 0999. "MDM " for index groups beginning with 30xx and some fault codes in group 0999.
eee	Log Number Three numeric characters representing the MSS15000/MG15000 or MDM Alarm Type. Note that the Alarm Type "debug" is not translated as a fault, but rather as information log.	"300" = communications "301" = quality of service "302" = processing "303" = equipment "304" = environmental "305" = security "306" = operator "307" = unknown
f	A single space for all MSS15000/MG15000 and MDM alarm logs.	" "
gg	Global Sequence Number Generated by SDM. Two numeric characters, incremented by SDM upon receipt of every alarm log.	Ranges from 00 to 99, right justified, padded with zeros.
hh	Device Sequence Number Generated by SDM. Two numeric characters, incremented by SDM upon receipt of every device specific alarm log from MDM (originated by MSS15000/MG15000 or MDM).	Ranges from 00 to 99, right justified, padded with zeros.
i	single space	" "
jjjj	Event Type Assigned by SDM. String assigned for all MSS15000/MG15000 and MDM alarm logs.	"TBL " Four characters, left justified, padded with blanks.
Lines 2, 3, 4, 5, 6, 7, 8	Body Text Seven textual lines, each of form <AlarmFieldName>: <AlarmFieldValue>	"time: " "event: " "compId: " "severity: " "faultCode: " "alarmType: " "commentData: " Comment data is truncated so that entire log does not exceed 900 bytes.

3. MSS15000/MG15000 Alarm Logs

Table 2 presents the list of MSS15000 and MG15000 set/clear alarm logs that are applicable for Carrier VOIP.

Table 2 does not explicitly state all MSS15000/MG15000 clear alarm logs that correspond to each set. The SCC2 header for the clear differs from its corresponding set by only the first two characters. The characters “aa” are replaced by “ “ (two spaces). This format is presented in Table 1.

The MSS15000/MG15000 alarm identifier consists of an eight-digit number identifying the alarm. The first four digits comprise the **Index Group**, which represents logical groupings of alarms. The last four digits are the **SubIndex**, which is an identifier within each index group.

Component Name indicates the managed object against which the alarm Log is generated. This table contains the CLI format of a component name. The “compId” field in SCC2 format contains this information (with the module’s <nodename> pre-pended). Also, “compId” follows the MDM API-style format (with component type and instance separated by a space instead of a slash, and ‘$’ appearing in place of a null instance value). Variables (usually instance value ranges) are denoted by <> and the reader should reference the Alarms NTP’s [3] and [6] for further information.

Table 2 MSS15000 Set/Clear Alarms Supported for Succession

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
0000	OSI administrative state changes, general engineering and memory alarms, internal software error detected, etc.				
	This alarm can apply to many MSS15000 components.		0000		bb CA eee gghh TBL where: eee = 302, 303, 306
	This alarm can apply to many MSS15000 components.		1000		aabb CA eee gghh TBL where: aa = “*C”, “**”, “* ” eee = 300, 306
	This alarm can apply to many MSS15000 components.		1001		aabb CA 303 gghh TBL where: aa = “*C”, “**”, “* ”
	This alarm can apply to many MSS15000 components.		3000		aabb CA eee gghh TBL where: aa = “*C”, “**”, “* ” eee = 300, 302
	This alarm can apply to many MSS15000 components.		3001		aabb CA 302 gghh TBL where: aa = “*C”, “**”, “* ”
			3002		
7000	Provisioning alarms. These alarms apply to failures resulting from provisioning attempts. e.g., loading a provisioning file has failed. Card instance range (<n>): 0-15 LP instance range (<m>): 0-15				

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	Prov		0007		aabb PPEM306 gghh TBL where: aa = “*C”, “**”, “* ”
	This alarm can apply to many MSS15000 components.		0010		* bb PPEM302 gghh TBL
	Prov Migration		0033		aabb PPEM306 gghh TBL where: aa = “*C”, “* ”
	Prov		0036		aabb PPEM301 gghh TBL where: aa = “**”, “* “
	Prov		0037		*Cbb PPEM301 gghh TBL
	Prov		0038		* bb PPEM301 gghh TBL
	Prov		0040		**bb PPEM302 gghh TBL
	Provisioning Patch		0041		* bb PPEM306 gghh TBL or *Cbb PPEM306 gghh TBL
	Prov CriticalAttributeActivation		0042		* bb PPEM306 gghh TBL for warning/clear or *Cbb PPEM306 gghh TBL for set/clear
	Prov ActivationMode		0043		* bb PPEM306 gghh TBL
	Shelf Card/<x> Lp/<m>		0044		*Cbb PPEM302 gghh TBL
7002	Backplane control system alarms; e.g., communication failure between a card and the backplane. Note: FabricCard instance range (<i>): X, Y Card instance range (<n>): 0-15				
	Shelf FabricCard/<i>		0002		**bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0003		*Cbb PPEM304 gghh TBL
	Shelf FabricCard/<i>		0004		*Cbb PPEM304 gghh TBL
	Shelf FabricCard/<i>		0005		**bb PPEM302 gghh TBL
	Shelf FabricCard/<i>		0006		**bb PPEM302 gghh TBL
	Shelf FabricCard/<i>		0007		**bb PPEM302 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	Shelf Card/<n>		0008		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0009		* bb PPEM303 gghh TBL
7003	Data collection system alarms; e.g., an alarm or log queue size has exceeded a threshold. Collector instance range (<t>): accounting, alarm, log, debug, scn, trap, stats, rtStats, appl Agent instance range (<n>): 0-15 LP instance range (<n>): 0-15				
	Collector/<t> Agent/<n>		0001		**bb PPEM301 gghh TBL
	Collector/<t> Spooler		0002		**bb PPEM302 gghh TBL
	Collector/<t> Spooler		0003		* bb PPEM301 gghh TBL
	LP/<n> Eng AAList		0007		**bb PPEM301 gghh TBL
7006	Radius security alarms.				
	Ac Radius		0100		*Cbb PPEM305 gghh TBL
7008	File system alarms. Disk instance range (<n>): 0-1				
	FileSystem		1001		**bb PPEM302 gghh TBL
	FileSystem		1002		*Cbb PPEM302 gghh TBL
	FileSystem		1004		*Cbb PPEM303 gghh TBL
	FileSystem		1005		* bb PPEM303 gghh TBL
	FileSystem		1006		**bb PPEM302 gghh TBL
	FileSystem Disk/<n>		1008		**bb PPEM303 gghh TBL
			1009		
			1010		
			1011		
	FileSystem		1019		* bb PPEM303 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
7011	Port management system and Automatic Protection Switching alarms. LP instance range (<n>): 0-15 Port types (<type>): Sonet, EDS1, DS3, BridgedSonet(Bso), Ethernet, Sdh Sonet instance range (<n2>): 0-15 (16-port); 0-3 (4-port) EDS1 instance range (<n2>): 0-1 IMA instance range (<n3>): 0-13 LK instance range (<n4>): 0-31 DS3 instance range (<n2>): 0-3 (4-port); 0-11 (12-port) DS1 instance range (<n3>): 1-28 Ethernet instance range (<n2>): 0-3 LAPS instance range (<n>): 0-15999 Chan instance range (<n4>): 0-23 Bso instance range (<n2>): 0-15 Pbg instance range (<n>): 0-15999 Sdh instance range (<n2>): 0-n, where n is 1 less than the number of ports Sts instance range (<n2>): 0-11 Lag instance range (<y>): 0-7 Lag link instance range (<z>): 0-31				
	LP/<n> DS3/<n2> IMA <n3>		1100		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> IMA/<n3>… …LK/<n4>		1200		*Cbb PPEM300 gghh TBL
			1210		
			1211		
			1212		
			1213		
			1214		
			1215		
			1216		
	LP/<n> Lag/<y>		1500		*Cbb PPEM300 gghh TBL
	LP/<n> Lag/<y> Link/<z>		1501		*Cbb PPEM300 gghh TBL
	LP/<n> <type>/<n2>		2000		*Cbb PPEM303 gghh TBL
	LP/0 EDS1/<n2> LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/0 Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5000		*Cbb PPEM300 gghh TBL
	LP/0 EDS1/<n2> LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/0 Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5001		* bb PPEM300 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	LP/0 EDS1/<n2> Lp/<n> Sdh/0 Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5002		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5003		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5004		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5005		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} E1 Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1		5006		**bb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3> Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} DS1 Lp/<n> Sdh/0 Vc4/0 Vc12/{1-3,1-7,1-3} E1		5010		* bb PPEM300 gghh TBL
	LP/<n> DS3/<n2> DS1/<n3>		5011		* bb PPEM300 gghh TBL
	LP/0 EDS1/<n2>		5050		aabb PPEM303 gghh TBL where: aa = “*C”, “* “
	LP/<n> DS3/<n2>		5100		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5101		*Cbb PPEM300 gghh TBL
			5102		
			5103		
			5104		
	LP/<n> DS3/<n2>		5105		* bb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5110		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5111		* bb PPEM300 gghh

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
			5120		TBL
			5121		
			5122		
	LP/<n> Sonet/<n2> LP/<n> Sdh/<n2>		5200		*Cbb PPEM300 gghh TBL
			5201		
			5202		
	LP/<n> Sonet/<n2> LP/<n> Sdh/<n2>		5203		* bb PPEM300 gghh TBL
			5204		
			5210		
			5211		
	LP/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5250		*Cbb PPEM300 gghh TBL
			5251		
	LP/<n> Sonet/<n2> Sts/<n2> Lp/<n> sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5252		* bb PPEM300 gghh TBL
	LP/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5253		*Cbb PPEM300 gghh TBL
	LP/<n> Sonet/<n2> Sts/0 Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/0 LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5254		*Cbb PPEM300 gghh TBL
	Lp/<n> Sonet/<n2> Path/<n2> Lp/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sonet/<n2> Vc4/<n2> Lp/<n> Sdh/<n2> Path/0 Lp/<n> Sdh/<n2> Sts/0 Lp/<n> Sdh/<n2> Vc4/0 LAPS/<n> Path/0 LAPS/<n> Sts/0 LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5255		*Cbb PPEM300 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	Lp/<n> Sonet/<n2> Sts/<n2> Lp/<n> Sdh/<n2> Vc4/0 Lp/<num1> Sdh/<n2> Vc4/0 Vc12/{1-3, 1-7, 1-3} Laps/<n> Sts/<num3> Laps/<n> Sdh/<num2> Vc4/0 Laps/<n> Sdh/<n2> Vc4/0 Vc12/{1-3, 1-7, 1-3} Pbg/<n> Sts/{0-11}		5256		*Cbb PPEM300 gghh TBL
	LP/<n> Sonet/<n2> Sts/<n2> LP/<n> Sdh/<n2> Vc4/0 LAPS/<n> Sts/<n2> LAPS/<n> Vc4/0 Pbg/<n> Sts/0		5260 5261		* bb PPEM300 gghh TBL
	LAPS/<n>		5270		**bb PPEM300 gghh TBL
	LAPS/<n>		5271		* bb PPEM300 gghh TBL
	LAPS/<n>		5272		* bb PPEM300 gghh TBL
	LAPS/<n>		5273		* bb PPEM300 gghh TBL
	LAPS/n		5274		* bb PPEM300 gghh TBL
	LAPS/<n>		5275		*Cbb PPEM300 gghh TBL
	LAPS/<n> CrossConnect		5281		*Cbb PPEM300 gghh TBL
	LP/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} LAPS/<n> Vc4/0 Vc12//{1-3,1-7,1-3} LAPS/<n> Sts/<n2> Vt1dot5/{1-7,1-4}		5290 5291 5292 5293 5294		*Cbb PPEM303 gghh TBL
	LP/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} LAPS/<n> Vc4/0 Vc12//{1-3,1-7,1-3} LAPS/<n> Sts/<n2> Vt1dot5/{1-7,1-4}		5295 5296		*Cbb PPEM303 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	LP/<n> Sdh/<n2> Vc4/0 Vc12/{1-3,1-7,1-3} Lp/<n> Sonet/<n2> Sts/<n2> Vt1dot5/{1-7,1-4} LAPS/<n> Vc4/0 Vc12//{1-3,1-7,1-3} LAPS/<n> Sts/<n2> Vt1dot5/{1-7,1-4}		5297		*Cbb PPEM303/6 gghh TBL
	LP/<n> Ethernet/<n2> LP/<n> Ethernet/<n2> LP/<n> Ethernet/<n2> LP/<n> Ethernet/<n2> LP/<n> Ethernet/<n2> OpticalModule		5400		*Cbb PPEM300 gghh TBL
			5401		*Cbb PPEM300 gghh TBL
			5402		*Cbb PPEM300 gghh TBL
			5403		*Cbb PPEM300 gghh TBL
			5480		**bb PPEM300 gghh TBL
	LP/<n> Sonet/<n2> LP/<n> Sonet/<n2> Sts/0 LAPS/<n> Sts/0 LP/<n> DS3/<n2> LP/<n> DS3/<n2> DS1/<n3> LP/<n> DS3/<n2> DS1/<n3> Chan/<n4> Pbg/<n> Sts/0		5501		*Cbb PPEM300 gghh TBL
	LP/<n> DS3/<n2>		5601		* bb PPEM300 gghh TBL
			5602		
	LP/<n> DS3/<n2>		5603		**bb PPEM300 gghh TBL
			5604		
7012	Processor control system alarms. LP instance range (<n>): 0-15 Card instance range (<n>): 0-15 FabricCard instance range (<i>): X, Y				
	Shelf		0050		**bb PPEM303 gghh TBL
	Shelf		0051		aabb PPEM303 gghh TBL where: aa = “*C”, “**”
	Shelf Shelf FabricCard/<i>		0052		**bb PPEM303 gghh TBL
	Shelf		0053		**bb PPEM303 gghh TBL
	Shelf		0055		aabb PPEM303 gghh TBL where: aa = “**”, “* ”
	Shelf		0056		* bb PPEM303 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	Shelf		0057		**bb PPEM303 gghh TBL
			0058		
	Shelf		0059		*Cbb PPEM304 gghh TBL
	Shelf Card/<n>		0100		aabb PPEM303 gghh TBL where: aa = "*C", "* "
	Shelf Card/<n>		0103		**bb PPEM303 gghh TBL
			0104		
	Shelf Card/<n>		0105		* bb PPEM306 gghh TBL
	LP/<n>		0200		*Cbb PPEM302 gghh TBL
	LP/<n>		0202		* bb PPEM306 gghh TBL
	Shelf Card/<n> SpServ		0301		* bb PPEM302 gghh TBL
7013	Message block usage alarms. LP instance range (<n>): 0-15				
	LP/<n>		0000		* bb PPEM301 gghh TBL
	LP/<n>		0001		**bb PPEM301 gghh TBL
	LP/<n>		0002		* bb PPEM301 gghh TBL
			0003		
			0004		
			0005		
			0011		
	LP/<n>		0021		**bb PPEM301 gghh TBL
	LP/<n>		0022		* bb PPEM301 gghh TBL
7014	Memory management alarms				
	LP/<n>		0000		* bb PPEM301 gghh TBL
	LP/<n>		0001		**bb PPEM301 gghh TBL
7015	Network time-of-day (TOD) synchronization alarms. Server instance range (<n>): 1-10				
	Time		0000		**bb PPEM304 gghh TBL
			0002		
	Time Server/<n>		0010		* bb PPEM300 gghh TBL
			0011		
	Time Server/<n>		0012		* bb PPEM300 gghh TBL
7017	Network clock synchronization alarms				
	NS		1000		* bb PPEM300 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
7021	Internet protocol alarms. For Succession VOA, the IP stack is used only for network management connectivity purposes. For VOIP VR is used to connect to IP network. More than 1 VR may be provisioned in this configuration. VR instance range (<i>): any string, but often specified simply as a digit (e.g., "0") Cache instance range (<n>): 0-15 Name of the vrf (<y>) LP number (<lpnum>): 0-15 IP address (<ipaddress>): address of the local IpLogicalInterface Protocol Port Id (<ppId>) VirtualIfEntry identifier (<virtIfId>)				
	Vr/<i> Ip Cache/<n>		0006		**bb PPEM302 gghh TBL
	Vr/<i> Ip Cpp IsolatedDa/<ipaddress>, <lpnum> Rtr/<i> Cpp IsolatedDa/<ipaddress>, <lpnum> Rtr/<i> Vrf/<y> Cpp IsolatedDa/<ipaddress>, <lpnum>		0013 0014		* bb PPEM305 gghh TBL **bb PPEM305 gghh TBL
	Vr/<i> Pp/<ppId> IpPort logicalIf/<ipaddress> OspfIf Rtr/<i> Interface/<ipaddress> OspfIf		1002		**bb PPEM305 gghh TBL
	Vr/<i> Ip Ospf VirtIfEntry/<virtIfId>		1003		**bb PPEM305 gghh TBL
	VR/<i> Ip OSPF		1017		* bb PPEM305 gghh TBL
7026	LAN port management system alarms. For Succession VOA, the LAN port management system is used only for network management connectivity purposes Same alarms are used for VOIP.				
	LP/0 OamEnet/0		3000		*Cbb PPEMeee gghh TBL where: eee = 300, 303
	LP/0 OamEnet/0		3005		* bb PPEMeee gghh TBL where: eee = 300, 303
7039	ATM Core alarms. AtmIf instance range (<n>): 1-4095 Vcc instance range (<n2.n3>): n2 is VPI; n3 is VCI				
	Atmif/<n>		1000		* bb PPEM300 gghh TBL
	Atmif/<n>, AtmIf/<n> Ca Cbr/0,		1001 1002		* bb PPEM301 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	AtmIf/<n> Ca rtVbr/0, AtmIf/<n> Ca nrtVbr/0, AtmIf/<n> Ca Ubr/0		1003 1004		
	Atmif/<n> Vcc/<n2.n3>		2000 2003		**bb PPEM302 gghh TBL
	Atmif/<n> Vpt/<n2>		3000		* bb PPEM300 gghh TBL
	Atmif/<n>		4001		**bb PPEM300 gghh TBL
	Atmif/<n>		5000		*Cbb PPEM300 gghh TBL
7041	ATM Networking alarms. AtmIf instance range (<n>): 1-4095 Vpt instance range (<n2>): 0-4095 CfgNode instance range (<n>): 0-104				
	Atmif/<n> Uni Ilmi		0050		**bb PPEMeee gghh TBL where: eee = 300, 303
	AtmIf/<n> Uni Ilmi		0052		*Cbb PPEM300 gghh TBL
	Atmif/<n> Uni Sig Atmif/<n> Pnni Sig		0150		**bb PPEM300 gghh TBL
	Atmif/<n> Uni Sig Atmif/<n> Pnni Sig Atmif/<n> Uni Ilmi Atmif/<n> Pnni Rcc		0200		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0250		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0253		**bb PPEM300 gghh TBL
	Artg Pnni		0301		**bb PPEM300 gghh TBL
	Artg Pnni CfgNode<n> Rcc		0302		**bb PPEM300 gghh TBL
	Atmif/<n> Uni Atmif/<n> Pnni		0400		* bb PPEM300 gghh TBL
	Atmif/<n>		0401		**bb PPEM30? gghh TBL
	Atmif/<n> Uni Atmif/<n> Pnni		0500		* bb PPEM300 gghh TBL
	Atmif/<n> Uni Atmif/<n> Pnni		0600 0601		* bb PPEM302 gghh TBL
	Artg Pnni CfgNode /<n>		0700		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0701		**bb PPEM300 gghh TBL
	Artg Pnni CfgNode /<n>		0703		* bb PPEM300 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
7042	Circuit Emulation Service (CES) alarms. Aal1Ces instance range (<n>) : 1-16383				
	Aal1Ces/<n>		0001		**bb PPEM301 gghh TBL
	Aal1Ces/<n>		0002		**bb PPEM302 gghh TBL
	Aal1Ces/<n>		0003		**bb PPEM300 gghh TBL
7054	Sparing panel subsystem alarms. Card instance range (<n>): 0-15				
	Shelf Card/<n>		0100		**bb PPEM303 gghh TBL
			0101		
			0102		
			0103		
			0104		
			0105		
7056	Voice Services Processor (VSP) / Narrowband Service Trunk over ATM (Nsta) This group is specific to MG15000 application (e.g. severe failure of the VSP card) Lp instance range (<x>): 0-15 PModule instance range (<y>): 1-24 PBlock instance range (<z>): 1-2 NSTA instance range (<i>): 0-15999 GigE instance range (<m>): 0-1 Control instance range (<n>): mg or sg Conn instance range (<l>): 0-128 Brag instance range (<d>): 0-159999 Q921 instance range (<r>): 1-31 LapV5 instance value (<w>): 15, 16, 31 Tag instance range (<u>): 0-16777215 AtmTConn instance range (<h>): 1-2700 (max 4094) dBrag instance range (<t>): 0-127 BragS instance range (<k>): 0-15 CasDefn instance range (<z>): 0-24 Security policy database name (<spd_name>): string				
	Lp/<x> Vsp PModule/<y>		0002		** bb PPEM306 gghh TBL
	Lp/<x> Vsp PModule/<y> PBlock/<z>		0003		*Cbb PPEM303 gghh TBL
	Lp/<x> Vsp GigE/<m>		0500		** bb PPEM300 gghh TBL
			0501		
			0502		
	Nsta/<i> Conn/<l> Nsta/<i> Vgs AtmTConn/<h>		1000		**bb PEM300 gghh TBL
	Nsta/<l> Vgs		1200		* bb PPEM300 gghh TBL
	Nsta/<i> Vgs IpMConn		1201		** bb PPEM300 gghh TBL

MSS15000 Index Group	Component Name	MSS15000/MG15000 configuration (N/A)	MSS15000 SubIndex	Importance Category (N/A)	SCC2 Header
	Nsta/<i> Vgs Control/<n> Mediagateway Nsta/<i> Vgs Control/<n> Signalingateway		1202		** bb PPEM300 gghh TBL
	Nsta/<i> Vgs Control/<n> MediaGataway Aap Nsta/<i> Vgs Control/<n> Signalinggateway Aap Nsta/<i>Vgs Control/<n> SpvcAp Nsta/<i> Vgs IpMConn Aap Nsta/<i> Vgs IpMConn SpvcAp Nsta/<i> Vgs AtmTConn/<h> Aap Nsta/<I> Vgs AtmTConn/<h> Aap		1203		** bb PPEM300 gghh TBL
	Nsta/<i> Vgs		1204		* bb PPEM302 gghh TBL
	Nsta/<i> Vgs CasDefn/<z>		1208		* bb PPEM302 gghh TBL
	Lp/<x> Vsp PModule/<y>		1209		* bb PPEM303 gghh TBL
	Nsta/<x> Vgs Brag/<d> Q921/<r> Nsta/<i> Vgs BragS/<k> dBrag/<t> Q921		1210		** bb PPEM300 gghh TBL
	Nsta/<x> Vgs Iua		1211		** bb PPEM300 gghh TBL
	Nsta/<x> Vgs Brag/<d> V5Link LapV5/<w>		1213		** bb PPEM300 gghh TBL
	Nsta/<x> Vgs Tag/<u>		1217		*Cbb PPEM302 gghh TBL
	Nsta/<x> Vgs Ctrl/<n> Spd/<spd_name> IkePolicy/1		1219		** bb PPEM300 gghh TBL
7060	ATM and Frame Resource Control alarms. LP instance range (<n>): 0-15 Aqm instance range (<n2>): 0-3				
	LP/<n> Eng Fcrc		1000		**bb PPEM300 gghh TBL
	LP/<n> Eng Arc Aqm/<n2>		1100		* bb PPEM300 gghh TBL
7082	Routine Exercise alarms.				
	Rex		0001		* bb PPEM302 gghh TBL
	Rex		0002		* bb PPEM306 gghh TBL

The following table specifies the alarms where field “event” has the value “message”. There won’t be a “clear” for these, but some action may still be required (e.g., security issue).

Table 3 MSS15000 Message Alarms Supported for Succession VOA/VOIP

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
0000	OSI administrative state changes, general engineering and memory alarms, etc.				
	These alarms can apply to many MSS15000 components. Often, it is: EM/<nodename>		9000		* bb CA eee gghh TBL where: eee = 300, 302
			9001		
			9002		
			9003		
7000	Provisioning alarms. These alarms apply to failures resulting from provisioning attempts. e.g., loading a provisioning file has failed.				
	Prov		0001		*Cbb PPEM302 gghh TBL
	Prov		0002		* bb PPEM302 gghh TBL
	Prov		0003		*Cbb PPEM302 gghh TBL
	Prov		0004		*Cbb PPEM302 gghh TBL
	Prov		0005		* bb PPEM302 gghh TBL
	Prov		0006		*Cbb PPEM302 gghh TBL
	Prov		0008		**bb PPEM302 gghh TBL
	Prov		0009		**bb PPEM302 gghh TBL
	Prov		0012		* bb PPEM306 gghh TBL
	Prov		0013		* bb PPEM302 gghh TBL
	Prov		0015		* bb PPEM302 gghh TBL
	Prov		0016		* bb PPEM30? gghh TBL
	Prov		0029		* bb PPEM30? gghh TBL
	Prov		0030		* bb PPEM30? gghh TBL
	Prov		0031		* bb PPEM302 gghh TBL
	Prov		0032		* bb PPEM30? gghh TBL
	This alarm can apply to many MSS15000 components.		0035		* bb PPEM307 gghh TBL
	Prov		0039		* bb PPEM306 gghh TBL

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
7002	Backplane control system alarms; e.g., communication failure between a card and the backplane. Note: Card instance range (<n>): 0-15 FabricCard instance range (<i>): X,Y				
	Shelf FabricCard/<i>		0010		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0012		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0013		* bb PPEM303 gghh TBL
	Shelf FabricCard/<i>		0014		* bb PPEM303 gghh TBL
	Shelf Card/<n>		1000		*Cbb PPEM303 gghh TBL
7003	Data collection system alarms; e.g., an alarm or log queue size has exceeded a threshold. Collector instance range (<t>): accounting, alarm, log, debug, scn, trap, stats, rtstats, appl Agent instance range (<n>): 0-15				
	Collector/<t> Agent/<n>		0004		* bb PPEM301 gghh TBL
	Collector/log Spooler		0008		* bb PPEM306 gghh TBL
7006	Network Management Interface system alarms and Radius security alarms. Management Interface type (<type>): Fmip, Ftp, Local, Telnet Session instance range (<n>): 1-35 (Fmip); 1-16 (Ftp); 1-2 (Local); 1-16 (Telnet) Radius Server instance range (<m>): 0-1				
	Nmis <type>		0001		**bb PPEM305 gghh TBL
	Nmis <type> Session/<n>		0002		* bb PPEM305 gghh TBL
	Nmis <type> Session/<n>		0003		**bb PPEM300 gghh TBL
	Nmis Ftp		0005		**bb PPEM302 gghh TBL
	Nmis Fmip		0006		**bb PPEM305 gghh TBL
	Nmis <type> Session/<n>		0007		**bb PPEM300 gghh TBL
	Nmis Fmip		0008		**bb PPEM300 gghh TBL
	Ac		0009		* bb PPEM300 gghh TBL or * bb PPEM305 gghh TBL
	Ac Radius Server/<m>		0101		**bb PPEM305 gghh TBL
	Ac Radius Server/<m>		0102		**bb PPEM305 gghh TBL
	Ac Radius		0103		**bb PPEM305 gghh TBL
	Ac Radius		0104		**bb PPEM305 gghh TBL

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
	Ac Radius Server/<m>		0105		**bb PPEM305 gghh TBL
7008	File system alarms. Disk instance range (<n>): 0-1 Card instance range (<x>): 0-1				
	FileSystem		1003		**bb PPEM302 gghh TBL
	FileSystem Disk/<n>		1012		* bb PPEM303 gghh TBL
	FileSystem Disk/<n>		1013		**bb PPEM303 gghh TBL
	FileSystem Disk/<n>		1014		**bb PPEM307 gghh TBL
	FileSystem Disk/<n>		1015		* bb PPEM307 gghh TBL
	FileSystem Disk/<n>		1016		* bb PPEM307 gghh TBL
	FileSystem Disk/<n>		1018		* bb PPEM303 gghh TBL
	FileSystem		1020		* bb PPEM303 gghh TBL
	Shelf Card/<x>		1021		**bb PPEM303 gghh TBL
7011	Port management system and Automatic Protection Switching alarms. LP instance range (<n>): 0-15 Port types (<type>): Sonet, DS3 Sonet instance range (<n2>): 0-15 (16-port); 0-3 (4-port) DS3 instance range (<n2>): 0-11 (12-port); 0-3 (4-port)				
	LP/<n> <type>/<n2>		2002		**bb PPEM303 gghh TBL
	LP/<n> DS3/<n2>		5112		* bb PPEM300 gghh TBL
	LP/<n> <type>/<n2>		8000		* bb PPEM300 gghh TBL
7012	Processor control system alarms. LP instance range (<n>): 0-15 Card instance range (<n>): 0-15				
	Shelf		0054		**bb PPEM303 gghh TBL
	Shelf Card/<n>		0101		* bb PPEM303 gghh TBL
	Shelf Card/<n>		0102		* bb PPEM301 gghh TBL
	Shelf Card/<n>		0151		**bb PPEM302 gghh TBL
			0152		
			0153		
	Shelf Card/<n>		0154		**bb PPEM303 gghh TBL
			0155		
			0156		

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
	LP/<n>		0201		* bb PPEM306 gghh TBL
	LP/0		0203		* bb PPEM303 gghh TBL
	LP/<n>		0204		* bb PPEM306 gghh TBL
	Shelf Card/<n> SpServ		0300		aabb PPEMeee gghh TBL where: aa = "*C", "* " eee=any
7015	Network time-of-day (TOD) synchronization alarms.				
	Time		0001		* bb PPEMeee gghh TBL eee=304, 306, 307
7017	Network clock synchronization alarms.				
	Ns		1001		* bb PPEM301 gghh TBL
7021	Internet protocol alarms. For Succession VOA, the IP stack is used only for network management connectivity purposes. For VOIP VR is used to connect to IP network. OSPF and IP static Routes can be used. More than 1 VR can be provisioned. VR instance range (<i>): any string, but often specified simply as a digit (e.g., "0")				
	VR/<i> Ip		0000		* bb PPEM302 gghh TBL
	VR/<i> Ip OSPF		1000		
	VR/<i> Ip OSPF		1001		
	VR/<i> Ip OSPF		1011		
	VR/<i> Ip OSPF		1016		**bb PPEM302 gghh TBL
	VR/<i> Ip OSPF		1100		* bb PPEM300 gghh TBL
	Vr/<i>		1021		**bb PPEM302 gghh TBL
	Vr/<i> Ip Ospf		1101		* bb PPEM302 gghh TBL
	Vr/<i> Ip Ospf		1103		* bb PPEM302 gghh TBL
7026	LAN port management system alarms. For Succession VOA, the LAN port management system is used only for network management connectivity purposes. For VOIP same alarms are used.				
	LP/0 OamEnet/0		3002		* bb PPEM30? gghh TBL
	LP/0 OamEnet/0		3003		* bb PPEM303 gghh TBL

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
	LP/0 OamEnet/0		3006		* bb PPEM302 gghh TBL
7039	ATM Core alarms. AtmIf instance range (<n>): 1-4095 Vcc instance range (<n2.n3>): n2 is VPI; n3 is VCI				
	Atmif/<n> Vcc/<n2.n3>		2001		* bb PPEM302 gghh TBL
	Atmif/<n>		4000		* bb PPEM300 gghh TBL
7041	ATM Networking alarms. AtmIf instance range (<n>): 1-4095 CfgNode instance range (<n>): 0-104 Top instance range (<n>): 0-104 Node instance range (<id>): 44-hex digit id Vpt instance range (<n2>): 0-4095				
	Atmif/<n> Uni		0000		* bb PPEM306 gghh TBL
	Atmif/<n> Uni		0001		* bb PPEM303 gghh TBL
	Atmif/<n> Uni Ilmi		0051		**bb PPEM300 gghh TBL
	Atmif/<n> Uni Atmif/<n> Pnni Atmif/<n> Vpt/<n2> Uni Atmif/<n> Vpt/<n2> Pnni		0151		*Cbb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0251		**bb PPEM300 gghh TBL
	Atmif/<n> Pnni Rcc		0252		**bb PPEM300 gghh TBL
	Artg Pnni Top/<n> Node/<id>		0602		**bb PPEM301 gghh TBL
	Artg		0603		**bb PPEM303 gghh TBL
7056	Voice Services Processor (VSP) / Narrowband Service Trunk over ATM (Nsta) This group is specific to MG15000 application (e.g. severe failure of the VSP card) Lp instance range (<x>): 0-15 PModule instance range (<y>): 1-24 PBlock instance range (<z>): 1-2 NSTA instance range (<i>): 0-15999 Conn instance range (<l>): 0-128 Brag instance range (<d>): 0-159999 BragS instance range (<p>): 0-15				
	<Any MSS15000 component>		0000		* bb PPEM302 gghh TBL
	Lp/<x> Vsp PModule/<y>		0006		* bb PPEM303 gghh TBL
	Nsta/<i> Conn/<l> Brag/<d> Ccst		1101		* bb PPEM300 gghh TBL
	Nsta/<i> Vgs H248/0		1206		* bb PPEM300 gghh TBL

MSS15000 Index Group	Component Name	Solution Notes	MSS15000 Subindex	Importance Category	SCC2 Header
	Nsta/<i> Vgs lua		1212		* bb PPEM300 gghh TBL
	Lp/<x> Vsp PModule/<y>		1214		**bb PPEM302 gghh TBL
	Nsta/<i> Vgs BragS/<p>		1215		** bb PPEM302 gghh TBL
7060	ATM and Frame Resource Control alarms. LP instance range (<n>): 0-15				
	LP/<n> Eng Arc Ov		1200		* bb PPEM301 gghh TBL
	LP/<n> Eng		1300		
	LP/<n> Eng		1400		
	LP/<n> Eng		1500		
	LP/<n> Eng		1600		
7061	Security policy violation alarms. VR instance range (<i>): any string, but often specified simply as a digit. <spd_name>: name of the security policy database <pol_id>: instance number of the Policy component <ip_addr,esp,spi>: IP address of the peer with which this SecurityAssociation component is established, the security protocol (ESP), and the Security Parameter Index (SPI) value				
	Vr/<i> Ip Spd/<spd_name> Pol/<pol_id> Sa/<ip_addr,esp,spi>		0001		**bb PPEM305 gghh TBL
7071	LAN ApplicationLAN application instance (<n>): 0-255				
	LA/<n>		1000		*Cbb PPEM302 gghh TBL
7080	Software file system. <name> = name of the software application				
	Sw Av/<name>		0100		**bb PPEM302 gghh TBL
7082	Routine Exercise alarms.				
	Rex		0003		**bb PPEM303 gghh TBL
7083	Flash burning alarms. Card instance range (<x>): 0-15				
	Shelf Card/<x> Fpga		0100		**bb PPEM302 gghh TBL
	Shelf Card/<x> Fpga		0101		**bb PPEM303 gghh TBL

Reference [6] provides detailed descriptions of MSS15000 alarm logs, of which only a portion are applicable for Succession VOA/VOIP.

4. MDM Alarm Logs

Table 4 presents the list of MDM and MDM proxy set/clear alarm logs that are applicable for Succession VOA/VOIP. Table 5 presents the list of MDM and MDM proxy message alarm logs that are applicable for Succession VOA/VOIP.

Applicable MDM set/clear alarms logs include those due to MDM software failure, and alarms related to the monitoring of the platform on which MDM is operating. MDM proxy alarm logs are alarms that MDM initiates on behalf of MSS15000 (for a number of reasons) and injects into the MSS15000 alarm log stream.

The table does not explicitly state all MDM clear alarm logs that correspond to each set. The clear differs from its corresponding set by only the first two characters. The characters “aa” are replaced by “ “ (two spaces). This format is presented in Table 1.

The MDM alarm identifier consists of an eight-digit number identifying the alarm. The first four digits comprise the **Index Group**, which represents logical groupings of alarms. The last four digits are the **SubIndex**, which is an identifier within each index group.

Component Name indicates the managed object against which the alarm Log is generated. This table contains the CLI format of a component name. The “compId” field in SCC2 format contains this information (with the module’s <nodename> pre-pended). Also, “compId” follows the MDM API-style format (with component type and instance separated by a space instead of a slash, and ‘$’ appearing in place of a null instance value). Variables (usually instance value ranges) are denoted by <> and the reader should reference the Alarms NTP’s [3] and [4] for further information.

Table 4 MDM Set/Clear Alarms Supported for Succession VOA/VOIP

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
0999	Loss of access to a MSS15000 shelf from MDM. MDM tries to reconnect and when it succeeds in doing so, will do a “state walk” of major components on the shelf and issue alarms for those components that are out-of-service. EM instance range (<nodename>): a string, typically the CLLI identifier for the MSS15000				
	EM/<nodename>		0001		*Cbb MDM 303 gghh TBL
0999	MDM Proxy-alarm. MDM-originated alarm sent on behalf of the MSS15000, either due to a state walk or a state-change notification.				
	This alarm can apply to many MSS15000 components.		0012		**bb PPEMeee gghh TBL where: eee = 300, 301, 302, 303, 304, 305, 306, 307

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
3010	Indicates faults on MDM server processes, which are needed by the MDM tools/applications. The MDM Log Display GUI or corresponding Unix Utility (nmslog) may also be used to find the information for the cause of the problem. NMS instance range (<x>): a string, typically the hostname of the MDM server platform APP instance range (<a>): a string, denoting the name of an MDM software application Autopatch nodes (<nodes parameter>): typically, this is the name of an HGDS group or a node name or file name containing a list of node names. EM node name (<node name>): the name of the MSS15000 or MG15000 shelf				
	NMS/<x> APP/<a>		0000		**bb MDM 302 gghh TBL
	NMS/<x> APP/PPAUTOPATCH		0801		*bb MDM 306 gghh TBL
	NMS/<x> APP/PPAUTOPATCH NODES/<nodes parameter>		0802		*bb MDM 302 gghh TBL
	NMS/<x> APP/PPAUTOPATCH NODES/<nodes parameter>		0803		**bb MDM 302 gghh TBL
	NMS/<x> APP/PPAUTOPATCH EM/<node name>		0820		**bb MDM 302 gghh TBL
	NMS/<x> APP/PPAUTOPATCH EM/<node name>		0821		**bb MDM 302 gghh TBL
3011	MDM Platform monitoring; e.g. Solaris and Sun monitoring, including: CPU, disk space, memory, local ports and connectivity to adjacent neighbors. The severity of resource problems are determined via thresholds. Connectivity problems are determined using ping command. The alarms 3011 xxFF (where xx can be 01,02,03,04,05,06, or 07) are clear alarms only. A single 3011xxFF alarm clears all outstanding alarms from 3011xx00 through 3011xx99. NMS instance range (<x>): a string, typically the hostname of the MDM server platform APP instance range (<a>): a string, denoting the name of an MDM software application DISK instance range (<v>): a string, denoting disk volume name CPU instance range (<c>): a string, denoting the CPU id PORT and CONNECTION instance range (<ip>): an IP address or host name SDS instance range (<d>): logical disk name				
	NMS/<x> APP/<a>		0001		*Cbb MDM 303 gghh TBL
	NMS/<x> DISK/<v>		0100		aabb MDM 303 gghh TBL where: aa = “*C”, “**”, “* ”
	NMS/<x> CPU/<c>		0200		aabb MDM 303 gghh TBL where: aa = “*C”, “**”, “* ”
	NMS/<x> MEMORY		0300		aabb MDM 303 gghh TBL where: aa = “*C”, “**”, “* ”
	NMS/<x> PORT/<ip>		0401		**bb MDM 303 gghh TBL
	NMS/<x> CONNECTION/<ip>		0501		*Cbb MDM 303 gghh TBL

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
	NMS/<x> SDS/<d>		0600		*Cbb MDM 303 gghh TBL
	NMS/<x>		0700		aabb MDM 303 gghh TBL where: aa = "*C", "**"
	NMS/<x>		01FF		bb MDM 303 gghh TBL
			02FF		bb MDM 303 gghh TBL
			03FF		bb MDM 303 gghh TBL
			04FF		bb MDM 303 gghh TBL
			05FF		bb MDM 303 gghh TBL
			06FF		bb MDM 303 gghh TBL
			07FF		bb MDM 303 gghh TBL
3012	Template configuration audit alarms. Indicates problems with MSS configuration, detected by audit tool. EM node name (<node name>): the name of the MSS15000 or MG15000 shelf				
	NMS_APP/CFGAUDIT EM/<node name>		0001 0002		**bb MDM 302 gghh TBL

Reference [4] provides detailed descriptions of MDM and MDM proxy alarm logs, of which only a portion are applicable for Succession VOA/VOIP.

Table 5 MDM Message Alarms Supported for Succession VOA/VOIP

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
0999	MDM proxy-alarm. Issued when a loss of redundancy of alarm feed occurs. The MDM has lost its direct network alarm feed, but is still collecting them from its mate MDM. Note that this message alarm will not be issued for all conditions that could lead to a loss of redundancy, nor is it "cleared" when the problem is resolved. Thus, we do not recommend that this alarm be keyed upon, but include it here because it is likely to be seen. <deviceType> is any IP-enabled device, such as "EM" or "PP8600". <nodeName> is the name of the device or shelf.				
	<deviceType>/<nodeName>		0100		* bb MDM 303 gghh TBL

MDM Index Group	Component Name	N/A	MDM SubIndex	Importance category (N/A)	SCC2 Header
3010	Indicates faults on MDM server processes, which are needed by the MDM tools/applications. The MDM Log Display GUI or corresponding Unix Utility (nmslog) may also be used to find the information for the cause of the problem. NMS instance range (<x>): a string, typically the hostname of the MDM server platform GROUP instance range (<g>): a string, which is the HGDS group name for a set of MSS15000s PP instance range (<nodename>): a string, typically the CLLI identifier for the MSS15000				
	NMS/<x> GROUP/<g>		0700		* bb MDM 305 gghh TBL
	NMS/<x> PP/<nodename>		0701		* bb MDM 300 gghh TBL
	NMS/<x> PP/<nodename>		0702		* bb MDM 300 gghh TBL
	NMS/<x> APPL/TODCHANGEOVER		0703		* bb MDM 304 gghh TBL
600x	MDP application alarms. NMS instance range (<x>): a string, typically the hostname of the MDM server platform MDP instance range (<a>): a string, denoting the name of an MDP software application				
	NMS/<x> MDP/<a>		00001-40000		aabb MDM 307 gghh TBL where: aa = “*C”, “**”, “* “

5. SN06(VOA)-to-SN06.2(VOA/VOIP) Delta Summary

The following table captures the SN06.2 (VOA/VOIP) alarm log delta that includes MG15000 application as compared with SN06 (VOA) documentation that did not include any MG15000 application specifics

Table 6 SN06 (non MG15000 content) -to-SN06.2 (including MG15000 content) Change Summary Description

Fault Code	Description of Change
SET ALARMS	
70115400	New
70115401	New
70115402	New
70115403	New
70115480	New
7026 3000	New
7056 0002	New
7056 0003	New
7056 0500	New
7056 0501	New
7056 0502	New
7056 1000	New
7056 1200	New
7056 1201	New
7056 1202	New
7056 1203	New
7056 1204	New
7056 1209	New
7056 1210	New
7056 1211	New
7056 1213	New
MESSAGE Alarms	
7000 0039	New
7021 1000	New
7021 1002	New
7021 1003	New
7021 1004	New
7021 1005	New
7021 1006	New
7021 100B	New
7021 1100	New
7056 1101	New
7056 1212	New
70561214	New
7056 1215	New

7060 1300	New
7060 1400	New
7060 1500	New
7060 1600	New
7071 1200	New

6. SN06.2-to-SN07(VOA/VOIP) Delta Summary

The following table captures the SN07 (VOA/VOIP) alarm log delta as compared with SN06.2 (VOA/VOIP) documentation.

Table 7 SN06.2-to-SN07 Change Summary Description

Fault Code	Description of Change
SET ALARMS	
7000 0041	New
7011 1500	New
7011 1501	New
7011 5254	New
7011 5255	New
7011 5256	New
7012 0059	New
7021 0013	New
7021 0014	New
7041 0700	New
7041 0701	New
7041 0703	New
7056 1208	New
7056 1217	New
0999 0004	New
3011 01FF	New
3011 02FF	New
3011 03FF	New
3011 04FF	New
3011 05FF	New
3011 06FF	New
3011 07FF	New
MESSAGE Alarms	
7003 0008	New
7008 1021	New
7021 1021	New
7021 1101	New

7041 0151	New
7056 0006	New
7080 0100	New

7. SN07-to-SN08 (VOA/VOIP) Delta Summary

The following table captures the SN08 (VOA/VOIP) alarm log delta as compared with SN07 (VOA/VOIP) documentation.

Table 8 SN07-to-SN08 Change Summary Description

Fault Code	Description of Change
SET ALARMS	
7000 0041	Changed
7002 0003	Changed
7002 0004	New
7006 0100	New
7021 1002	Changed
7021 1003	Changed
7041 0052	New
7056 1219	New
0999 0004	Removed (applies only to PP8600 and other DCD managed devices)
3010 0801	New
3010 0802	New
3010 0803	New
3010 0820	New
3010 0821	New
MESSAGE Alarms	
0999 0100	New
7006 0009	New
7006 0101	New
7006 0102	New
7006 0103	New
7006 0104	New
7006 0105	New
7061 0001	New

8. SN08-to-SN09 (VOA/VOIP) Delta Summary

The following table captures the SN08 (VOA/VOIP) alarm log delta as compared with SN07 (VOA/VOIP) documentation.

Table 9 SN08-to-SN09 Change Summary Description

Fault Code	Description of Change
SET Alarms	
3012 0001	New
3012 0002	New
7000 0042	New
7000 0043	New
7000 0044	New
7011 5281	New
7011 5501	Changed
7011 5290	Changed
7011 5291	Changed
7011 5292	Changed
7011 5293	Changed
7011 5294	Changed
7039 1001	New
7039 1002	New
7039 1003	New
7039 1004	New
7039 2000	Changed
7039 2003	Changed
7082 0001	New
7082 0002	New
MESSAGE Alarms	
7021 1103	New
7056 0000	New
7056 1206	New
7082 0003	New
7083 0100	New
7083 0101	New

9. References

1. Passports and MDM Logs, draft 1.2, March 2001 (PassportMDMLog_v1.2.doc), by the SDM team.
2. Passport 15000 for Universal Access – AAL1 (SN06) Integrated Solution Specification, Issue 3.04, Oct 22, 2002
3. NTP 241-6001-501 Nortel Networks Multiservice Data Manager Alarms Reference, 15.3D2, June 2005.
4. NTP 241-6001-309 Preside MDM Management Data Provider User Guide, 14.3RSUP, 2003.
5. Supernode Data Manager - Log Applications Enhancement Design Summary (DSUM), 2002.
6. NTP NN10600-500 Multiservice Switch 7400/15000/20000 Alarms Reference, 7.1M1, June 2005
7. NTP NN10092-911 Nortel Networks Multiservice Switch 15000 Media Gateway 15000 and Preside MDM in Succession Networks Fault Management Overview PT-AAL1/UA-AAL1/UA-IP, SN07S1, Dec 2004

Appendix D: USP Operational Measurements

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	ATM Driver Messaging, Plane 1 CRC Error Count	This OM measures the number of Plane 1 CRC errors.
Accumulation OM	AS Master, BICC Discard Count	This OM measures the number of BICC origination messages that were discarded due to Core Overload Control.
Accumulation OM	AS Master, BSSAP Discard Count	This OM measures the number of SCCP connection request messages for the BSSAP subsystem that were discarded due to Core Overload Control.
Accumulation OM	AS Master, Core Overload Duration	This OM measures the total time, in seconds, that the Core was in Overload.
Accumulation OM	AS Master, ISUP Discard Count	This OM measures the number of ISUP origination messages that were discarded due to Core Overload Control.
Accumulation OM	AS Master, RANAP Discard Count	This OM measures the number of SCCP connection request messages for the RANAP subsystem that were discarded due to Core Overload Control.
Accumulation OM	AS Master, TUP Discard Count	This OM measures the number of TUP origination messages that were discarded due to Core Overload Control.
Accumulation OM	ASP Path Management, Path Down Time	This OM measures the total time that a Path was in the Down state.
Accumulation OM	ASP Path Management, Path entered Down state	This OM measures the total number of times per measurement period that a Path entered the Down state.
Accumulation OM	ASP Path Management, Path entered Restoring state	This OM measures the total number of times per measurement period that a Path entered the Restoring state.
Accumulation OM	ASP Path Management, Path entered Up state	This OM measures the total number of times per measurement period that a Path entered the Up state.
Accumulation OM	ASP Path Management, Path Restore Time	This OM measures the total time that a Path was in the Restoring state.
Accumulation OM	ASP Path Management, Path Up Time	This OM measures the total time that a Path was in the Up state.
Accumulation OM	ASP Path Traffic, Discarded MSUs Count	This OM measures the total number of received MSUs on an ASP Path which were discarded because the Network Appearance (or System Identity) associated with the incoming message was not found on the USP
Accumulation OM	ASP Path Traffic, Discarded MTP3b MSUs Count	This OM measures the total number of received MTP3B MSUs (> 272 octets) on an ASP Path which were discarded because the outgoing link is not MTP3B capable. This doesn't apply to SCCP/LUDT messages since on IPS7 Paths, these messages will be segmented and then sent out. For non-SCCP messages such as BICC messages > 272 octets, this will apply.
Accumulation OM	ASP Path Traffic, Originated MSUs Count	This OM measures the number of originated MSUs (MSUs that contain the PC or capability code for the USP in the OPC field) that are successfully passed to the ASP Path for transmission (for example, network management messages).
Accumulation OM	ASP Path Traffic, Received MSUs Count	This OM measures the total number of received MSUs on an ASP Path

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	ASP Path Traffic, Sent MSUs Count	This OM measures the number of through-switched MSUs (MSUs that do not contain the PC or capability code for the USP in either the OPC or DPC) that are acknowledged, translated, and successfully passed to the ASP Path for transmission.
Accumulation OM	ASP Path Traffic, Terminated MSUs Count	This OM measures the number of terminated MSUs (acknowledged, incoming MSUs that contain the PC or capability code of the USP in the DPC field) received.
Accumulation OM	ASP Path Utilization, DAUD Received Count	This OM measures the number of destination audit (DAUD) messages transmitted.
Accumulation OM	ASP Path Utilization, DAVA Transmitted Count	This OM measures the number of destination available (DAVA) messages transmitted.
Accumulation OM	ASP Path Utilization, DUNA Transmitted Count	This OM measures the number of destination unavailable messages transmitted.
Accumulation OM	ASP Path Utilization, DUPU Transmitted Count	This OM measures the number of destination user part unavailable messages transmitted.
Accumulation OM	ASP Path Utilization, SCON Transmitted Count	This OM measures the number of Signaling Congestion (SCON) messages transmitted.
Accumulation OM	ATM Driver Messaging, Duplicate Messages Count	This OM measures the number of duplicate messages.
Accumulation OM	ATM Driver Messaging, IP Message Count	This OM measures the number of incoming IP messages.
Accumulation OM	ATM Driver Messaging, Plane 1 Messages Count	This OM measures the number of incoming Plane 1 messages.
Accumulation OM	ATM Driver Messaging, Plane 2 CRC Error Count	This OM measures the number of Plane 2 CRC errors.
Accumulation OM	ATM Driver Messaging, Plane 2 Messages Count	This OM measures the number of incoming Plane 2 messages.
Accumulation OM	ATM Driver Messaging, Raw Cell Count	This OM measures the number of raw cells. Raw cells are typically bad cells or OAM cells.
Accumulation OM	ATM Driver Messaging, Raw Message Count	This OM measures the number of ATM raw messages. Raw messages are messages not assigned to a protocol.
Accumulation OM	ATM Driver Messaging, Sequence Number Reset Count	This OM measures the number of times the sequence numbers are reset due to the receipt of five consecutive duplicate cells.
Accumulation OM	ATM Driver Messaging, SSCOP Message Count	This OM measures the number of incoming SSCOP messages.
Accumulation OM	ATM Link Traffic, Discarded cells with HEC Viol.	This OM measures the number of ATM cells discarded due to Header Error Control (HEC) violations.
Accumulation OM	ATM Link Traffic, Discarded cells with Prot. Errs	This OM measures the number of cells discarded due to Protocol (ATM-Layer Header) Errors.
Accumulation OM	ATM Link Traffic, In NDC-valid cells on HSL VCL	This OM measures the number of incoming Network Data Collection (NDC) valid cells on the High Speed Links (HSL) VCL.
Accumulation OM	ATM Link Traffic, Incoming ATM UI cells	This OM measures the number of incoming ATM User Information (UI) cells.
Accumulation OM	ATM Link Traffic, OCD Anomalies	This OM measures the number of Out of Cell Delineation (OCD) anomalies.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	ATM Link Traffic, Out NDC-valid cells on HSL VCL	This OM measures the number of outgoing Network Data Collection (NDC) valid cells on the High Speed Links (HSL) VCL.
Accumulation OM	ATM Link Traffic, Outgoing ATM UI cells	This OM measures the number of outgoing ATM User Information (UI) cells.
Accumulation OM	BICC Received Message Counts, BICC Call P Received Count	This OM measures the number of BICC call processing messages received from the SS7 Network.
Accumulation OM	BICC Received Message Counts, BICC Error No OPC Route	This OM measures the number of BICC messages discarded as a result of not being able to find the associated OPC route for the received BICC message
Accumulation OM	BICC Received Message Counts, BICC Error No Path	This OM measures the number of BICC messages discarded as a result of not being able to find an inservice path to a given AS.
Accumulation OM	BICC Received Message Counts, BICC Error No Route	This OM measures the number of BICC messages discarded as a result of not being able to find a route to a given AS.
Accumulation OM	BICC Received Message Counts, BICC Maint Received Count	This OM measures the number of BICC maintenance messages received from the SS7 Network.
Accumulation OM	BICC Received Message Counts, Wrong NE Received Count	This OM measures the number of BICC messages discarded as a result of not receiving the message for a SG Network Element
Accumulation OM	Carrier, Far End Line - Errored Seconds	This OM measures the Far End Performance data: Far End Errored Seconds - Line.
Accumulation OM	Carrier, Far End P - Sev Err Frm/AIS Sec	This OM measures the Far End Performance data: Far End Severely Errored Frame/AIS Seconds - Path.
Accumulation OM	Carrier, Far End P - Severely Err Secs	This OM measures the Far End Performance data: Far End Severely Errored Seconds - Path.
Accumulation OM	Carrier, Far End P - Unavailable Seconds	This OM measures the Far End Performance data: Far End Unavailable Seconds - Path.
Accumulation OM	Carrier, Far End Path - Code Violations	This OM measures the Far End Performance data: Far End Code Violations - Path.
Accumulation OM	Carrier, Far End Path - Controlled Slips	This OM measures the Far End Performance data: Far End Controlled Slips - Path
Accumulation OM	Carrier, Far End Path - Errored Seconds	This OM measures the Far End Performance data: Far End Errored Seconds - Path.
Accumulation OM	Carrier, Far End Path - Failure Count	This OM measures the Far End Performance data: Far End Failure Count - Path.
Accumulation OM	Carrier, Line - Code Violations	This OM measures the Near End Performance data: Code Violations - Line.
Accumulation OM	Carrier, Line - Errored Seconds	This OM measures the Near End Performance data: Errored Seconds - Line.
Accumulation OM	Carrier, Line - Loss of Signal Seconds	This OM measures the Near End Performance data: Loss of Signal Seconds - Line. All performance parameters including this parameter are defined in ANSI T1.231-1997 'Digital Hierarchy - Layer 1 in-Service Digital Transmission Performance Monitoring'.
Accumulation OM	Carrier, Line - Severely Errored Seconds	This OM measures the Near End Performance data: Severely Errored Seconds - Line.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	Carrier, P - Severely Err Frame/AIS Secs	This OM measures the Near End Performance data: Severely Errored Frame/AIS Seconds - Path.
Accumulation OM	Carrier, Path - AIS Seconds	This OM measures the Near End Performance data: AIS Seconds - Path.
Accumulation OM	Carrier, Path - Code Violations	This OM measures the Near End Performance data: Code Violations - Path.
Accumulation OM	Carrier, Path - Errored Seconds	This OM measures the Near End Performance data: Errored Seconds - Path.
Accumulation OM	Carrier, Path - Failure Count	This OM measures the Near End Performance data: Failure Count - Path.
Accumulation OM	Carrier, Path - Severely Errored Seconds	This OM measures the Near End Performance data: Severely Errored Seconds - Path.
Accumulation OM	Carrier, Path - Unavailable Seconds	This OM measures the Near End Performance data: Unavailable Seconds - Path.
Accumulation OM	Gateway Screening Results, Disallowed Cld Party Addr Count	This OM measures the number of MSUs rejected on a particular link, because of disallowed SCCP Called Party Addresses.
Accumulation OM	Gateway Screening Results, Disallowed ISUP Count	This OM measures the number of MSUs rejected on a particular link, because of a disallowed ISDN User Part message type.
Accumulation OM	Gateway Screening Results, Disallowed Trans Type Count	This OM measures the number of MSUs rejected on a particular link, because of a disallowed SCCP GTT type.
Accumulation OM	Gateway Screening Results, Invalid Affct Destination Count	This OM measures the number of MSUs rejected on a particular link, because the destination fields in signaling-routeset-test, TFx/TCx, or TFC messages from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid Affct PC-SSN Count	This OM measures the number of MSUs rejected on a particular link, because the affected PCs in SCCP subsystem-prohibited (SSP) and subsystem-allowed (SSA) messages and an invalid PC or SSN in SCCP subsystem-status-test (SST) messages from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid Cng Party Addr Count	This OM measures the number of MSUs rejected on a particular link, because the Calling Party Addresses (PC or SSN) from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid DPC Count	This OM measures the number of MSUs rejected on a particular link, because the DPCs from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid OPC Count	This OM measures the number of MSUs rejected on a particular link, because the OPCs from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	Gateway Screening Results, Invalid SIO Count	This OM measures the number of MSUs rejected on a particular link, because the SIOs from the MSUs did not pass GWS checking based on the provisioned criteria.
Accumulation OM	GTT Type, GTTs Not Performed Count	This OM measures the total number of GTTs that could not be performed for a particular translation type (all reasons).
Accumulation OM	GTT Type, GTTs Performed Count	This OM measures the total number of MSUs that successfully completed GTT (that is, a match was found for the global title) for a particular translation type.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	GTT Type, No Translation for Addr Count	This OM measures the number of times the Address Not Found error was encountered for a particular translation type (that is, there was no match found for the global title in the GTT table).
Accumulation OM	ISUP Received Message Counts, ACM Received Count	This OM measures the number of ISUP Address Complete Messages (ACM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, ALT Received Count	This OM measures the number of ISUP Altering Messages (ALT) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, ANM Received Count	This OM measures the number of ISUP Answer Messages (ANM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, BLA Received Count	This OM measures the number of ISUP Blocking Acknowledgement (BLA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, BLO Received Count	This OM measures the number of ISUP Blocking Messages (BLO) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CCR Received Count	This OM measures the number of ISUP Continuity Check Request Messages (CCR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CFN Received Count	This OM measures the number of ISUP Confusion Messages (CFN) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CGB Received Count	This OM measures the number of ISUP Circuit Group Blocking Messages (CGB) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CGBA Received Count	This OM measures the number of ISUP Circuit Group Blocking Acknowledgement Messages (CGBA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CGU Received Count	This OM measures the number of ISUP Circuit Group Unblocking Messages (CGU) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CGUA Received Count	This OM measures the number of ISUP Circuit Group Unblocking Acknowledgement Messages (CGUA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CMC Received Count	This OM measures the number of ISUP Call Modification Completed Messages (CMC) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CMR Received Count	This OM measures the number of ISUP Call Modification Request Messages (CMR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CMRJ Received Count	This OM measures the number of ISUP Call Modification Rejected Messages (CMRJ) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CON Received Count	This OM measures the number of ISUP Connect Messages (CON) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, COT Received Count	This OM measures the number of ISUP Continuity Test Messages (COT) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CPG Received Count	This OM measures the number of ISUP Call Progress Messages (CPG) received from the SS7 Network. (Only for SG Identities)

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	ISUP Received Message Counts, CQM Received Count	This OM measures the number of ISUP Circuit Query Messages (CQM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CQR Received Count	This OM measures the number of ISUP Circuit Query Response Messages (CQR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CRA Received Count	This OM measures the number of ISUP Circuit Reservation Acknowledgement Messages (CRA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CRG Received Count	This OM measures the number of ISUP Charge Information Messages (CRG) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CRM Received Count	This OM measures the number of ISUP Circuit Reservation Messages (CRM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CSVR Received Count	This OM measures the number of ISUP Closed User Group Selection and Validation Request Messages (CSVR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CSVS Received Count	This OM measures the number of ISUP Closed User Group Selection and Validation Response Messages (CSVS) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CVR Received Count	This OM measures the number of ISUP Circuit Validation Response Messages (CVR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, CVT Received Count	This OM measures the number of ISUP Circuit Validation Test Messages (CVT) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, DRS Received Count	This OM measures the number of ISUP Delayed Release Messages (DRS) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, EXM Received Count	This OM measures the number of ISUP Exit Messages (EXM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, FAA Received Count	This OM measures the number of ISUP Facility Accepted Messages (FAA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, FAC Received Count	This OM measures the number of ISUP Facility Messages (FAC) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, FAD Received Count	This OM measures the number of ISUP Facility Deactivated Messages (FAD) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, FAI Received Count	This OM measures the number of ISUP Facility Information Messages (FAM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, FAR Received Count	This OM measures the number of ISUP Facility Request Messages (FAR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, FOT Received Count	This OM measures the number of ISUP Forward Transfer Messages (FOT) received from the SS7 Network. (Only for SG Identities)

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	ISUP Received Message Counts, FRJ Received Count	This OM measures the number of ISUP Facility Rejected Messages (FRJ) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, GRA Received Count	This OM measures the number of ISUP Circuit Group Reset Acknowledgement Messages (GRA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, GRS Received Count	This OM measures the number of ISUP Circuit Group Reset Messages (GRS) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, IAM Received Count	This OM measures the number of ISUP Initial Address Message Messages (IAM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, IAMN1 Received Count	This OM measures the number of ISUP Initial Address Message Not Priority One Messages (IAMN1) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, IDR Received Count	This OM measures the number of ISUP Identification Request Messages (IDR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, INF Received Count	This OM measures the number of ISUP Information Messages (INF) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, INR Received Count	This OM measures the number of ISUP Information Request Messages (INR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, IRS Received Count	This OM measures the number of ISUP Identification Response Messages (IRS) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, ISUP Error No AS for OPC/CIC	This OM measures the number of ISUP messages discarded as a result of not being able to find a valid AS for a given OPC/CIC. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, ISUP Error No OPC/CIC Data	This OM measures the number of ISUP messages discarded as a result of missing database entry for a given OPC/CIC. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, ISUP Error No Path	This OM measures the number of ISUP messages discarded as a result of not being able to find a path to a given AS. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, ISUP Error No Route	This OM measures the number of ISUP messages discarded as a result of not being able to find a route to a given AS. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, ISUP Error Unknown Message	This OM measures the number of unrecognized ISUP Messages received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, LOP Received Count	This OM measures the number of ISUP Loop Prevention Messages (LOP) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, LPA Received Count	This OM measures the number of ISUP Loop Back Acknowledgement Messages (LPA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, NRM Received Count	This OM measures the number of ISUP Network Resource Management Messages (NRM) received from the SS7 Network. (Only for SG Identities)

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	ISUP Received Message Counts, PAM Received Count	This OM measures the number of ISUP Pass Along Message Messages (PAM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, PRG Received Count	This OM measures the number of ISUP Progress Messages (PRG) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, REL Received Count	This OM measures the number of ISUP Release Messages (REL) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, RES Received Count	This OM measures the number of ISUP Resume Messages (RES) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, RLC Received Count	This OM measures the number of ISUP Release Complete Messages (RLC) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, RPM Received Count	This OM measures the number of ISUP Reconfiguration Progress Message Messages (ACM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, RSC Received Count	This OM measures the number of ISUP Reset Circuit Messages (RSC) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, SAM Received Count	This OM measures the number of ISUP Subsequent Address Message Messages (SAM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, SGM Received Count	This OM measures the number of ISUP Segmentation Messages (SGM) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, SUS Received Count	This OM measures the number of ISUP Suspend Messages (SUS) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, UBA Received Count	This OM measures the number of ISUP Unblocking Acknowledgement Messages (UBA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, UBL Received Count	This OM measures the number of ISUP Unblocking Messages (UBL) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, UCIC Received Count	This OM measures the number of ISUP Unequipped Circuit Identification Code Messages (UCIC) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, UPA Received Count	This OM measures the number of ISUP User Part Available Messages (UPA) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, UPT Received Count	This OM measures the number of ISUP User Part Test Messages (UPT) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, USR Received Count	This OM measures the number of ISUP User-to-User Information Messages (USR) received from the SS7 Network. (Only for SG Identities)
Accumulation OM	ISUP Received Message Counts, Wrong NE Received Count	This OM measures the number of ISUP messages discarded as a result of not receiving the message from a SG Network Element.
Accumulation OM	Link Faults and Performance, Number of negative ack.received	1.9 of Q.752 This OM measures number of negative acknowledgements received on the link indicating that the far end did not receive the message correctly.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	Link Faults and Performance, Number of SUs received in error	1.8 of Q.752 This OM measures signaling units on a link, received in error.
Accumulation OM	Link Faults and Performance, Octets Retransmitted	3.2 of Q.752 This OM counts number of bytes that are retransmitted. This count includes SIO, SIF, opening flags and check bits.
Accumulation OM	Link Faults and Performance, SL alignment or proving failure	1.7 of Q.752 This OM measures link synchronization failures during alignment or proving and indicates a signaling data link fault which prevents the SdL moving into service.
Accumulation OM	Link Faults and Performance, SL failure-Abnormal FIBR/BSNR	1.3 of Q.752 This OM measures link synchronization failures and indicates complex failures in transmission or an intermittent hardware fault or even designer error.
Accumulation OM	Link Faults and Performance, SL failure-All reasons	1.2 of Q.752 This OM measures in_service link failures due to any reason. It does not count link activation failures.
Accumulation OM	Link Faults and Performance, SL failure-Exc. delay of ack	1.4 of Q.752 This OM measures link synchronization failures and indicates serious disturbances or an interruption of signaling data link.
Accumulation OM	Link Faults and Performance, SL failure-Exc. duration of cong.	1.6 of Q.752 This OM measures link synchronization failures caused by prolonged congestion on the link.
Accumulation OM	Link Faults and Performance, SL failure-Excessive error rate	1.5 of Q.752 This OM measures link synchronization failures and indicates noisy link.
Accumulation OM	Link Faults and Performance, SL failure-Other reasons	This OM measures link synchronization failures due to reasons other than Abnormal FIBR/BSNR, Excessive delay of ack, Excessive error rate or Excessive duration of congestion .
Accumulation OM	Link Management, Changeover Procedure Count	This OM measures the number of times the changeover procedure is used to move traffic from a link taken out of service to one or more alternate in-service links.
Accumulation OM	Link Management, Far End Mgmt Inhibit Count	This OM measures the number of times a link was successfully inhibited from the far end.
Accumulation OM	Link Management, Level 1 Congestion Count	This OM measures the number of times a link entered Level 1 congestion from no congestion.
Accumulation OM	Link Management, Level 1 Congestion Duration	This OM measures the total time, in seconds, a link was in Level 1 congestion.
Accumulation OM	Link Management, Level 2 Congestion Count	This OM measures the number of times a link entered Level 2 congestion from Level 1 or no congestion.
Accumulation OM	Link Management, Level 2 Congestion Duration	This OM measures the total time, in seconds, a link was in Level 2 congestion.
Accumulation OM	Link Management, Level 3 Congestion Count	This OM measures the number of times a link entered Level 3 congestion from Level 1, Level 2, or no congestion.
Accumulation OM	Link Management, Level 3 Congestion Duration	This OM measures the total time, in seconds, a link was in Level 3 congestion.
Accumulation OM	Link Management, Link Available Duration	This OM measures the total time, in seconds, a link was available to MTP Level 3.
Accumulation OM	Link Management, Link Deactivated Duration	This OM measures the total time, in seconds, a link was manually made unavailable to MTP Level 3 by deactivation.
Accumulation OM	Link Management, Link Local Inhibit Duration	This OM measures the total time, in seconds, a link was manually made unavailable to MTP Level 3 by local inhibition.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	Link Management, Link Remote Inhibit Duration	This OM measures the total time, in seconds, a link was manually made unavailable to MTP Level 3 by remote inhibition.
Accumulation OM	Link Management, Near End Forced Unavailable Count	This OM measures the number of times a link was manually made unavailable to MTP Level 3.
Accumulation OM	Link Management, RPO Count	This OM measures the number of times a link became unavailable to MTP Level 3 after the system received SIPO from the far end. This OM is not applicable for SAAL-based High Speed Links.
Accumulation OM	Link Management, RPO Cumulative Duration	This OM measures the total time, in seconds, that a link was unavailable to MTP Level 3 after the system received SIPO from the far end. This OM is not applicable for SAAL-based High Speed Links.
Accumulation OM	Link Management, Unavailable Duration	This OM measures the total time, in seconds, a link was unavailable (automatically or manually made unavailable) to MTP Level 3.
Accumulation OM	Link Traffic, MSUs Received Count	This OM measures the number of MSUs received on a link, including those MSUs for which retransmission was requested in the SS7 network. For the SAAL-based High Speed Links, the above description applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, MSUs Requiring GTT Count	This OM measures the number of incoming MSUs that require GTT, regardless of the outcome of any GWS operation. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, MSUs Transmitted Count	This OM measures the number of MSUs transmitted to the far end, including those MSUs that were retransmitted in the SS7 network. For the SAAL-based High Speed Links, the above description applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, MTP3b Discard Count	This OM measures the number of received MTP3B MSUs (> 272 octets) which were discarded because the outgoing link is not MTP3b capable. This OM only applies to MTP3B links since non-MTP3B links are not capable of receiving message > 272 octets.
Accumulation OM	Link Traffic, Network Indicator Discard Count	This OM measures the number of received MSUs which were discarded due to a mismatch between the MSU's network indicator (NI) and the NI provisioned in this system. The NI may be provisioned on a network appearance basis. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Octets Received Count	This OM measures the total number of octets actually received for all MSUs counted in the MSUs Received Count OM, before the octets are removed in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	Link Traffic, Octets Requiring GTT Count	This OM measures the total number of MSU octets received for MSUs requiring GTT, including octets removed in MTP Level 2 processing. For the MTP2-based links, this count applies to MSU octets (MTP User Data + MTP L3 Data + MTP L2 Data octets). For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Octets Transmitted Count	This OM measures the total number of octets actually transmitted for all MSUs counted in the MSUs Transmitted Count OM, including octets added in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, OPC Screening Discard Count	This OM measures the number of received MSUs which were discarded because the OPC in the MSU matches the pointcode of this system ID or the OPC in the MSU matches the mate's pointcode but the MSU is not received from the C-link. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Originated MSU Octets Count	This OM measures the total number of originated MSU octets (MSU that contains the PC or capability code of this system in the OPC field) transmitted, including those octets that were added in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Originated MSUs Count	This OM measures the number of originated MSUs (MSUs that contain the PC or capability code of this system in the OPC field) that are successfully passed to Level 2 for transmission (for example, network management messages and MSUs completing GTT) in the SS7 network. For the MTP2-based links, this count applies to MSU octets (MTP User Data + MTP L3 Data + MTP L2 Data octets). For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Pri 0 MSU Inbd Discard Count	This OM measures the number of priority 0 MSUs discarded by the inbound link due to congestion at levels 1, 2, or 3 in the transmit buffers for the outbound link in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 0 MSU Outbd Discard Count	This OM measures the number of priority 0 MSUs discarded due to congestion at levels 1, 2, or 3 in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 1 MSU Inbd Discard Count	This OM measures the number of priority 1 MSUs discarded by the inbound link due to congestion at levels 2 or 3 in the transmit buffers in the outbound link in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	Link Traffic, Pri 1 MSU Outbd Discard Count	This OM measures the number of priority 1 MSUs discarded due to congestion at levels 2 or 3 in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 2 MSU Inbd Discard Count	This OM measures the number of priority 2 MSUs discarded by the inbound link due to congestion at level 3 in the transmit buffers for the outbound link in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 2 MSU Outbd Discard Count	This OM measures the number of priority 2 MSUs discarded due to level 3 congestion in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 3 MSU Inbd Discard Count	This OM measures the number of priority 3 MSUs discarded by the inbound link due to full transmit buffers for the outbound link in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Pri 3 MSU Outbd Discard Count	This OM measures the number of priority 3 MSUs discarded due to a full transmit buffer in the SS7 network. For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data) instead of MSUs (MTP User Data + MTP L3 Data + MTP L2 Data).
Accumulation OM	Link Traffic, Terminated MSU Octets Count	This OM measures the total number of terminated MSU octets (acknowledged, incoming MSU that contains the PC or capability code of this system in the DPC field) received, including octets removed in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).
Accumulation OM	Link Traffic, Terminated MSUs Count	This OM measures the number of terminated MSUs (acknowledged, incoming MSUs that contain the PC or capability code of this system in the DPC field) received from the SS7 network. For the MTP2-based links, this count applies to MSUs (MTP User Data + MTP L3 Data + MTP L2 Data). For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data).
Accumulation OM	Link Traffic, Through-Switched MSUs Count	This OM measures the number of through-switched MSUs (MSUs that do not contain the PC or capability code of this system in either the OPC or DPC) that are acknowledged, translated, and successfully passed to MTP Level 2 for transmission in the SS7 network. For the MTP2-based links, this count applies to MSUs (MTP User Data + MTP L3 Data + MTP L2 Data). For the SAAL-based High Speed Links, this count applies to Messages (MTP User Data + MTP L3 Data).
Accumulation OM	Link Traffic, Thru-Switched MSU Octets Count	This OM measures the total number of through-switched MSU octets (MSU that does not contain the PC or capability code of this system in either the OPC or DPC) received, including those octets that were added in MTP Level 2 processing for the SS7 network. For the MTP2-based links, this count accounts for MTP User Data + MTP L3 Data + MTP L2 Data octets. For the SAAL-based High Speed Links, this count applies to Message octets (MTP User Data + MTP L3 Data octets).

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	Linkset Utilization, Linkset Inactivity Duration	This OM measures the total time, in seconds, that all links in the linkset were unavailable (automatically or manually made unavailable) to MTP Level 3.
Accumulation OM	Linkset Utilization, RST Received Count	This OM measures the number of restart (RST) messages received.
Accumulation OM	Linkset Utilization, RST Transmitted Count	This OM measures the number of restart (RST) messages transmitted.
Accumulation OM	Linkset Utilization, TFA and TCA Received Count	This OM measures the number of transfer-allowed (TFA) and transfer-cluster-allowed (TCA) messages received.
Accumulation OM	Linkset Utilization, TFA and TCA Transmitted Count	This OM measures the number of transfer-allowed (TFA) and transfer-cluster-allowed (TCA) messages transmitted.
Accumulation OM	Linkset Utilization, TFC Received Count	This OM measures the number of transfer-controlled (TFC) messages received by the gateway, listed by the originating network.
Accumulation OM	Linkset Utilization, TFC Transmitted Count	This OM measures the number of transfer-controlled (TFC) messages transmitted by the gateway, listed by the destination network.
Accumulation OM	Linkset Utilization, TFP and TCP Received Count	This OM measures the number of transfer-prohibited (TFP) and transfer-cluster-prohibited (TCP) messages received.
Accumulation OM	Linkset Utilization, TFP and TCP Transmitted Count	This OM measures the number of transfer-prohibited (TFP) and transfer-cluster-prohibited (TCP) messages transmitted.
Accumulation OM	Linkset Utilization, TFR and TCR Received Count	This OM measures the number of transfer-restricted (TFR) and transfer-cluster-restricted (TCR) messages received.
Accumulation OM	Linkset Utilization, TFR and TCR Transmitted Count	This OM measures the number of transfer-restricted (TFR) and transfer-cluster-restricted (TCR) messages transmitted.
Accumulation OM	Linkset Utilization, UPU Received Count	This OM measures the number of user part unavailable messages received.
Accumulation OM	Log Server, Critical Alarms Ack Count	This OM measures the number of critical alarms acknowledged by the Log server.
Accumulation OM	Log Server, Critical Alarms Cleared Count	This OM measures the number of critical alarms cleared by the Log server.
Accumulation OM	Log Server, Critical Alarms Received Count	This OM measures the number of critical alarms received by the Log server.
Accumulation OM	Log Server, Major Alarms Ack Count	This OM measures the number of major alarms acknowledged by the Log server.
Accumulation OM	Log Server, Major Alarms Cleared Count	This OM measures the number of major alarms cleared by the Log server.
Accumulation OM	Log Server, Major Alarms Received Count	This OM measures the number of major alarms received by the Log server.
Accumulation OM	Log Server, Minor Alarms Ack Count	This OM measures the number of minor alarms acknowledged by the Log server.
Accumulation OM	Log Server, Minor Alarms Cleared Count	This OM measures the number of minor alarms cleared by the Log server.
Accumulation OM	Log Server, Minor Alarms Received Count	This OM measures the number of minor alarms received by the Log server.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	NP Database Totals, Add/Change Updates	This OM measures the total number of add/change updates received from the LSMS.
Accumulation OM	NP Database Totals, Delete Updates	This OM measures the total number of delete updates received from the LSMS.
Accumulation OM	NP Database Totals, Emergency Updates	This OM measures the total number of application database updates received from the USP debug facility and can only be displayed from the debug facility Note: Debug is only accessible by Nortel Networks Support Personnel.
Accumulation OM	NP Database Totals, Operational Time	This OM measures the total time within the OM interval that the NPDB was operational.
Accumulation OM	NP Database Totals, Retransmitted Updates	This OM measures the total number of updates retransmitted within the system.
Accumulation OM	NP INAP Totals, INAP CdPN Normalize Failures	This OM measures the number of called party number normalization failures.
Accumulation OM	NP INAP Totals, INAP Indeterminate Queries	This OM measures the number of INAP indeterminate queries.
Accumulation OM	NP INAP Totals, INAP Invalid Context	This OM measures the number of INAP queries with invalid application context.
Accumulation OM	NP INAP Totals, INAP Queries Non-Ported	This OM measures the number of INAP non ported number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Ported	This OM measures the number of INAP ported number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Ported Across	This OM measures the number of INAP ported across number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Ported In	This OM measures the number of INAP ported in number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Ported Out	This OM measures the number of INAP ported out number queries received.
Accumulation OM	NP INAP Totals, INAP Queries Unknown	This OM measures the number of INAP queries received for numbers with unknown ported status.
Accumulation OM	NP INAP Totals, INAP Query Failures	This OM measures the number of INAP query failures.
Accumulation OM	NP INAP Totals, INAP Query Time Outs	This OM measures the total number of INAP query time outs.
Accumulation OM	NP INAP Totals, INAP Total Queries	This OM measures the total number of INAP queries received.
Accumulation OM	NP LSSI Totals, MR Query Received	This OM measures the total number of MR queries received by an application database system node.
Accumulation OM	NP LSSI Totals, NP Query Received	This OM measures the total number of NP queries received by an application database system node.
Accumulation OM	NP NETID Totals, MR Failures	This OM measures the total number of MR query failures identified. The MR Failures value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, MR GTT Overrides	This OM measures the total number of MR queries receiving GTT override. The MR GTT Overrides value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, MR Loop Detection	This OM measures the total number of potential looping detections. The MR Loop Detection value is based upon the Network ID of a received SCCP message.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	NP NETID Totals, MR Non-Ported	This OM measures the total number of MR queries received for non-ported numbers. The MR Non-Ported value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, MR Ported	This OM measures the total number of MR queries received for ported numbers. The MR Ported value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, MR Total	This OM measures the total number of MR queries received. The MR Total value is based upon the Network ID of a received SCCP message.
Accumulation OM	NP NETID Totals, NP Failures	This OM measures the total number of NP query failures. The NP Failures value is based upon the Network ID of a received TCAP message.
Accumulation OM	NP NETID Totals, NP Non-Ported	This OM measures the total number of NP queries received for non-ported numbers. The NP Non-Ported value is based upon the Network ID in the TCAP message.
Accumulation OM	NP NETID Totals, NP Ported	This OM measures the total number of NP queries received for ported numbers. The NP Ported value is based upon the Network ID contained in the NETID of a received TCAP message.
Accumulation OM	NP NETID Totals, NP Total	This OM measures the total number of NP queries received. The NP Total value is based upon the Network ID of a received TCAP message.
Accumulation OM	NP Service Rule Totals, Service Rule Match	This OM measures the total number of matches for the Service Rule.
Accumulation OM	NP Service Rule Totals, Service Rule Mismatch	This OM measures the total number of mismatches for all the Service Rules.
Accumulation OM	NP Service Totals, Database Mismatches	This OM measures the total number of Database mismatches. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, GTA Normalization Failures	This OM measures the total number of GTA number normalization failures. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, GTA Replacement	This OM measures the total number of service queries receiving GTA replacement. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, GTT Overrides	This OM measures the total number of service queries receiving GTT override. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, RN Check Failures	This OM measures the total number of RN check failures on incoming messages using the NoA/RN table. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, Service Failures	This OM measures the total number of Service query failures identified. Service query failures occur when the query logic is unable to process the Service query. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, Service Non-Ported	This OM measures the total number of Service queries received for non-ported numbers. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, Service Ported	This OM measures the total number of Service queries received for ported numbers. The Service Ported value is the total of OMR_SERVICE_PORTED_IN, OMR_SERVICE_PORTED_OUT, and OMR_SERVICE_PORTED_ACROSS This OM is collected by Service ID.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	NP Service Totals, Service Total	This OM measures the total number of Service queries received. This OM is collected by Service ID.
Accumulation OM	NP Service Totals, TT Replacement	This OM measures the total number of service queries receiving TT replacement. This OM is collected by Service ID.
Accumulation OM	NP SMI Totals, High Congestion	This OM measures the total number of times that the high level congestion state was entered.
Accumulation OM	NP SMI Totals, Login Failures	This OM measures the total number of failed LSMS login attempts.
Accumulation OM	NP SMI Totals, Low Congestion	This OM measures the total number of times that the low level congestion state was entered.
Accumulation OM	NP SMI Totals, Medium Congestion	This OM measures the total number of times that the medium level congestion state was entered.
Accumulation OM	NP SMI Totals, Messages Invalid	This OM measures the total number of invalid messages received from the LSMS.
Accumulation OM	NP SMI Totals, Messages Received	This OM measures the total number of messages received from the LSMS.
Accumulation OM	NP SMI Totals, Messages Rejected	This OM measures the total number of received messages from the LSMS that were rejected.
Accumulation OM	NP SRF Totals, SRF Ind. Routing with Ref. Sub.	This OM measures the number of SRF messages relayed to the subscription network via indirect routing with reference to the subscription network.
Accumulation OM	NP SRF Totals, SRF No NP DB Record Found	This OM measures the number of SRF queries received when no record is found in the NP DB.
Accumulation OM	NP SRF Totals, SRF Queries Non-Ported	This OM measures the number of SRF non ported number queries received.
Accumulation OM	NP SRF Totals, SRF Queries Ported Across	This OM measures the number of SRF ported across number queries received.
Accumulation OM	NP SRF Totals, SRF Queries Ported In	This OM measures the number of SRF ported in number queries received.
Accumulation OM	NP SRF Totals, SRF Queries Ported Out	This OM measures the number of SRF ported out number queries received.
Accumulation OM	NP SRF Totals, SRF Queries Unknown	This OM measures the number of SRF queries received for numbers with unknown ported status.
Accumulation OM	NP SRF Totals, SRF Query Failures	This OM measures the number of SRF query failures.
Accumulation OM	NP SRF Totals, SRF Relayed to HLR	This OM measures the number of SRF messages relayed to the HLR.
Accumulation OM	NP SRF Totals, SRF Successful Messages to MSC	This OM measures the number of SRF successful messages sent back to the MSC.
Accumulation OM	NP SRF Totals, SRF Total Queries	This OM measures the total number of SRF queries received.
Accumulation OM	NP SRF Totals, SRF Total Queries Ported	This OM measures the total number of SRF ported number queries received.
Accumulation OM	NP SRF Totals, SRF Transaction Errors Sent Out	This OM measures the number of SRF transaction error messages sent out.
Accumulation OM	NP TnT Totals, TNT Acks Sent	This OM measures the number of Tariff non Transparency acknowledgement messages transmitted.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	NP TnT Totals, TNT Decode Errors	This OM measures the number of Tariff non Transparency MAP decode failures due to incorrect parameters that could not be decoded.
Accumulation OM	NP TnT Totals, TNT Decode Invalid Params	This OM measures the number of Tariff non Transparency MAP decode failures due to invalid parameters. (i.e. IMSI instead of MSISDN included)
Accumulation OM	NP TnT Totals, TNT No NP DB Rec Found	This OM measures the number of Tariff non Transparency queries received for numbers not found in the NP DB.
Accumulation OM	NP TnT Totals, TNT Queries Non-Ported	This OM measures the number of Tariff non Transparency non ported number queries received.
Accumulation OM	NP TnT Totals, TNT Queries Ported Across	This OM measures the number of Tariff non Transparency ported across number queries received.
Accumulation OM	NP TnT Totals, TNT Queries Ported In	This OM measures the number of Tariff non Transparency ported in number queries received.
Accumulation OM	NP TnT Totals, TNT Queries Ported Out	This OM measures the number of Tariff non Transparency ported out number queries received.
Accumulation OM	NP TnT Totals, TNT Queries Unknown	This OM measures the number of Tariff non Transparency queries received for numbers with unknown ported status.
Accumulation OM	NP TnT Totals, TNT Query Failures	This OM measures the number of Tariff non Transparency query failures during processing.
Accumulation OM	NP TnT Totals, TNT Total Messages Received	This OM measures the total number of Tariff non Transparency queries received.
Accumulation OM	NP TnT Totals, TNT Total Queries Ported	This OM measures the total number of Tariff non Transparency ported number queries received.
Accumulation OM	NP TnT Totals, TNT Transmission Failures	This OM measures the number of Tariff non Transparency failures during transmission of Ack.
Accumulation OM	Route Set Management, RouteSet Congested Count	This OM measures the number of times, a routeset went into network congestion.
Accumulation OM	Route Set Management, Routeset Man-busied Count	This OM measures the number of times a routeset was manually made unavailable.
Accumulation OM	Route Set Management, Routeset Unavailability Count	This OM measures the number of times a routeset was unavailable.
Accumulation OM	Route Set Management, Routeset Unavailability Dur.	This OM measures the total time, in seconds, a routeset was unavailable.
Accumulation OM	RTC Sanity, RTC12 Passive Audit Count	This OM hooks into the node maintenance audit, and is pegged on the control shelf CCs, when it does not receive audit request from RTC12 even once.Thus this is a passive audit of RTC
Accumulation OM	RTC Sanity, RTC15 Passive Audit Count	This OM hooks into the node maintenance audit, and is pegged on both the control shelf CCs, when it does not receive audit request from RTC15 even once. Thus this is a passive audit of RTC.
Accumulation OM	SAAL Link Management, Cum. Dur. of FE Processor Out.	This OM measures the cumulative duration in seconds during which the use of the link was precluded due to a remote (far-end) processor outage condition, summed across all far-end processor outage events.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	SAAL Link Management, Cum. Dur. of Lack-of-Credit	This OM measures the cumulative duration of time in seconds during which SSCOP had PDUs to send to its peer but could not do so because it was not given credit by the far end, summed over all the Lack-of-Credit events occurring during the measurement interval.
Accumulation OM	SAAL Link Management, Duration of Link in Service	This OM measures the number of seconds the link is regarded in service.
Accumulation OM	SAAL Link Management, Invalid SSCOP PDUs Rx	This OM measures the number of Invalid SSCOP PDUs Received.
Accumulation OM	SAAL Link Management, Lack of Credit Events	This OM measures the number of Lack-of-Credit Events.
Accumulation OM	SAAL Link Management, PDUs Tx Requiring RTx	This OM measures the number of SSCOP PDUs transmitted that required retransmission because they were not acknowledged by the far-end's SSCOP peer.
Accumulation OM	SAAL Link Management, Signaling Link Alig. Failures	This OM measures the number of Signaling Link Alignment Failures.
Accumulation OM	SAAL Link Management, SSCOP Connection Disconnects	This OM measures the number of SSCOP Connection Disconnects which are characterized by the expiry of Timer_NO_RESPONSE.
Accumulation OM	SAAL Link Management, SSCOP Connection Init. Fails	This OM measures the number of SSCOP Initiation Failures, i.e. the inability to establish an SSCOP Connection.
Accumulation OM	SAAL Link Management, SSCOP Connection Re-est/Resync	This OM measures the number of SSCOP Re-establishments/Resynchronizations.
Accumulation OM	SAAL Link Management, SSCOP Connection Sum-of-Errors	This OM measures the total number of SSCOP Connection Disconnects, Connection Initiation Failures and Connection Re-establishment/Resynchronization.
Accumulation OM	SAAL Link Management, SSCOP PDUs Sum-of-Errors	This OM measures the total number of Unexpected SSCOP PDUs, Invalid SSCOP PDUs and SSCOP PDUs with Other/List Element Errors.
Accumulation OM	SAAL Link Management, SSCOP PDUs with List Elem. Errs	This OM measures the number of SSCOP PDUs Received with List Element Errors.
Accumulation OM	SAAL Link Management, Unexpected SSCOP PDUs Rx	This OM measures the number of Unexpected SSCOP PDUs Received.
Accumulation OM	SAAL Link Traffic, PDU Octets RTx	This OM measures the number of octets associated with retransmitted SSCOP Sequenced Data PDUs.
Accumulation OM	SAAL Link Traffic, PDU Octets Rx	This OM measures the number of octets associated with SSCOP Sequenced Data PDUs received.
Accumulation OM	SAAL Link Traffic, PDU Octets Tx	This OM measures the number of octets associated with SSCOP Sequenced Data PDUs transmitted, including retransmissions.
Accumulation OM	SAAL Link Traffic, PDUs RTx	This OM measures the number of SSCOP Sequenced Data PDUs retransmitted.
Accumulation OM	SAAL Link Traffic, PDUs Rx	This OM measures the number of SSCOP Sequenced Data PDUs received.
Accumulation OM	SAAL Link Traffic, PDUs Tx	This OM measures the number of SSCOP Sequenced Data PDUs transmitted including retransmissions.
Accumulation OM	SAAL Link Traffic, Total PDU Octets Rx	This OM measures the number of octets associated with received SSCOP PDUs of all types.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	SAAL Link Traffic, Total PDU Octets Tx	This OM measures the number of octets associated with transmitted SSCOP PDUs of all types which may include Sequenced Data PDU retransmissions.
Accumulation OM	SAAL Link Traffic, Total PDUs Rx	This OM measures the number of SSCOP PDUs of all types received.
Accumulation OM	SAAL Link Traffic, Total PDUs Tx	This OM measures the number of transmitted SSCOP PDUs of all types including Sequenced Data PDU retransmissions.
Accumulation OM	SCCP GTT, Alt Routing on Cong Count	This OM measures the number of times a message is routed to the backup system because the routeset to the primary system is congested.
Accumulation OM	SCCP GTT, GTT Performed Count	This OM measures the total number of MSUs that successfully completed GTT (that is, a match was found for the global title). The count is kept across all translation types.
Accumulation OM	SCCP GTT, Hop Counter Violation Count	This OM measures the number of times that a SCCP hop counter violation has occurred.
Accumulation OM	SCCP GTT, No Translation for Addr Count	This OM measures the number of times a match could not be found for the GTA in the translation table. The count is kept across all translation types.
Accumulation OM	SCCP GTT, Trans Type Not Found Count	This OM measures the number of times the translation type specified in the MSU was not supported by the USP.
Accumulation OM	SCCP Local Subsystem, # Msgs for Local SS discarded	This OM measures the number of messages destined to local subsystems that were discarded.
Accumulation OM	SCCP Local Subsystem, # Msgs for Local SS UDTSed	This OM measures the number of messages destined to local subsystems that receive an error response (UDTS).
Accumulation OM	SCCP Local Subsystem, Subsystem Activated	This OM measures the number of times a subsystem has been manually activated.
Accumulation OM	SCCP Local Subsystem, Subsystem Allowed	This OM measures the number of times a subsystem has gone in service (allowed).
Accumulation OM	SCCP Local Subsystem, Subsystem Allowed Duration	This OM measures the total duration that the subsystem was in service (allowed).
Accumulation OM	SCCP Local Subsystem, Subsystem Deactivated	This OM measures the number of times a subsystem has been manually deactivated.
Accumulation OM	SCCP Local Subsystem, Subsystem Prohibited	This OM measures the number of times a subsystem has gone out of service (prohibited). Unit of measure is a 10 second period.
Accumulation OM	SCCP Local Subsystem, Subsystem Prohibited Duration	This OM measures the total duration that a subsystem was out of service (prohibited). Unit of measure is a 10 second period.
Accumulation OM	SCCP LSS Instance, SSI Activated	This OM measures the number of times a subsystem instance has been manually activated.
Accumulation OM	SCCP LSS Instance, SSI Allowed	This OM measures the number of times a subsystem instance has gone in service (allowed).
Accumulation OM	SCCP LSS Instance, SSI Allowed Duration	This OM measures the duration that the subsystem instance was in service (allowed). Unit of measure is a 10 second period.
Accumulation OM	SCCP LSS Instance, SSI Application Failure	This OM measures the number of times a subsystem instance has gone out of service (application failure).

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	SCCP LSS Instance, SSI Congested	This OM measures the number of times a subsystem instance has gone into congestion.
Accumulation OM	SCCP LSS Instance, SSI Deactivated	This OM measures the number of times a subsystem instance has gone out of service (manually deactivated).
Accumulation OM	SCCP LSS Instance, SSI Platform Failure	This OM measures the number of times a subsystem instance has gone out of service (platform failure).
Accumulation OM	SCCP LSS Instance, SSI Prohibited Duration	This OM measures the duration a local subsystem instance has been out of service (prohibited). Unit of measure is a 10 second period.
Accumulation OM	SCCP System Totals, Conn-Orient IP Dist Viol Count	This OM measures the number of IP originated connection-oriented messages that were discarded because they requested SCCP distribution
Accumulation OM	SCCP System Totals, Conn-Orient Msg Handled Count	This OM measures the number of connection- oriented messages that were successfully routed
Accumulation OM	SCCP System Totals, Conn-Orient Msg Rtg Fail Count	This OM measures the number of connection- oriented messages that the USP was unable to route
Accumulation OM	SCCP System Totals, LUDT Msg Rcvd Count	This OM measures the number of LUDT messages that the SCCP level received.
Accumulation OM	SCCP System Totals, LUDT Msg Sent Count	This OM measures the number of LUDT messages that the SCCP level sent.
Accumulation OM	SCCP System Totals, LUDTS Msg Rcvd Count	This OM measures the number of LUDTS messages that the SCCP level received.
Accumulation OM	SCCP System Totals, LUDTS Msg Sent Count	This OM measures the number of LUDTS messages that the SCCP level sent.
Accumulation OM	SCCP System Totals, Msg Incompatibility	This OM measures the number of times XUDT to UDT conversion fails.
Accumulation OM	SCCP System Totals, Msg too large for segmentation	This OM measures the number of times segmentation fails due to an over-long message.
Accumulation OM	SCCP System Totals, MSUs Disc-Unrec SCCP Msg Count	This OM measures the number of MSUs discarded because of an unrecognized SCCP message type.
Accumulation OM	SCCP System Totals, Out of sequence SCCP msg count	This OM measures the number of times Segments are received out of sequence
Accumulation OM	SCCP System Totals, Reassembly buffer unavailable	This OM measures the number of times Reassembly resources unavailable occurred
Accumulation OM	SCCP System Totals, Reassembly failed	This OM measures the number of times Reassembly fails for any non-specified reason.
Accumulation OM	SCCP System Totals, Reassembly Timer Expired	This OM measures the number of times Reassembly Timer expired
Accumulation OM	SCCP System Totals, Routing Failure - Unequip.User	This OM measures the number of times SCCP Routing control fails to find a subsystem to route the message.
Accumulation OM	SCCP System Totals, SCCP Routing Failure Count	This OM measures the number of messages that SCCP was unable to route.
Accumulation OM	SCCP System Totals, Segmentation failed	This OM measures the number of times segmentation fails for any non-specified reason.
Accumulation OM	SCCP System Totals, Segmentation not supported	This OM measures the number of messages dumped because segmentation is not supported

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	SCCP System Totals, SSA Received Count	This OM measures the number of subsystem-allowed (SSA) messages received.
Accumulation OM	SCCP System Totals, SSA Transmitted Count	This OM measures the number of subsystem-allowed (SSA) messages transmitted.
Accumulation OM	SCCP System Totals, SSP Received Count	This OM measures the number of subsystem-prohibited (SSP) messages received.
Accumulation OM	SCCP System Totals, SSP Transmitted Count	This OM measures the number of subsystem-prohibited (SSP) messages transmitted.
Accumulation OM	SCCP System Totals, SST Received Count	This OM measures the number of subsystem-status-test (SST) messages received.
Accumulation OM	SCCP System Totals, SST Transmitted Count	This OM measures the number of subsystem-status-test (SST) messages transmitted.
Accumulation OM	SCCP System Totals, Total messages handled	This OM measures all messages processed by SCCP routing control in both incoming and outgoing directions, whether or not the message is processed or delivered successfully. It includes Class 2 and Class 3 connection oriented messages. It does not include Subsystem Status messages such as SSP, SSA, or SST.
Accumulation OM	SCCP System Totals, UDT Msg Rcvd Count	This OM measures the number of UDT messages that the SCCP level received.
Accumulation OM	SCCP System Totals, UDT Msg Sent Count	This OM measures the number of UDT messages sent from the SCCP level.
Accumulation OM	SCCP System Totals, UDTS Msg Rcvd Count	This OM measures the number of UDTS messages that the SCCP level received.
Accumulation OM	SCCP System Totals, UDTS Msg Sent Count	This OM measures the number of UDTS messages sent from the SCCP level.
Accumulation OM	SCCP System Totals, XUDT Msg Rcvd Count	This OM measures the number of XUDT messages that the SCCP level received.
Accumulation OM	SCCP System Totals, XUDT Msg Sent Count	This OM measures the number of XUDT messages sent from the SCCP level.
Accumulation OM	SCCP System Totals, XUDTS Hopcounter violation	This OM measures the number of MSUs discarded because of Hopcounter violations.
Accumulation OM	SCCP System Totals, XUDTS Msg Rcvd Count	This OM measures the number of XUDTS messages that the SCCP level received.
Accumulation OM	SCCP System Totals, XUDTS Msg Sent Count	This OM measures the number of XUDTS messages sent from the SCCP level.
Accumulation OM	SCTP Management/Traffic Counts, Association Aborted Count	This OM measures the number of associations that are aborted by the application, the peer connection or a failure in the network.
Accumulation OM	SCTP Management/Traffic Counts, Association Establish Attempts	This OM measures the number of associations which the user or peer SCTP tried to established.
Accumulation OM	SCTP Management/Traffic Counts, Association Terminated Count	This OM measures the number of associations that are terminated by the application or the peer connection.
Accumulation OM	SCTP Management/Traffic Counts, Chunk Retransmitted Count	This OM measures the number of SCTP chunks retransmitted due to SCTP Packets or SCTP Sacks lost in the network. Note: A SCTP packet may contain more than one chunk.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	SCTP Management/Traffic Counts, Chunks Received Count	This OM measures the number of SCTP chunks received. Note: A SCTP packet may contain more than one chunk.
Accumulation OM	SCTP Management/Traffic Counts, Chunks Transmitted Count	This OM measures the number of SCTP chunks transmitted. Note: A SCTP packet may contain more than one chunk.
Accumulation OM	SCTP Management/Traffic Counts, Established Association Count	This OM measures the number of associations which are in a established state.
Accumulation OM	SCTP Management/Traffic Counts, Out of Blue SCTP Packet	This OM measures the number of SCTP packets that are received but are not able to identify the association to which they belong.
Accumulation OM	SIP Application Service Totals, SIP Call Timeout	This OM measures the total number of SIP call timeout. This value will be pegged when the SIP transaction stay alive for too long and get cleaned up by the Transaction audit.
Accumulation OM	SIP Application Service Totals, SIP message Received	This OM measures the total number of SIP message received from the Application Server (including all SIP Response msgs)
Accumulation OM	SIP Application Service Totals, SIP message Transmitted	This OM measures the total number of SIP message transmitted to the Application Server (including all Invite/Notify msgs)
Accumulation OM	SIP Application Service Totals, SIP TCAP Application Timeout	This OM measures the total number of SIP TCAP application timeout
Accumulation OM	SIP Application Service Totals, TCAP message received	This OM measures the total number of TCAP orig Or UNI MSUs received for the SIP application on this IP LINK Node.
Accumulation OM	SIP Application Service Totals, TCAP message transmitted	This OM measures the total number of TCAP Response MSUs received for the SIP application on this IP LINK Node
Accumulation OM	SLR Database Totals, Add/Change Updates	This OM measures the total number of add/change updates received from the HLR provisioning system.
Accumulation OM	SLR Database Totals, Delete Updates	This OM measures the total number of delete updates received from the HLR provisioning system.
Accumulation OM	SLR Database Totals, Emergency Updates	This OM measures the total number of application database updates received from the USP debug facility and can only be displayed from the debug facility Note: Debug is only accessible by Nortel Networks Support Personnel.
Accumulation OM	SLR Database Totals, Operational Time	This OM measures the total time within the OM interval that the SLRDB was operational.
Accumulation OM	SLR Database Totals, Retransmitted Updates	This OM measures the total number of updates retransmitted within the BroadBand STP.
Accumulation OM	SLR LSSI Totals, Total Failed Queries	This OM measures the total number of SLR queries received by an SLR application database system node that failed for any reason across all services and message types.
Accumulation OM	SLR LSSI Totals, Total Queries Received	This OM measures the total number of SLR queries received by an SLR application database system node across all services and message types.
Accumulation OM	SLR Message Type Totals, IMSI Failed Queries	This OM measures the total number of IMSI queries received by an SLR application database system node that failed for any reason.
Accumulation OM	SLR Message Type Totals, IMSI Failed SLRDB Lookup	This OM measures the total number of IMSI queries received by an SLR application database system node that failed in their SLRDB lookup.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	SLR Message Type Totals, IMSI Query Received	This OM measures the total number of IMSI queries received by an SLR application database system node.
Accumulation OM	SLR Message Type Totals, IMSI Successful SLRDB Lookup	This OM measures the total number of IMSI queries received by an SLR application database system node that succeeded in their SLRDB lookup.
Accumulation OM	SLR Message Type Totals, MSISDN Failed Queries	This OM measures the total number of MSISDN queries received by an SLR application database system node that failed for any reason.
Accumulation OM	SLR Message Type Totals, MSISDN Failed SLRDB Lookup	This OM measures the total number of MSISDN queries received by an SLR application database system node that failed in their SLRDB lookup.
Accumulation OM	SLR Message Type Totals, MSISDN Query Received	This OM measures the total number of MSISDN queries received by an SLR application database system node.
Accumulation OM	SLR Message Type Totals, MSISDN Successful SLRDB Lookup	This OM measures the total number of MSISDN queries received by an SLR application database system node that succeeded in their SLRDB lookup.
Accumulation OM	SLR SMI Totals, High Congestion	This OM measures the total number of times that the high level congestion state was entered.
Accumulation OM	SLR SMI Totals, Login Failures	This OM measures the total number of failed HLR provisioning system login attempts.
Accumulation OM	SLR SMI Totals, Low Congestion	This OM measures the total number of times that the low level congestion state was entered.
Accumulation OM	SLR SMI Totals, Medium Congestion	This OM measures the total number of times that the medium level congestion state was entered.
Accumulation OM	SLR SMI Totals, Messages Failed Authentication	This OM measures the total number of received messages from the HLR provisioning system that failed authentication of the retrieved RN against an associated GTT entry with an RN matching the retrieved value.
Accumulation OM	SLR SMI Totals, Messages Invalid	This OM measures the total number of invalid messages received from the HLR provisioning system.
Accumulation OM	SLR SMI Totals, Messages Passed Authentication	This OM measures the total number of received messages from the HLR provisioning system that successfully authenticated the retrieved RN against an associated GTT entry with an RN matching the retrieved value.
Accumulation OM	SLR SMI Totals, Messages Received	This OM measures the total number of messages received from the HLR provisioning system.
Accumulation OM	SLR SMI Totals, Messages Rejected	This OM measures the total number of received messages from the HLR provisioning system that were rejected.
Accumulation OM	Special Study Totals, MSUs Received Count	This OM measures the number of incoming MSUs acknowledged on the specified linkset with the specified OPC/DPC/SIO combination.
Accumulation OM	Special Study Totals, MSUs Transmitted Count	This OM measures the number of outgoing MSUs successfully transmitted to the far end on the specified linkset with the specified OPC/DPC/SIO combination.
Accumulation OM	Special Study Totals, Octets Received Count	This OM measures the total number of MSU octets received on a specified linkset with the specified OPC/DPC/SIO combination, including the octets removed in MTP Level 2 processing.

OM TYPE	OM TITLE	OM DESCRIPTION
Accumulation OM	Special Study Totals, Octets Transmitted Count	This OM measures the total number of MSU octets transmitted on the specified linkset with the specified OPC/DPC/SIO combination, including those octets that were added in MTP Level 2 processing.
Accumulation OM	System Node State, Disabled, Locked Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is disabled and locked.
Accumulation OM	System Node State, Disabled, Unlocked Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is disabled and unlocked.
Accumulation OM	System Node State, Enabled, Locked Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is enabled and locked.
Accumulation OM	System Node State, Enabled, Unlocked Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is enabled and unlocked.
Accumulation OM	System Node State, Locked, Off-line Duration	This OM measures the number of seconds that a specific RTC, CC, or application system node is locked and off-line.
Accumulation OM	System Totals, No Route MSU Discard Count	This OM measures the number of MSUs discarded due to routing failure of various causes (for example, an inaccessible DPC).
Accumulation OM	Task Management, Idle Task Duration	This OM measures the number of milliseconds spent in idle time.
Accumulation OM	TUP Received Message Counts, B/TUP Error No AS for OPC/CIC	This OM measures the number of TUP messages discarded as a result of not being able to find a valid AS for a given OPC/CIC.
Accumulation OM	TUP Received Message Counts, B/TUP Error No OPC/CIC Data	This OM measures the number of TUP and BTUP messages discarded as a result of missing database entry for a given OPC or OPC/CIC.
Accumulation OM	TUP Received Message Counts, B/TUP Error No Path	This OM measures the number of TUP and BTUP messages discarded as a result of not being able to find an inservice path to a given AS.
Accumulation OM	TUP Received Message Counts, B/TUP Error No Route	This OM measures the number of TUP messages discarded as a result of not being able to find a route to a given AS.
Accumulation OM	TUP Received Message Counts, BTUP Call P Received Count	This OM measures the number of BTUP call processing messages received from the SS7 Network.
Accumulation OM	TUP Received Message Counts, BTUP Maint Received Count	This OM measures the number of BTUP maintenance messages received from the SS7 Network.
Accumulation OM	TUP Received Message Counts, TUP Call P Received Count	This OM measures the number of TUP call processing messages received from the SS7 Network.
Accumulation OM	TUP Received Message Counts, TUP Maint Received Count	This OM measures the number of TUP maintenance messages received from the SS7 Network.
Accumulation OM	TUP Received Message Counts, Wrong NE Received Count	This OM measures the number of TUP messages discarded as a result of not receiving the message for a SG Network Element
Accumulation OM	UDP, Full Socket Count	This OM measures the number of counts that the udpstat full_socket variable has changed in the om period.
Maximum OM	Link Traffic, Link utilization	This OM provides percentage of link utilization. For LSL it is calculated in erlangs while for HSL it is calculated as percentage of processor utilization.

OM TYPE	OM TITLE	OM DESCRIPTION
Maximum OM	NP Database Totals, Max Average Update Rate	This OM measures the highest update rate (in updates per second) averaged over a 60 second period. ie total updates over the 60 second window divided by 60. If the number of updates received in the 60 second window is less than 60 , the OM will be 0.
Maximum OM	NP Transaction Mgmt Totals, TxMgr Percent Used	This OM measures the maximum percentage of used transactions in the Transaction Management application.
Maximum OM	SLR Database Totals, Max. Update Rate	This OM measures the highest update rate (in updates per second) during any 60 second period
No Action	System Node State, Percentage Enabled	This OM measures the percentage of time that a specific RTC, CC, or application system node is enabled, or busy (for the Processor Utilization OM, GR-82-CORE section 6.4.5, item 10). The value for this OM ranges from 0 to 100 percent.
No Action	Task Management, Collection Period Duration	This OM measures the total number of milliseconds for an OM collection period. This OM can be used to calculate the percentage of use for all the other Task Management OMs.
No action	Task Management, Level 0 Priority Task Duration	This OM measures the number of milliseconds spent in Level 0 priority task(s).
No Action	Task Management, Level 1 Priority Task Duration	This OM measures the number of milliseconds spent in Level 1 priority task(s).
No Action	Task Management, Level 2 Priority Task Duration	This OM measures the number of milliseconds spent in Level 2 priority task(s).
No Action	Task Management, Level 3 Priority Task Duration	This OM measures the number of milliseconds spent in Level 3 priority task(s).
No Action	Task Management, Level 4 Priority Task Duration	This OM measures the number of milliseconds spent in Level 4 priority task(s).
No Action	Task Management, Level 5 Priority Task Duration	This OM measures the number of milliseconds spent in Level 5 priority task(s).
No Action	Task Management, Level 6 Priority Task Duration	This OM measures the number of milliseconds spent in Level 6 priority task(s).
No Action	Task Management, Level 7 Priority Task Duration	This OM measures the number of milliseconds spent in Level 7 priority task(s).
No Action	Task Management, Level 8 Priority Task Duration	This OM measures the number of milliseconds spent in Level 8 priority task(s).
No Action	Task Management, Level 9 Priority Task Duration	This OM measures the number of milliseconds spent in Level 9 priority task(s).
No Action	Task Management, OS System Tasks Duration	This OM measures the number of milliseconds spent in VxWorks OS tasks.

New or changed in SN09

Appendix E: MG9000 Reported Alarms, Event Logs, Audit Logs

Alarm Id	Fault Type	Severity	Description	Supported	Procedure To Generate Alarm, and Alarm Recovery
norCarrFault (NORTEL-UEMG-CARRIER-MIB)					
CES305	cesLossOfCell	Major	Loss of Cells	Yes	This alarm is raised when CES IWF stops reciveing cells for the ATM network. To introduce this condition SVC between the local endpoint and the remote endpoint must be broken. This can be done 2 ways: 1. At **Dshell** prompt, type /cesnv/disconn IfIndex. 2. From EM, this can only be done for 'half services'. Disconnect the remote endpoint to observe Loss of Cells at the local. **Recovery:** The alarm will be cleared when ATM connection is restored. So, any issue with the ATM connection needs to be investigated
MGCA301	los	DS1 - Minor OC3 - Critical	lossOfSignal	yes	On DS1 Link, pull Rx fiber to set LOS
MGCA302	ais	DS1 - Minor OC3 - Critical	alarm indication signal	yes	On DS1 Link, use test set (TBERD) to inject line AIS
MGCA303	lof	DS1 - Minor OC3 - Critical	lossOfFrame	yes	On DS1 Link, Use test (TBERD) set to inject LOF
MGCA304	rai	DS1 - Minor	remote alarm indication	yes	
MGCA305	bersf	OC3 - Critical	bitErrorRate S F...	yes	On DS1 Link, Use test set (TBERD) to inject line B2, Bit Error Rate of 10e-3
MGCA306	bersd	OC3 - Major	bitErrorRate SigDegrade	yes	On DS1 Link, Use test set (TBERD) to inject line B2, Bit Error Rate of 10e-5
MGCA307	rdi	OC3 - Minor	remote defect indication	yes	On DS1 Link, Use test set (TBERD) to inject line RDI
MGCA308	plm	OC3 - Minor	path label mismatch	yes	On DS1 Link, Use test set (TBERD) to change C2 label from 0x13 to 0x00
MGCA309	lop	OC3 - Minor	loss of Pointer	yes	On DS1 Link, Use test set (TBERD) to inject path LOP error
MGCA310	uneq	OC3 - Minor	unequipped	yes	On DS1 Link, Use test set (TBERD) to set C2 to 0x00 (unequipped)
MGCA312	imaLinkLif	Minor	IMA link- Loss of IMA Frame	yes	At the IMA card pull the DS1 cable **(Can't report Alarm if link is down)**
MGCA313	imaLinkLods	Minor	IMA link- Loss of delayed synchronization	yes	This alarm cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easist way to generate is using the "fakelnkfm" command in the /hal/ima MG9K Dshell directory.
MGCA314	imaLinkRfi	Minor	IMA link- Remote failure indication	yes	At the Edgelink (or other MUX) manually send AIS to the PP15000
MGCA315	imaLinkTxMisConnect	Minor	IMA link Transmit misconnect	yes	This alarm cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easist way to generate is using the "fakelnkfm" command in the /hal/ima MG9K Dshell directory.
MGCA316	imaLinkRxMisConnect	Minor	IMA link receive misconnect	yes	Same as above
MGCA317	imaLinkTxFault	Minor	IMA link transmit fault	yes	Change the "transmit Clock Mode" to ITC on the IMA link at the PP15000
MGCA318	imaLinkRxFault	Minor	IMA link receive fault	yes	This alarm cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easist way to generate is using the "fakelnkfm" command in the /hal/ima MG9K Dshell directory.
MGCA319	imaLinkTxUnusableFe	Minor	IMA link transmit unusable far end	yes	Change the "transmit Clock Mode" to ITC on the IMA link at the PP15000
MGCA320	imaLinkRxUnusableFe	Minor	IMA link receive unusable far end	yes	Same as above
MGCA321	imaGroupStartupFe	Major	IMA group startup far end	yes	This alarm cannot be externally invoked by a manual action. It will only occur if there is some HW or SW errors. The easist way to generate is using the "fakelgrpfm" command in the /hal/ima MG9K Dshell directory.
MGCA322	imaGroupCfgAbort	Critical	IMA group configuration abort	yes	Same as above

MGCA323	imaGroupCfgAbortFe	Major	IMA group configuration abort far end	yes	Same as above
MGCA324	imaGroupInsuffLinks	Critical	IMA group insufficient links	yes	At the IMA card pull the DS1 cable **(Can't report Alarm if link is down)**
MGCA325	imaGroupInsuffLinksFe	Major	IMA group insufficient links far end	yes	Same as above
MGCA326	imaGroupBlockedFe	Minor	IMA group blocked far end	yes	Block the IMA group at the PP15000
MGCA327	imaGroupTimingSynch	Major	IMA group timing synchronization	yes	Change the "transmit Clock Mode" to ITC on the IMA link at the PP15000
MGCA328	abiLossOfClock	Critical	ABI Loss of Clock on DS512 optical link	yes	On the DS512 link, Use test set (TBERD) to set LOC
MGCA329	abiLossOfFrame	Critical	ABI Loss of Frame on DS512 optical link	yes	On the DS512 link, Use test set (TBERD) to set LOF
MGCA330	abiLowLightLevel	Critical	ABI Loss of Signal (low light level) on DS512 optical link	yes	On the DS512 link, Use test set (TBERD) to set LOS
MGCA331	abiChannelParityError	Minor	ABI Channel parity error on DS512 optical link	yes	On the DS512 link, Use test set (TBERD) to set C2 to 0x00 (unequipped)
MGCA332	tim	Minor	SDH Path Trace Identifier Mismatch Alarm (only applies to SDH and not SONET). The Path Trace Identifier being seen by the OC3 card at the carrier Path level does not match what has been provisioned for that carrier.	yes	**Recovery:** 1) Ensure that the host carrier is generating the correct Trace Identifier . 2) Ensure that the correct fiber is connected to the OC3 card. 3) Update the Path Trace Identifier at the LCI. 4) Using the STM-1 EM GUI screen button check the transmitted Path Trace Identifier to ensure it is the "provisioned" Path Trace Identifier.
MGCA333	ds3Ais		DS3 - Alarm Indication Signal - Check far-end carrier faults	yes	
MGCA334	ds3Lof		DS3 - Loss Of Frame	yes	
MGCA335	ds3Rai		DS3 - Remote Indication Signal - Check far-end carrier faults	yes	
nnAtmFaultType (NORTEL-UEMG-ATM-MIB)					
VC301	vclTpAis	Minor	atmVcl Alarm indication signal	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" aisalarm. **Recovery:** Tear down the SVC and reestablish, check DS1 card for proper operation.
VC302	vclTpRdi	Minor	atmVcl Remote Detection Indicator	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" rdialarm. **Recovery:** Tear down the SVC and reestablish, check DS1 card for proper operation.
VC303	vclLoc	Minor	loss of continuity, vcl	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" ccalarmon. **Recovery:** Tear down the SVC and reestablish, check DS1 card for proper operation.
VC304	vccTpAis	Minor	atmVcc Alarm indication signal	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" aisalarm. **Recovery**: Tear down the SVC and reestablish, check DS1 card for proper operation.
VC305	vccTpRdi	Minor	atmVcc Remote Detection Indicator	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" rdialarm. **Recovery:** Tear down the SVC and reestablish, check DS1 card for proper operation.
VC306	vccLoc	Minor	loss of continuity, vcc	yes	This Alarm cannot be generated under normal condition or with a test set. The following Dshell commacd must be used "cd atmss/atmoam" ccalarmon. **Recovery:** Tear down the SVC and reestablish, check DS1 card for proper operation.
nnShfFault (NORTEL-UEMG-SHF-MIB)					
SHLF301	shelfTalkBatteryA	Critical	SIC Talk Battery A	yes	Pull Talk Battery A Fuse (at BIP panel) **Recovery**: Check Fuse
SHLF302	shelfTalkBatteryB	Critical	SIC Talk Battery B	yes	Pull Talk battery B fuse (at BIP panel)
SHLF303	shelfSignalBatteryA	Major	SIC Signal Battery A	yes	Pull Signal Battery A fuse (at BIP panel) **Recovery:** Check Fuse

SHLF304	shelfSignalBatteryB	Major	SIC Signal Battery B	yes	Pull Signal Battery B fuse (at BIP panel) **Recovery:** Check Fuse
SHLF305	shelfSignalBatteryAfuse	Major	SIC Signal Battery A Fuse	yes	Put Blown Signal Battery A fuse in BIP Panel **Recovery:** Check Fuse
SHLF306	shelfSignalBatteryBfuse	Major	SIC Signal Battery B Fuse	yes	Put Blown Signal Battery B fuse in BIP Panel **Recovery:** Check Fuse
SHLF307	shelfFailLED	Indeterminate	SIC Shelf Fail LED	yes	Any Shelf failure **Recovery:** Remove all Shelf Failures.
SHLF308	bipSignalBatteryA1	Major	BIP Signal Battery A1	yes	Pull Signal Battery A1 Fuse (at BIP panel) **Recovery:** Check Fuse
SHLF309	bipSignalBatteryA2	Major	BIP Signal Battery A2	yes	Pull Signal Battery A2 Fuse (at BIP panel) **Recovery:** Check Fuse
SHLF310	bipSignalBatteryB1	Major	BIP Signal Battery B1	yes	Pull Signal Battery B1 Fuse (at BIP panel) **Recovery:** Check Fuse
SHLF311	bipSignalBatteryB2	Major	BIP Signal Battery B2	yes	Pull Signal Battery B2 Fuse (at BIP panel) **Recovery:** Check Fuse
SHLF312	bipTalkBatteryA	Minor	BIP Talk Battery A	yes	Remove (or Offline/Lock ate EM) TB A Filter card **Recovery:** Re-insert (or Unlock/Online ate EM) TB A Filtercard
SHLF313	bipTalkBatteryB	Minor	BIP Talk Battery B	yes	Remove (or Offline/Lock ate EM) TB B Filter card **Recovery:** Re-insert (or Unlock/Online ate EM) TB A Filtercard
SHLF314	bipFilterA	Minor	BIP Filter A Fail	yes	Requires Bad card or use of Dshell to generate the alarm **Recovery**: Replace bad card.
SHLF315	bipFilterB	Minor	BIP Filter B Fail	yes	Requires Bad card or use of Dshell to generate the alarm **Recovery**: Replace bad card.
SHLF316	bipScanPoint1	Indeterminate	BIP Scan Point 1	yes	Requires closure of Specific Scan Point pins on the Scan Point cable. This may require a test board. Alternatively **Dshell** can be used to generate this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend **XX** 03 01 b5 70 06 07 00 82 **YY** 01 00 b2 e9". To clear the alarm use "/glan/dsend **XX** 03 01 b5 70 06 07 00 82 **YY** 00 00 b2 e9". XX = ITP slot number and YY = 08. **Recovery:** Investigate Scan Point Source to determine problem.
SHLF317	bipScanPoint2	Indeterminate	BIP Scan Point 2	yes	Same as above except XX = 09 **Recovery:** Same as above.
SHLF318	bipScanPoint3	Indeterminate	BIP Scan Point 3	yes	Same as above except XX = 0a **Recovery:** Same as above.
SHLF319	bipScanPoint4	Indeterminate	BIP Scan Point 4	yes	Same as above except XX = 0b **Recovery:** Same as above.
SHLF320	bipScanPoint5	Indeterminate	BIP Scan Point 5	yes	Same as above except XX = 0c **Recovery:** Same as above.
SHLF321	bipScanPoint6	Indeterminate	BIP Scan Point 6	yes	Same as above except XX = 0d **Recovery:** Same as above.
SHLF322	bipScanPoint7	Indeterminate	BIP Scan Point 7	yes	Same as above except XX = 0e **Recovery:** Same as above.
SHLF323	bipScanPoint8	Indeterminate	BIP Scan Point 8	yes	Same as above except XX = 0f **Recovery:** Same as above.
SHLF324	bipScanPoint9	Indeterminate	BIP Scan Point 9	yes	Same as above except XX = 10 **Recovery:** Same as above.
SHLF325	bipScanPoint10	Indeterminate	BIP Scan Point 10	yes	Same as above except XX = 11 **Recovery:** Same as above.
SHLF326	bipScanPoint11	Indeterminate	BIP Scan Point 11	yes	Same as above except XX = 12 **Recovery:** Same as above.
SHLF327	bipTalkBatteryA1	Major	Talk Battery A1 Power Feed	yes	Pull PDA fuse **Recovery:** Check Power feed connection and PDA fuse
SHLF328	bipTalkBatteryA2	Major	Talk Battery A Power Feed	yes	Pull PDA fuse **Recovery:** Check Power feed connection and PDA fuse
SHLF329	bipTalkBatteryB1	Major	Talk Battery B1 Power Feed	yes	Pull PDA fuse **Recovery:** Check Power feed connection and PDA fuse
SHLF330	bipTalkBatteryB2	Major	Talk Battery B2 Power Feed	yes	Pull PDA fuse **Recovery:** Check Power feed connection and PDA fuse

SHLF332	bipEcuTemp0	Minor	BIP Environmental Control Unit 0 Temperature	yes	Through **Dshell** reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend **XX** 03 01 b5 70 06 07 00 82 **YY** 01 00 b2 e9". To clear the alarm use "/glan/dsend **XX** 03 01 b5 70 06 07 00 82 **YY** 00 00 b2 e9". XX = ITP slot number and YY = 18
SHLF333	bipEcuTemp1	Minor	BIP Environmental Control Unit 1 Temperature	yes	Through **Dshell** reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend **XX** 03 01 b5 70 06 07 00 82 **YY** 01 00 b2 e9". To clear the alarm use "/glan/dsend **XX** 03 01 b5 70 06 07 00 82 **YY** 00 00 b2 e9". XX = ITP slot number and YY = 1A
SHLF334	bipEcuFan0	Minor	BIP Environmental Control Unit 0 Fan	yes	Remove Fan Cable **Recovery:** Check Fan cable, fuses, or replace fan
SHLF335	bipEcuFan1	Minor	BIP Environmental Control Unit 1 Fan	yes	Remove Fan Cable **Recovery:** Check Fan cable, fuses, or replace fan
SHLF336	bipRemoteAlarmcutoff	Indeterminate	BIP Remote Alarm Cut Off	yes	Engage Remote Alarm Cut Off button on BIP panel **Recovery:** Disengage Alarm cut Off button on BIP panel.
SHLF337	bipLocalAlarmcutoff	Indeterminate	BIP Local Alarm Cut Off	yes	Engage Alarm Cut Off button on BIP panel **Recovery:** Disengage Remote Alarm cut Off button on BIP panel.
SHLF338	bipAbsFusefail	Major	BIP ABS Fuse Fail	yes	Remove ABS fuse **Recovery:** Replace ABS fuse.
SHLF339	bipAbsPowerSupply	Critical	BIP ABS Battery Power Supply	yes	Remove ABS power cable **Recovery:** Check (replace if necessary) ABS Power supply, Check Power supply power cables and leads.
SHLF340	bipShfBreakerTrip	Major	BIP Shelf Circuit Breaker Trip	yes	Turn off Breaker **Recovery:** Check Breaker; turn on Breaker.
SHLF341	bipCsApresence	Major	Presence of BIP's Current-Sense Card A	yes	Remove BIP's Current-Sense Card A **Recovery:** Install BIP's Current-Sense Card A
SHLF342	bipCsBpresence	Major	Presence of BIP's Current-Sense Card B	yes	Remove BIP's Current-Sense Card B **Recovery:** Install BIP's Current-Sense Card B
SHLF343	bipAlmRelayPresence	Major	Presence of BIP's Alarm Relay Card	yes	Remove BIP's Alarm Relay Card **Recovery:** Install BIP's Alarm Relay Card
SHLF344	bipCSAshf0HighThres	Minor	Current-Sense Card A Shelf 0 High Threshold exceeded	yes	Through **Dshell** reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend **XX** 03 01 b5 70 06 07 7a 92 **YY** 04 c0 ff". To clear the alarm use "/glan/dsend **XX** 03 01 b5 70 06 07 68 92 **YY** 03 c0 ff". XX = ITP slot number and YY = 3E
SHLF345	bipCSAshf1HighThres	Minor	Current-Sense Card A Shelf 1 High Threshold exceeded	yes	Same as above except YY = 3F
SHLF346	bipCSAshf2HighThres	Minor	Current-Sense Card A Shelf 2 High Threshold exceeded	yes	Same as above except YY = 40
SHLF347	bipCSAshf3HighThres	Minor	Current-Sense Card A Shelf 3 High Threshold exceeded	yes	Same as above except YY = 41
SHLF348	bipCSBshf0HighThres	Minor	Current-Sense Card B Shelf 0 High Threshold exceeded	yes	Same as above except YY = 42
SHLF349	bipCSBshf1HighThres	Minor	Current-Sense Card B Shelf 1 High Threshold exceeded	yes	Same as above except YY = 43
SHLF350	bipCSBshf2HighThres	Minor	Current-Sense Card B Shelf 2 High Threshold exceeded	yes	Same as above except YY = 44
SHLF351	bipCSBshf3HighThres	Minor	Current-Sense Card B Shelf 3 High Threshold exceeded	yes	Same as above except YY = 45
SHLF352	bipTempHighThres	Minor	Current High Temperature Threshold exceeded	yes	Through **Dshell** reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend **XX** 03 01 b5 70 06 07 50 92 3d 04 co ff". XX = ITP slot number.
SHLF353	bipCSAshf0LowThres	Minor	Current-Sense Card A Shelf 0 Low Threshold exceeded	yes	Through **Dshell** reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend **XX** 03 01 b5 70 06 07 5f 92 **YY** 02 c0 ff". To clear the alarm use "/glan/dsend **XX** 03 01 b5 70 06 07 58 92 **YY** 01 c0 ff". XX = ITP slot number and YY = 3E
SHLF354	bipCSAshf1LowThres	Minor	Current-Sense Card A Shelf 1 Low Threshold exceeded	yes	Same as above except YY = 3F
SHLF355	bipCSAshf2LowThres	Minor	Current-Sense Card A Shelf 2 Low Threshold exceeded	yes	Same as above except YY = 40

SHLF356	bipCSAshf3LowThres	Minor	Current-Sense Card A Shelf 3 Low Threshold exceeded	yes	Same as above except YY = 41
SHLF357	bipCSBshf0LowThres	Minor	Current-Sense Card B Shelf 0 Low Threshold exceeded	yes	Same as above except YY = 42
SHLF358	bipCSBshf1LowThres	Minor	Current-Sense Card B Shelf 1 Low Threshold exceeded	yes	Same as above except YY = 43
SHLF359	bipCSBshf2LowThres	Minor	Current-Sense Card B Shelf 2 Low Threshold exceeded	yes	Same as above except YY = 44
SHLF360	bipCSBshf3LowThres	Minor	Current-Sense Card B Shelf 3 Low Threshold exceeded	yes	Same as above except YY = 45
SHLF361	bipTempLowThres	Minor	Current Low Temperature Threshold exceeded	yes	Through **Dshell** reset the the threshold to value that will trigger this alarm. To do this Telnet into an active ITX card and enter the following command "/glan/dsend **XX** 03 01 b5 70 06 07 00 92 3d 01 c0 ff". XX = ITP slot number.
SHLF362	bipSignalBattery Fuse	Major	Status of the Signal Battery Fuse	yes	Pull Signal Battery Fuse at the BIP panel **Recovery:** Check fuse and replace if necessary.
SHLF363	bipTalkBatteryAFuse	Major	Status of Talk Battery A Fuse	yes	Pull Talk Battery A Fuse at the BIP panel **Recovery:** Check fuse and replace if necessary.
SHLF364	bipTalkBatteryBFuse	Major	Status of Talk Battery B Fuse	yes	Pull Talk Battery B Fuse at the BIP panel **Recovery:** Check fuse and replace if necessary.
SHLF365	bipEcuFuse0	Minor	Status of Cooling Unit 0 Fuse	yes	Pull Cooling Unit 0 Fuse at the BIP panel **Recovery:** Check fuse and replace if necessary.
SHLF366	bipEcuFuse1	Minor	Status of Cooling Unit 1 Fuse	yes	Pull Cooling Unit 1 Fuse at the BIP panel **Recovery:** Check fuse and replace if necessary.
SHLF367	bipEndAisleFuse	Minor	Status of the End-Aisle Fuse	yes	Pull End-Aisle Fuse at the BIP panel **Recovery:** Check fuse and replace if necessary.
SHLF368	bipSignalDistribution1	Indeterminate	BIP Signal Distribution Point 1	yes	At the MG9000 EM enable this SDP
SHLF369	bipSignalDistribution2	Indeterminate	BIP Signal Distribution Point 2	yes	At the MG9000 EM enable this SDP
SHLF370	bipSignalDistribution3	Indeterminate	BIP Signal Distribution Point 3	yes	At the MG9000 EM enable this SDP
SHLF371	bipSignalDistribution4	Indeterminate	BIP Signal Distribution Point 4	yes	At the MG9000 EM enable this SDP
SHLF372	bipVisualCritical	Indeterminate	BIP Visual Critical	yes	Generate any Critical Alarm on an MG9000 within the Frame **Recovery:** Clear any Critical Alarm on an MG9000 within the Frame.
SHLF373	bipVisualMajor	Indeterminate	BIP Visual Major	yes	Generate any Major Alarm on an MG9000 within the Frame **Recovery:** Clear any Major Alarm on an MG9000 within the Frame.
SHLF374	bipVisualMinor	Indeterminate	BIP Visual Minor	yes	Generate any Minor Alarm on an MG9000 within the Frame **Recovery:** Clear any Minor Alarm on an MG9000 within the Frame.
SHLF375	bipAudibleCritical	Indeterminate	BIP Audible Critical	yes	Generate any Critical Alarm on an MG9000 within the Frame **Recovery:** Clear any Critical Alarm on an MG9000 within the Frame.
SHLF376	bipAudibleMajor	Indeterminate	BIP Audible Major	yes	Generate any Major Alarm on an MG9000 within the Frame **Recovery:** Clear any Major Alarm on an MG9000 within the Frame.
SHLF377	bipAudibleMinor	Indeterminate	BIP Audible Minor	yes	Generate any Minor Alarm on an MG9000 within the Frame **Recovery:** Clear any Minor Alarm on an MG9000 within the Frame.
SHLF378	bipAlarmCutOffLED	Indeterminate	BIP Alarm CutOff LED	yes	Engage Alarm Cut Off button on BIP panel **Recovery:** Disengage Remote Alarm cut Off button on BIP panel.
SHLF379	bipTalkBatteryFaiIALED	Indeterminate	BIP Talk Battery A Fail LED	yes	Remove (or Offline/Lock ate EM) TB A Filter card **Recovery:** Re-insert (or Unlock/Online ate EM) TB A Filtercard.
SHLF380	bipTalkBatteryFaiIBLED	Indeterminate	BIP Talk Battery B Fail LED	yes	Remove (or Offline/Lock ate EM) TB B Filter card **Recovery:** Re-insert (or Unlock/Online ate EM) TB B Filtercard.

SHLF381	bipCriticalLEDbank	Indeterminate	BIP Critical LED Bank	yes	Generate any Critical Alarm on an MG9000 within the Frame **Recovery:** Clear any Critical Alarm on an MG9000 within the Frame.
SHLF382	bipMajorLEDbank	Indeterminate	BIP Major LED Bank	yes	Generate any Major Alarm on an MG9000 within the Frame **Recovery:** Clear any Major Alarm on an MG9000 within the Frame.
SHLF383	bipMinorLEDbank	Indeterminate	BIP Minor LED Bank	yes	Generate any Minor Alarm on an MG9000 within the Frame **Recovery:** Clear any Minor Alarm on an MG9000 within the Frame.
SHLF384	bipEcu1LED	Indeterminate	BIP Environmental Control Unit 0 LED	yes	Remove Fan Cable **Recovery:** Check Fan cable, fuses, or replace fan
SHLF385	bipEcu2LED	Indeterminate	BIP Environmental Control Unit 1 LED	yes	Remove Fan Cable **Recovery:** Check Fan cable, fuses, or replace fan
SHLF386	bipAlarmFailLED	Indeterminate	BIP Alarm Processor Card Fail LED	yes	At EM Offline/Lock the BIP Alarm Processor Card **Recovery:** At EM Offline/Unlock the BIP Alarm Processor Card.
SHLF387	bipAisleAlarm	Indeterminate	BIP Aisle Alarm	yes	Generate any SHLF alarm **Recovery:** Clear all SHLF alarms.
SHLF388	bipFrameFail	Indeterminate	BIP Frame Fail	yes	Generate any Frame alarm **Recovery:** Clear all Frame alarms.
SHLF389	bipAlmRelayLed	Indeterminate	Presence of BIP's Alarm Relay Card LED	yes	Remove BIP's Alarm Relay Card **Recovery:** Install BIP's Alarm Relay Card
SHLF390	bipCsAled	Indeterminate	Status of Current-Sense Card A LED	yes	At EM Offline/Lock the BIP Current-Sense Card A **Recovery:** At EM Offline/Unlock the BIP Current-Sense Card A.
SHLF391	bipCsBled	Indeterminate	Status of Current-Sense Card B LED	yes	At EM Offline/Lock the BIP Current-Sense Card B **Recovery:** At EM Offline/Unlock the BIP Current-Sense Card B.
SHLF392	shelfCompatibility		This log is generated when a shelfCompatibility fault is received	yes	
SHLF393	cardDiscovery		This log is generated when a cardDiscovery fault is received	yes	
	cardDiscPowIo		This log is generated when a cardDiscPowIo fault is received	yes	
	cardDiscPowSic		This log is generated when a cardDiscPowSic fault is received	yes	
	cardDiscSlot02		This log is generated when a cardDiscSlot2 fault is received	yes	
	cardDiscSlot03		This log is generated when a cardDiscSlot3 fault is received	yes	
	cardDiscSlot04		This log is generated when a cardDiscSlot4 fault is received	yes	
	cardDiscSlot05		This log is generated when a cardDiscSlot5 fault is received	yes	
	cardDiscSlot06		This log is generated when a cardDiscSlot6 fault is received	yes	
	cardDiscSlot07		This log is generated when a cardDiscSlot7 fault is received	yes	
	cardDiscSlot08		This log is generated when a cardDiscSlot8 fault is received	yes	
	cardDiscSlot09		This log is generated when a cardDiscSlot9 fault is received	yes	
	cardDiscSlot10		This log is generated when a cardDiscSlot10 fault is received	yes	
	cardDiscSlot11		This log is generated when a cardDiscSlot11 fault is received	yes	
	cardDiscSlot12		This log is generated when a cardDiscSlo12 fault is received	yes	
	cardDiscSlot13		This log is generated when a cardDiscSlot13 fault is received	yes	
	cardDiscSlot14		This log is generated when a cardDiscSlot14 fault is received	yes	
	cardDiscSlot15		This log is generated when a cardDiscSlot15 fault is received	yes	
	cardDiscSlot16		This log is generated when a cardDiscSlot16 fault is received	yes	
	cardDiscSlot17		This log is generated when a cardDiscSlot17 fault is received	yes	
	cardDiscSlot18		This log is generated when a cardDiscSlot18 fault is received	yes	

	cardDiscSlot19		This log is generated when a cardDiscSlot19 fault is received	yes	
	cardDiscSlot20		This log is generated when a cardDiscSlot20 fault is received	yes	
	cardDiscSlot21		This log is generated when a cardDiscSlot21 fault is received	yes	
norLineFault (NORTEL-UEMG-LINE-MIB)					
SWLN301	lineFault	Minor	Line in Fault	yes	Requires bad hardware. **Recovery:** Perform Line Card diag and replace card if faulty.
SWLN302	lineProtectionFault	Minor	Hazardous Voltage	yes	Apply higher voltage across the loop. An alternitive if to do the following: You can force a line to be in fault (HazardVoltage) via the sethazard command on the active itp. (/linemtc/circuit/setbabble). Do this on a WLC based linecard circuit. ITP [3 2 12] dSH> setbabble 2 31 Slot: 2 Circuit: 31 **Recovery:** Remove voltage. Perform Line Card Diag and Replace card if faulty.
SWLN303	lineBabbleState	Minor	Line in Babbling state	yes	Requires test gear to generate this alarm condition. An alternitive if to do the following:You can force a line to be in fault (HazardVoltage) via the sethazard command on the active itp. (/linemtc/circuit/sethazard). Do this on a WLC based linecard circuit. ITP [3 2 12] dSH> sethazard 2 31 Slot: 2 Circuit: 31 **Recovery:** Perform Line Card diag and replace card if faulty.
nnDslFault (NORTEL-UEMG-DSL-MIB)					
XDSL301	losATUC	Minor	Loss of signal - Local modem	yes	At the DSL line card pull the cable connector **Recovery:** See lolATUC
XDSL302	lofATUC	Minor	Loss of frame - Local modem	yes	Utilize the UASHOST PC program to generate faults. A notebook PC is connected directly to the line card via a serial cable and RS232-TTL converter. **Recovery:** See lolATUC
XDSL303	lprATUC	Critical	Loss of Power - Local modem	yes	Utilize the UASHOST PC program to generate faults. A notebook PC is connected directly to the line card via a serial cable and RS232-TTL converter. **Recovery:** Reset and/or reseat line card. Investigate shelf/linecard power supplies.
XDSL304	lolATUC	Minor	Loss of link - Local modem	yes	At the DSL line card pull the cable connector **Recovery:** Generally indicates the CPE has been powered off. If customer complains, it may indicate loop impairment or faulty modem. Check subscriber connection to line card.
XDSL305	losATUR	Minor	Loss of signal - Remote modem	yes	Using an ADSL Modem **test set** inject this type of fault. **Recovery:** See lolATUR
XDSL306	lofATUR	Minor	Loss of frame - Remote modem	yes	Using an ADSL Modem **test set** inject this type of fault. **Recovery:** See lolATUR
XDSL307	lprATUR	Minor	Loss of power - Remote modem	yes	Using an ADSL Modem **test set** inject this type of fault. **Recovery:** None. This signifies a Dying Gasp from the remote modem (normal power-off condition).
XDSL308	lolATUR	Minor	Loss of link - Remote modem	yes	Using an ADSL Modem **test set** inject this type of fault. **Recovery:** See lolATUC
XDSL309	aturNotPresent	Minor	No remote modem present	yes	At the DSL line card pull the cable connector (wait a minute or two) **Recovery:** If persistent, changing provisioning parameters of the circuit may improve immunity to loop impairments. Replacing the remote modem or linecard may also correct the problem.
XDSL310	noClock	Critical	Local modem clock failure	yes	Using an ADSL Modem **test set** inject this type of fault. **Recovery:** Same as above.
XDSL311	handshakeFail	Critical	Protocol error	yes	At the ADSL Modem set it to G.lite **Recovery:** Same as above.
XDSL312	linkMismatch	Critical	Config uration error	yes	Using an ADSL Modem **test set** inject this type of fault. **Recovery:** Same as above.
XDSL313	vpiNonzero	Critical	ATM traffic dropped at WAC - upstream	yes	Using an ATM test set (ADTECH) inject this type of fault **Recovery:** If persistent, reset and/or reseat the linecard. If still not clear, replace linecard.

XDSL314	lcdIATUC	Critical	Loss of sync of ATM cells - upstream	yes	Using an ATM test set (ADTECH) inject this type of fault **Recovery:** If persistent, reset and/or reseat the linecard. If still not clear, replace remote modem and/or linecard.
XDSL315	lcdIATUR	Critical	Loss of sync of ATM cells - downstream	yes	Using an ATM test set (ADTECH) inject this type of fault **Recovery:** Same as above.
XDSL316	failATUC	Critical	Local modem critical failure - not responding, in Kernel mode, download failure or message	yes	Using an ADSL Modem test set inject this type of fault. **Recovery:** See vpiNonzero
XDSL317	circuitHardwareFault	Critical	General H/W fault indication - circuit	yes	Utilize the UASHOST PC program to generate faults. A notebook PC is connected directly to the line card via a serial cable and RS232-TTL converter. **Recovery:** Replace linecard.
BWShelfFault (NORTEL-UEMG-BANDWIDTH-MIB)					
BW300	bwResBandwShelfFault	Warning	Reserved bandwidth used on the indicated shelf has exceeded the Bandwidth Congestion Threshold	yes	At EM (Bandwidth Management view) set this threshold to a very low value. Generate enough traffic on the shelf (including PLoA) to exceed the threshold. **Recovery:** Alarm is cleared when reserved bandwidth on the shelf is 10% below the Bandwidth Congestion Threshold. Increase threshold, try to decrease the number of active calls on the shelf, or take no action.
BandwidthFault (NORTEL-UEMG-BANDWIDTH-MIB)					
BW301	bwResBandwTotalFault	Warning	This alarm is generated when reserved bandwidth use on the network interface has exceeded the Bandwidth Congestion Threshold. The alarm is cleared when reserved bandwidth on the network interface is 10% less than the threshold.	yes	At EM (Bandwidth Management view) set this threshold to a very low value. Generate enough traffic on the MG9000 (including PLoA) to exceed the threshold. **Recovery:** The alarm is cleared when reserved bandwidth on the network interface is 10% less than the threshold.
BW302	bwResBandwSloaFault	Warning	This alarm is generated when reserved bandwidth dedicated to switched lines connections on the network interface has exceeded the Bandwidth Congestion Threshold with respect to the amount of bandwidth configured the network interface for switched lines.	yes	At EM (Bandwidth Management view) set this threshold to a very low value. Generate enough SLoA traffic on the MG9000 to exceed the threshold. **Recovery:** The alarm is cleared when reserved Switched lines bandwidth on the network interface is 10% less than the threshold.
BW304	bwSwitchFabricTotalFault	Warning	Overall Cell Queue Congestion Alarm. Overall atm cell queue is at least 90% full.	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following **Dshell** command. To do this "cd" to SNMP and use the "bwevents" command with the "swfabric" option. **Recovery:** Alarm is cleared when the overall cell queue fill is less than 80% full.
BW305	bwSwitchFabricCbrFault	Warning	CBR Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following **Dshell** command. To do this "cd" to SNMP and use the "bwevents" command with the "swfabric" option. **Recovery:** Alarm is cleared when this service type cell queue is less than 80% full.
BW306	bwSwitchFabricRtVbrFault	Warning	RT-VBR Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following **Dshell** command. To do this "cd" to SNMP and use the "bwevents" command with the "swfabric" option. **Recovery:** Alarm is cleared when this service type cell queue is less than 80% full.
BW307	bwSwitchFabricNrtVbrFault	Warning	NRT-VBR Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following **Dshell** command. To do this "cd" to SNMP and use the "bwevents" command with the "swfabric" option. **Recovery:** Alarm is cleared when this service type cell queue is less than 80% full.
BW308	bwSwitchFabricUbrFault	Warning	UBR Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following **Dshell** command. To do this "cd" to SNMP and use the "bwevents" command with the "swfabric" option. **Recovery:** Alarm is cleared when this service type cell queue is less than 80% full.

BW309	bwSwitchFabricUbrPlusFault	Warning	UBR-PLUS Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following **Dshell** command. To do this "cd" to SNMP and use the "bwevents" command with the "swfabric" option. **Recovery:** Alarm is cleared when this service type cell queue is less than 80% full.
BW310	bwSwitchFabricControlFault	Warning	CONTROL Channel Cell Queue Congestion Alarm. Atm cell queue for this service type is at least 90% full.	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following **Dshell** command. To do this "cd" to SNMP and use the "bwevents" command with the "swfabric" option. **Recovery:** Alarm is cleared when this service type cell queue is less than 80% full.
BW311	bwResBandwAbiFault	Warning	This alarm is generated when reserved bandwidth dedicated to ABI lines connections on the network interface has exceeded the Bandwidth Congestion Threshold with respect to the amount of bandwidth configured the network interface for switched lines.	yes	At EM (Bandwidth Management view) set this threshold to a very low value. Generate enough ABI traffic on MG9000 to exceed the threshold. **Recovery:** The alarm is cleared when reserved ABI lines bandwidth on the network interface is 10% less than the threshold.
nnClkSyncFault (NORTEL-UEMG-CLOCKSYNC-MIB)					
CLK301	lossOfPhaseLock	Minor	Phase PLD [altera 7064b] detected a minimum phase difference greater than eight nano seconds. (FRAME PULSES BETWEEN ITPs DO NOT MATCH)	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easist way to produce them is to use the MG9000 FITS **Dshell** commands. To set it ---> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0020 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0020 To clear it --> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0000 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0020
CLK302	lossOfFramePulseLock	Major	Frame pulse alignment did not get established with the active card -- it should occur in the inactive card only.(FRAME PULSES BETWEEN ITP DO NOT MATCH)	yes	Pull the Mate ITP card
CLK303	lossOfMyClock	Major	The high and low levels of the SYNC PLL clock are not toggling. (OUTPUT OF FREQUENCY PLL HAS BEEN LOST)	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easist way to produce them is to use the MG9000 FITS **Dshell** commands. To set it ---> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0080 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0080 To clear it --> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0000 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0080
CLK304	lossOfMateClock	Minor	The high and Low levels of the mate clock are not toggling	yes	Pull the Mate ITP card
CLK305	lossOfClockOutput	Major	Phase PLD reference clock oscillator not toggling. (OUTPUT OF PHASE PLL HAS BEEN LOST)	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easist way to produce them is to use the MG9000 FITS **Dshell** commands. To set it ---> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0100 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0100 To clear it --> 1. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a092 0x0000 2. /hal/writew 0x1230a08a 0x1324;/hal/writel 0x1230a090 0x0100

CLK306	singleReferenceFailure	Minor	Single monitored reference source has been lost	yes	With the MG9000 using BITS but with network clocking available, pull the BITS cable
CLK307	allReferenceFailure	Major	Absolute and Delta reference source signals have been lost	yes	Remove the receive side of the active DCC cards fiber
CLK308	singleSyncUnitFailure	Major	Stratum 3 unit on ITP failed	yes	This alarm cannot be generated by a test set or manual action. These are HW or SW faults. The easist way to produce them is to use the MG9000 **Dshell** FITS commands
CLK312	signalLos	Minor	Single/All source reference occurred due to loss of signal	yes	Remove both Clock sources (BITS and Network Interface)
CLK313	signalLof	Monor	Single/All source(s) reference occurred due to out of frame	yes	?
norNodeFault (NORTEL-UEMG-NODE-MIB)					
	FlashRsrc	Major	Flash Memory	yes	GW software may not detect all alarm conditions listed. However, GW provides capability to generate these alarms using the debug commands in DSHELL.In DSHELL enter the following commands: > cd /nmtc/resources > injectfault When this command is entered, values for additional parameters are listed. **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ProcessorRsrc	Major	Processor	yes	GW software may not detect all alarm conditions listed. However, GW provides capability to generate these alarms using the debug commands in DSHELL.In DSHELL enter the following commands: > cd /nmtc/resources > injectfault When this command is entered, values for additional parameters are listed. **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	idpromRsrc	Major	idprom	yes	Same as Processor fault **Recovery:** Same as above.
	Atm50PortRsrc	Minor	ATM200 Port [0-19]: Not at 200 speed, or Init failed	yes	Same as Processor fault **Recovery:** Same as above.
	RamRsrc	Major	RAM	yes	Same as Processor fault **Recovery:** Same as above.
	CardTypeMismatchRsrc	Critical	Incorrect Card In Slot	yes	Same as Processor fault **Recovery:** Same as above.
	RedundancyLostRsrc	Warning	Simplex Mode - No Redundancy	yes	Same as Processor fault **Recovery:** Same as above.
	CardPairOOSRsrc	Warning	Active/Master Card Out Of Service	yes	Same as Processor fault **Recovery:** Same as above.
	CardRsrc	Major	DS1 Card	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	DS1Aal1SarRsrc	Major	AAL1 SAR - DS1 Card TDM to ATM converter	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	DS1LinkRsrc	Minor	DS1 Link [0 to 15]	yes	Same as Processor fault **Recovery:** Same as above.
	DS1FramerRsrc	Major	DS1 Framer for DS1 links [0-7, or 8-15]	yes	Same as Processor fault **Recovery:** Same as above.
	DS1LIURsrc	Major	DS1 Line IF Unit for DS1 links [0-7, or 8-15]	yes	Same as Processor fault **Recovery:** Same as above.
	CardRsrc	Major	ITP card	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ITPTimeswitchRsrc	Major	Timeswitch - call processing enging	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ITPDspServiceCircuitsRsrc	Major	DSP [0-3]	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.

NE301	ITPEchoCancellationRsrc	Minor	ECAN	yes	Same as Processor fault **Recovery:** Same as above.
	ITPAal1SarRsrc	Major	AAL1 SAR - Call Traffic TDM to ATM converter	yes	Same as Processor fault **Recovery:** Same as above.
	ITPAtmBusControllerRsrc	Major	Serial Link Control - controls communication with ITX cards	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.
	ITPDdcIdpromRsrc	Minor	DDC Idprom - DSP Daughter Card Idprom	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ITPDdcCalistoRsrc	Major	DDC Calisto - DSP Daughter Card Calisto	yes	Same as Processor fault **Recovery:** Same as above.
	ITPVoicePathRsrc	Critical	Voice Path	yes	Same as Processor fault **Recovery:** Same as above.
	CardRsrc	Major	ITX Card	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	CardRsrc	Major	SCO/SCI card	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	SCTerminalIfRsrc	Warning	RS-232 Port	yes	Same as Processor fault **Recovery:** Same as above.
	SCBootFlashMemRsrc	Warning	Flash Memory containing software load	yes	Same as Processor fault **Recovery:** Same as above.
	SCLocalBusRamRsrc	Major	Local Memory	yes	Same as Processor fault **Recovery:** Same as above.
	SCEthernetIfRsrc	Warning	Ethernet port	yes	Same as Processor fault **Recovery:** Same as above.
	SCSWRsrc	Minor	ATM Switch - MMC Chipset	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	SCNetworkIfRsrc	Major	Network Interface (SCO) [0-7] (SCI)	yes	Same as Processor fault **Recovery:** Same as above.
	SCAtmFwdRsrc	Critical	ATM Cell Forwarder	yes	Same as Processor fault **Recovery:** Same as above.
	CardRsrc	Major	ABI card	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ABITimeswitchNetSideRsrc	Major	Timeswitch - call p engine (network side)	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.
	ABITimeswitchLineSideRsrc	Major	Timeswitch - call p engine (Line side)	yes	Same as Processor fault **Recovery:** Same as above.
	ABITimeswitchRsrc	Major	Timeswitch - call processing engine	yes	Same as Processor fault **Recovery:** Same as above.
	ABIEchoCancellationRsrc	minor	ECAN - unit 0 ECAN - unit 1	yes	Same as Processor fault **Recovery:** Same as above.
	ABIAal1SarRsrc	Major	AAL1 SAR - Call Traffic TDM to ATM converter	yes	Same as Processor fault **Recovery:** Same as above.
	ABIAal1NetSideRsrc	Major	Aal1 Network side - unit 0 Aal1 Network side - unit 1	yes	Same as Processor fault **Recovery:** Same as above.
	ABIAal1LineSideRsrc	Major	Aal1 Line side - unit 0 Aal1 Line side - unit 1	yes	Same as Processor fault **Recovery:** Same as above.
	ABIAtmBusControllerRsrc	Major	Serial Link Control - controls communication with ITX cards	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.
	ABIVoicePathRsrc	Critical	Voice Path	yes	Same as Processor fault **Recovery:** Same as above.
	CardRsrc	Major	8X8 ADSL Card	yes	Same as Processor fault **Recovery:** Lock/Unlock the card, wait for the restart to finish, and then run diagnostics. If the faults re-appear, then replace the card.

NE302	AtmDataSyncRsrc	Critical	ATM Data Sync	yes	Same as Processor fault **Recovery:** Lock/Unlock the card and the card will restart, most likely causing the alarm to go away. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
	BalDataSyncRsrc	Critical	BAL Data Sync	yes	Same as Processor fault **Recovery:** Same as above.
	MegacoDataSyncRsrc	Critical	Megaco Data Sync	yes	Same as Processor fault **Recovery:** Same as above.
	BaseSubsystemRsrc	Critical	Startup failure: Base Platform	yes	Same as Processor fault **Recovery:** Same as above.
	CarmSubsystemRsrc	Critical	Startup failure: Carrier Maintenance	yes	Same as Processor fault **Recovery:** Same as above.
	NodeSubsystemRsrc	Critical	Startup failure: Node Maintenance	yes	Same as Processor fault **Recovery:** Same as above.
	MegacoSubsystemRsrc	Critical	Startup failure: Megaco	yes	Same as Processor fault **Recovery:** Same as above.
	DLMSubsystemRsrc	Critical	Startup failure: Data Line Maintenance	yes	Same as Processor fault **Recovery:** Same as above.
	TestSubsystemRsrc	Critical	Startup failure: Test Mib	yes	Same as Processor fault **Recovery:** Same as above.
	MTASubsystemRsrc	Critical	Startup failure: MTA Mib	yes	Same as Processor fault **Recovery:** Same as above.
	ShfSubsystemRsrc	Critical	Startup failure: Shelf Maintenance	yes	Same as Processor fault **Recovery:** Same as above.
	LineSubsystemRsrc	Critical	Startup failure: Line Maintenance	yes	Same as Processor fault **Recovery:** Same as above.
	ClkSyncSubsystemRsrc	Critical	Startup failure: Clock Sync Mib	yes	Same as Processor fault **Recovery:** Same as above.
	PatchSubsystemRsrc	Critical	Startup failure: Patching	yes	Same as Processor fault **Recovery:** Same as above.
	DTASubsystemRsrc	Critical	Startup failure: DTA	yes	Same as Processor fault **Recovery:** Same as above.
	MegOMsSubsystemRsrc	Critical	Startup failure: Megaco OMs	yes	Same as Processor fault **Recovery:** Same as above.
	UpgSubsystemRsrc	Critical	Startup failure: Software Upgrade	yes	Same as Processor fault **Recovery:** Same as above.
	SnmpMASubsystemRsrc	Critical	Startup failure: SNMP Master Agent	yes	Same as Processor fault **Recovery:** Same as above.
	TimeSubsystemRsrc	Critical	Startup failure: Time of Day	yes	Same as Processor fault **Recovery:** Same as above.
	ESASubsystemRsrc	Critical	Startup failure: ESA	yes	Same as Processor fault **Recovery:** Same as above.
	LKMSubsystemRsrc	Critical	Startup failure: Link Maintenance	yes	Same as Processor fault **Recovery:** Same as above.
	MarketFitSubsystemRsrc	Critical	Startup failure: Market Fit	yes	Same as Processor fault **Recovery:** Same as above.
	TestRsrc	variable	Test Resource	yes	Same as Processor fault **Recovery:** Same as above.
	HeapRsrc	Critical/Major	Low Memory	yes	Same as Processor fault **Recovery:** Same as above.
	MateCommunicationRsrc	Critical	Mate Card Communication Failure	yes	Same as Processor fault **Recovery:** Same as above.
	SCAtmCPCSUniRsrc	Major	CPCS UNI Signalling	yes	Same as Processor fault **Recovery:** Same as above.
	ITPWBCallConnRsrc	Major	Call Control Connection	yes	Same as Processor fault **Recovery:** Lock/Unlock the card and the card will restart, most likely causing the alarm to go away. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
	NEDataSyncRsrc	Critical	NE Data Sync	yes	Same as Processor fault **Recovery:** Lock/Unlock the card and the card will restart, most likely causing the alarm to go away. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
	ABIWBCallConnRsrc	Major	Call Control Connection	yes	Same as Processor fault **Recovery:** Lock/Unlock the card and the card will restart, most likely causing the alarm to go away. Wait to make sure that the card goes enabled after the restart and no faults re-appear.
NE303		Crit/Maj/Minor	Card Restored (SWACT and now inactive)		

NE304	DS1NetworkLinkRsrc	Minor	Link to DCC Card in slot [10 or 11] - Isolation In Progress	yes	Same as Processor fault **Recovery:** This alarm means two cards cannot communicate with each other. The diagnostics will determine (isolate) wher the fault is and this alarm will change into an NE305 within 3 minutes.
	ITPLineSideExternalRsrc	Minor	Line Card 0, or link to Line Card	yes	Same as Processor fault **Recovery:** Same as above.
	ITPNetworkLinkRsrc	Minor	Link to ITX, port [0 to 1] - Isolation in progress Link to Mate ITP	yes	Same as Processor fault **Recovery:** Same as above.
	ITXLinkRsrc	Minor	Link to DCC in slot [10 or 11] - Isolation in progress Link 4 to ITP card - Isolation in progress Link 5 to ITP card - Isolation in progress Link 6 to ITP card - Isolation in progress Link 7 to ITP card - Isolation in progress Link 8 to ITP card - Isolation in progress Link 9 to ITP card - Isolation in progress Link 10 to ITP card - Isolation in progress Link 11 to ITP card - Isolation in progress Link 12 to ITP card - Isolation in progress Link 13 to ITP card - Isolation in progress Link 14 to ITP card - Isolation in progress Link 15 to ITP card - Isolation in progress Link 16 to ITP card - Isolation in progress Link 17 to ITP card - Isolation in progress	yes	Pull cable on ITP card (to ITX card) **Recovery:** Same as above.
	SCLineLinkRsrc	Minor	Link to Master Shf ITP 13 - Isolation in progress Link to Master Shf ITP 12 - Isolation in progress Link to Mate DCC - Isolation in progress Link to card in slot 2 - Isolation in progress Link to card in slot 6 - Isolation in progress Link to card in slot 14 - Isolation in progress Link to card in slot 18 - Isolation in progress Link to card in slot 3 - Isolation in progress Link to card in slot 7 - Isolation in progress Link to card in slot 15 - Isolation in progress Link to card in slot 19 - Isolation in progress Link to card in slot 4 - Isolation in progress Link to card in slot 8 - Isolation in progress Link to card in slot 16 - Isolation in progress Link to card in slot 20 - Isolation in progress Link to card in slot 5 - Isolation in progress	yes	Pull an ITX card **Recovery:** Same as above.
	ABINetworkLinkRsrc	minor	Link to DCC Card in slot 10 - Isolation in progress Link to DCC Card in slot 11 - Isolation in	yes	Same as Processor fault **Recovery:** Same as above.
	Aal5SarRsrc	Major	AAL5-SAR, Messaging	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.
	DS1NetworkExternalRsrc	minor	EXTERNAL: DCC Slot 10 EXTERNAL: DCC Slot 11	yes	Same as Processor fault **Recovery:** Check the DCC to see if it has alarms. If so, handle them first. If no alarms on DCC, or only EXTERNAL alarms on the DCC, there is a backplane issue between the DS1 and DCC. Reseat DS1 card, see if problem clears. Reseat DCC card, see if problem clears.
	DS1NetworkPortRsrc	Minor	Serial Device 0 - to DCC Card in slot 10 Serial Device 1 - to DCC Card in slot	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.
	DS1UtopiaBridgeRsrc	Major	Utopia Bus Master - AAL1, AAL5 to ATM PHYs	yes	Same as Processor fault **Recovery:** Same as above.
	ITPNetworkExternalRsrc	Minor	EXTERNAL: Mate ITP EXTERNAL: ITX attached to port [0,1]	yes	Same as Processor fault **Recovery:** Check the ITX to see if it has alarms. If so, handle them first. If no alarms on ITX, or only EXTERNAL alarms on the ITX, replace the cable between ITX and ITP.
	ITPNetworkPortRsrc	Minor	Serial Device [0 to 1] - to ITX cards HDLC Device - Connects to mate ITP	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.

NE305	ITPLineSideIfRsrc	Major	Serial device 0 - to Line Card	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.
	ITPDDCAAL5SA	Major	DDC AAL5 SAR - Call Traffic TDM to IP		
	ITXExternalRsrc	Minor	EXTERNAL: DCC Slot 10 serial device EXTERNAL: DCC Slot 11 serial device EXTERNAL: ITP attached to port [0-7]	yes	Same as Processor fault **Recovery:** Check the ITP to see if it has alarms. If so, handle them first. If no alarms on ITP, or only EXTERNAL alarms on the ITX, replace the cable between ITX and ITP. If the alarm is to a DCC card, fix any DCC alarms first. Reseat ITX card, see if problem clears. Reseat DCC card, see if problem clears.
	ITXPortRsrc	Minor	Serial Device 0 - to DCC card in slot 10 Serial Device 1 - to DCC card in slot 11 Serial Device 4 - to ITP card Serial Device 5 - to ITP card Serial Device 6 - to ITP card Serial Device 7 - to ITP card Serial Device 8 - to ITP card Serial Device 9 - to ITP card Serial Device 10 - to ITP card Serial Device 11 - to ITP card Serial Device 12 - to ITP card Serial Device 13 - to ITP card Serial Device 14 - to ITP card Serial Device 15 - to ITP card Serial Device 16 - to ITP card Serial Device 17 - to ITP card Serial Device 18 - to ITP card Serial Device 19 - to ITP card	yes	Same as Processor fault **Recovery:** Same as above.
	ITXLineSideGrpRsrc	Major	Link [0 to 7] to ITP pair	yes	Same as Processor fault **Recovery:** Same as above.
	ITXNetForwarderRsrc	Major	Net side cell forwarder	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.
	ITXLineForwarderRsrc	Major	Line side cell forwarder	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.
	SCLineExternalRsrs	Minor	EXTERNAL: Master Shelf ITP slot 13 EXTERNAL: Master Shelf ITP slot 12 EXTERNAL: Mate DCC EXTERNAL: Card in slot [2-9, 14-21]	yes	Same as Processor fault **Recovery:** Check the far end slot to see if it has alarms. If so, handle them first. If no alarms on far end card, or only EXTERNAL alarms on the far end slot, there is a backplane issue between the far end card and DCC. Reseat other card in question, see if problem clears. Reseat DCC card, see if problem clears.
	SCLinePortRsrc	Minor	Serial Device 0 - to Master Shelf ITP Slot 13 Serial Device 1 - to Master Shelf ITP Slot 12 Serial Device 3 - Link to Mate DCC Card Serial Device 4 - to card in slot 2 Serial Device 5 - to card in slot 6 Serial Device 6 - to card in slot 14 Serial Device 7 - to card in slot 18 Serial Device 8 - to card in slot 3 Serial Device 9 - to card in slot 7 Serial Device 10 - to card in slot 15 Serial Device 11 - to card in slot 19 Serial Device 12 - to card in slot 4 Serial Device 13 - to card in slot 8 Serial Device 14 - to card in slot 16 Serial Device 15 - to card in slot 20 Serial Device 16 - to card in slot 5 Serial Device 17 - to card in slot 9 Serial Device 18 - to card in slot 17 Serial Device 19 - to card in slot 21	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.

	SCQuadSerContGrpRsrc	Major	Group of Serial Ports	yes	Same as Processor fault **Recovery:** Same as above.
	ABINetworkExternalRsrc	Minor	EXTERNAL: DCC slot [10 or 11]	yes	Same as Processor fault **Recovery:** Check the DCC to see if it has alarms. If so, handle them first. If no alarms on DCC, or only EXTERNAL alarms on the DCC, there is a backplane issue between the ABI and DCC. Reseat ABI card, see if problem clears. Reseat DCC card, see if problem clears.
	ABINetworkPortRsrc	minor	Serial Device 0 - to DCC Card in slot 10 Serial Device 1 - to DCC Card in slot 11	yes	Same as Processor fault **Recovery:** If these types of alarms appear in conjunction with external faults, deal with the external faults first. If they appear alone, treat them as a card fault.
	ABINetworkSideGrpRsrc	Critical	Both links to DCC Card	yes	Same as Processor fault **Recovery:** Same as above.
NE306	GlanRsrc	minor	GLAN Link to hub on Active ITP card	yes	Same as Processor fault **Recovery:** The GLAN hub is located on the active ITP in the shelf where the fault appears. First try swacting ITPs and re-run diags on the afflicted card. If that fixes the problem, replace the newly inactive ITP, otherwise treat the fault as a card fault.
	ITPGlanHubRsrc	Critical	GLAN Hub, communicates with other cards on shelf	yes	Same as Processor fault **Recovery:** The GLAN hub is located on the active ITP in the shelf where the fault appears. First try swacting ITPs and re-run diags on the afflicted card. If that fixes the problem, replace the newly inactive ITP, otherwise treat the fault as a card fault.
NE307	ABILineSideIfRsrc	Major	DS512 port	yes	Same as Processor fault **Recovery:** - Verify UEMG is in service - Verify this ABI card is unlocked - Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. - Check DS512 fibers. (light check, clean fibers, verify fibers are present)
	ABILineSideExternalRsrc	minor	XPM unit, or DS512 connection	yes	Same as Processor fault **Recovery:** Same as above.
	ABILkmAllChnlsRsrc	Major	All DS512 channels closed	yes	Same as Processor fault **Recovery:** - Verify UEMG is in service - Verify this ABI card is unlocked - Verify this ABI card is not disabled, if so, solve other issues causing this card to be disabled. - Check DS512 fibers. (light check, clean fibers, verify fibers are present)
NE308	SCWanBldrOAMPRsrc	Major	Inband Messaging OAMP Link [0,1]	yes	Same as Processor fault **Recovery:** - Check for alarms on shelf controller - Use LCI to verify that AESA provisioning information is correct. - if the problem persists, call your next level of support.
	SCWanBldrCCRsrc	Major	Inband Messaging CC Link [0,1]	yes	Same as Processor fault **Recovery:** Same as above.
	SCWanBldrHBRsrc	Major	Heartbeat to Element Manager	yes	Same as Processor fault **Recovery:** Same as above.
	SCWanBldrDS512Rsrc	Major	Inband Messaging DS512 Link [0,1]	yes	Same as Processor fault **Recovery:** Same as above.
	ITPClockSyncRsrc	Critical	Clock Sync	yes	Same as Processor fault **Recovery:** - If fault is on both ITPs 1) Verify Clock source is connected. 2) Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3) If fault persists, lock/unlock to restart the card. 4) If fault persists, call next level of support. - If fault is on one ITP 1) Verify Clock source is connected. 2) Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3) If fault persists, lock/unlock to restart the card. 4) Replace the faulty card.
	ITPClockPhaseLockRsrc	Major	Clock Sync: Loss of Phase Lock	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPClockFramePulseRsrc	Major	Clock Sync: Loss of Frame Pulse Lock	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.

NE309	ITPClockMyClockRsrc	Major	Clock Sync: Loss of My Clock	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPClockMateClockRsrc	Minor	Clock Sync: Loss of Mate Clock	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPClockOutputRsrc	Major	Clock Sync: Loss of Clock Output	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPSyncSingleRefRsrc	Minor	Clock Sync: Single Reference Failure	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPSyncAllRefRsrc	Major	Clock Sync: All Reference Failure	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPSyncSingleSyncRsrc	Major	Clock Sync: Single Sync Unit Failure	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPSyncLOSRsrc	Minor	Clock Sync: Loss of Signal	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPSyncOOFRsrc	Minor	Clock Sync: Out of Frame	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPClockRsrc	variable	Clock Sync: Clock	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPSyncRsrc	variable	Clock Sync: Sync	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITPSyncHORsrc	Minor	Clock Sync: Holdover Mode	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	SCBitsFwdRsrc	Major	BITS Forwarder	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	SCBitsRefRsrc	Minor	BITS clock reference [A or B]	yes	Same as Processor fault **Recovery:** Same as Clock Sync above.
	ITXFramerRsrc	Major	Framer - timing synchronization device	yes	Same as Processor fault **Recovery:** - If fault is on both ITPs 1) Verify Clock source is connected. 2) Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3) If fault persists, lock/unlock to restart the card. 4) If fault persists, call next level of support. - If fault is on one ITP 1) Verify Clock source is connected. 2) Wait up to 2 minutes for the clock audit to have a chance to detect clock source. 3) If fault persists, lock/unlock to restart the card. 4) Replace the faulty card.
	ITXBITSrefRsrc	Minor	BITS clock reference A		
	ITXBITSrefRsrc	Minor	BITS clock reference B		
NE310	ITXNetworkSideif	Minor	Port 2 on serial device - port only used by		
	SCQuadsercontPortRsrc	Minor	Serial Port 1 - UNUSED link to ITP slot 12		
	SCQuadsercontPortRsrc	Minor	Serial Port 0 - UNUSED link to ITP slot 13		
	SCSerLinkRsrc	Minor	Unused [was serial link #]	yes	Same as Processor fault **Recovery:** N/A
	SCOctalPhyContRsrc	Warning	Octal PHY [Unused] Device for ports [0-5] or [8-13]	yes	Same as Processor fault **Recovery:** No action required.
	SCOctalPhyContPortRsrc	Warning	Octal PHY [Unused] Port [0-13]	yes	Same as Processor fault **Recovery:** No action required.
NE311	SCTimeOfDayRsrc	minor	Time of Day: Access to time server [ip] failed	yes	Same as Processor fault **Recovery:** Attempts to access the provisioned time server have failed. - Verify the provisioned ip address of time server is correct - Verify time server is operational and online. - Use the LCI to re-submit the Time of day parameters, this forces immediate time server access.
NE312	ITPCableRsrc	minor	Cable configuration conflict	yes	Same as Processor fault **Recovery:** One of the cables to the ITXs has been connected in an unsupported way. Check to see if the cable on the two ITXes match, and that the ITP ends of the cable are in the right ports.
	ITXCableRsrc	Minor	Cable configuration conflict, port [0 to 7]	yes	Same as Processor fault **Recovery:** One of the cables to the ITPs has been connected in an unsupported way. Check to see if the cable on this ITX matches the mate ITX, and that the ITP ends of the cable are in the right ports.

NE313	ABIActivityCableRsrc	minor	Activity control cable between ABI cards	yes	Pull activity cable between ABI card pair **Recovery:** The activity control cable is a small cable on the front of the ABI cards that is used for activity determination. - Verify the cable is attached to both cards. - Replace cable. - If the fault persists, replace the inactive card. - If the problem still persists, swact, replace newly inactive card.
NE314	SCXcRsrc	Minor	Backplane Cross Connect	yes	Same as Processor fault **Recovery:** The carriers between the two DCC cards cannot communicate. - Verify and fix any CARRIER alarms - If seen on Active DCC 1) Restart the inactive DCC 2) If problem persists, replace inactive DCC 3) If problem persists, call next level of support - If seen on inactive DCC 1) Restart the inactive DCC 2) If problem persists, swact DCC cards. This will cause carriers to go down momentarily. Be sure to call next level to verify it is permissable to swact. 3) Restart the newly inactive DCC card. 4) If problem persists, replace the newly inactive card. 5) If problem persists, call next level of support. - If both DCCs have this fault, there is a backplane problem in the shelf. Replace the entire shelf backplane.
NE315	SCLinksRsrc	Major	Resource Bandwidth	yes	Same as Processor fault **Recovery:** Some of the carriers are not providing bandwidth. - Verify and fix any CARRIER alarms. - If problem persists, restart the card.
NE316	downstreamFIFO	Major	ADSL: Downstream FIFO	yes	**Recovery:** Throttle back the downstream data from the SCO.
	downstreamHEC	Major	ADSL: Downstream HEC error	yes	
	atm50Fault	Critical	ADSL: ATM50 fault	yes	**Recovery:** Restart linecard.
	upstream buffer overflow	Critical	ADSL: Upstream buffer overflow	yes	**Recovery:** Throttle back the upstream data rate on the linecard.
	downstream buffer overflow	Critical	ADSL: Downstream buffer overflow	yes	**Recovery:** Throttle back the downstream data to the linecard.
	atm device timeout	Critical	ADSL: ATM Device timeout	yes	**Recovery:** Reset linecard.
	clock accuracy	Critical	ADSL: Loss of clock accuracy	yes	**Recovery:** Reset linecard.
	dsp lockup	Critical	ADSL: DSP Lockup	yes	**Recovery:** Reload DSPs.
NE317		Crit/Maj/Minor	Shelf SIC Card Alarm		
		Crit/Maj/Minor	Shelf PIO Card Alarm		
		Crit/Maj/Minor	Shelf BIP card Alarm		
NE318		Major	SCI Card NE Proxy		
NE320	AudRecoveryRsrc	Major	Require Audit Recovery Executed	yes	Clear Flash on an ITP pair, Pull both cards and replace **Recovery:** No action required.
MG9000 Manager Reported Faults					
MGEM300	EmDbUnavailable	Major	Generated when MG9000 EM is not able to make connection to the Element Manager Database	Yes	1. Make sure that persistence is turned on.2. Make the database unavailable. 3. Perform some action (add/delete/change) on a VMG or termination. 4. Check the alarm browser for the alarm being SET. **Recovery:** 1. Re-establish the database connection. 2. Perform some action (add/delete/change) on a VMG or termination. 3. Check the alarm browser for the alarm being CLEARED.

MGEM301	CommsLostToNE	Critical	Generated when the MG9000 EM loses SNMP communication with MG9000	Yes	Break connection between the GW and the MG9K EM server. This can be done by taking the GWs OC3 OOS at the PP15000, or disabling the Ethernet connect to the MG9K EM Server (disconnect the cable). **Recovery:** EM will periodically retry to establish communication to the Gateway. Check the following : 1. PING the IP address of the Shelf Controller to validate IP connectivity. 2. PING the IP address of the OC3 CIPOA port to validate IP connectivity. 3. Check connectivity between EM and MG. 4. Check for status of the OC3 card and Node Maintenance task.
MGEM302	invalidEMIPAddress	Major	Generated when the MG9000 Manager has added an ne MG9000 and tries to discover the NE. It will check the MG9000 EM IP address provisioned at the MG9000 and if it is incorrect will raise this alarm	Yes	At the MG9000 LCI set the IP address of the MG9000 Manager to an incorrect value. At the MG9000 Manager do a manual discovery of that MG9000. **Recovery:** At the MG9000 LCI check the IP address of the MG9000 Manager and correct if necessary.
MGEM303	AlarmsBeingThrottled	Critical	Generated when the MG9000 sends too many alarms within a 5 second window. When this happens the MG9000 Manager will request this particular MG9000 stop sending Alarms and display thia particular alarm. This condition will clear when the number of alarm within 5 sec falls below a set number	yes	At the MG9000 using DSHELL use the alarm generation utility an generate at least 15 alarms a second for at least 10 seconds. **Recovery:** At the MG9000 LCI check the IP address of the MG9000 Manager and correct if necessary.
MGEM304	MG9K AlarmAuditFailed	Critical	Alarm Audit Failed - The alarm audit on the GW failed	yes	
(MEDIA_GATEWAY_MIB)					
MGC300	medGwyInvalidControllerAddress		Indicates that a message was received from a controller that did not match any valid controller IP Address.	no	N/A
MGC301	medGwyInvalid-TerminationId		Indicates a mismatch of Termination ID	no	N/A
MGC302	medGwyInvalidPackageElement		Indicates that a message was received from a controller that contained an event, signal, or descriptor that was not recognized for the package	no	N/A
nMtaFault (NORTEL_MG_MTA_mib)					
TEST302	sicSysHardwareFault			no	N/A
TEST303	mtaSysHardware Fault			no	N/A
TEST 304	sysConfigAmbiguity			no	N/A
nnEsaFault (NORTEL-UEMG-ESA-MIB)					
ESA300	esaStatusChange	Critical	Communication between GWC and GW is lost. Entered ESA mode	yes	Break connection between the GW and the GWC when ESA is enabled. This can be done by taking the GWs OC3 OOS at the PP15000, or disabling the Ethernet connect to the GWC (disconnect the cable). **Recovery:** Using the Traceroute or Ping MG9000 Manager tool test the network communications path between the EM the the MG9K, and the EM and the GWC. Check OC3 connection at the MG900, PP15000, and the SAM21 Shelf Controller, Check the Ethernet connection at the GWC, PP8600, and SAM21 Shelf Controller, Check the state of the DCC cards at the MG9000. Correct any problems found.
ESA301	esaDataFileFailure	Critical	Data download of ESA data from the CS2K Core has failed	yes	
ESA303	esaEnterFailure	Critical	Failed to enter ESA	yes	
nnEsaColFault (NORTEL-UEMG-ESA-MIB)					

ESA304	esaCommOfInterest	Major	This log is generated by the EM in response to a trap from the MG9000 (nnEsaCoIFault). The MG9000 sends this trap when it detects communication problems to other nodes in the same community of interest.	yes	
MG9000 Manager Reported Faults					
ESA302		Critical	Failed to set up FTP connection: login failure - EM failed to push ESA to VMG	yes	
ESA311		Minor	Core Download Failed - This log is generated by the EM in when a problem is detected when trying to download the datafile from the core. This new condition is when the Core datafile is more than 48 hours old, indicating that the file on the Core is not being generated nightly.	yes	
ESA312		Major	This log is generated by the EM when a failure occurs whilst trying to provision internodal community of interest data for a given NE.	yes	
nnMegacoFault (NORTEL-UEMG-MEGACO-MIB)					
VMG300	VMG OOS	Critical	Generated when Root Termination goes out of service (Communication between Gateway and GWC is lost and ESA is not enabled)	yes	Break connection between the GW and the GWC when ESA is disabled. This can be done by taking the GWs OC3 OOS at the PP15000, or disabling the Ethernet connect to the GWC (disconnect the cable). **Recovery:** Using the Traceroute or Ping MG9000 Manager tool test the network communications path between the EM the the MG9K. Check OC3 connection at the MG900, Check the state of the DCC cards at the MG9000. Correct any problems found
nnMegacoQosFault (NORTEL-UEMG-MEGACO-MIB)					
VMG301	BadCalls	Minor	QoS Alarm that is generated when the number of bad call reaches a certain threshold	SLoIP only	In the MG9000 EM set the QoS thresholds to a low level. Using a "Packet Storm" or "Shunra" test set, inject errors on the OC3/STM1 network interface on a particular active calls SVC. **Recovery:** Check GWC QoS collector for any QoS error patterns. Narrow down probable areas where errors could occur. Run test calls to narrow down futher. If error is only on that one line there may be a card fault. If problem is in the network isolate problem area and correct.
VMG302	PacketLoss	Minor	QoS Alarm that is generated when the number of Packet Loss reaches a certain threshold	SLoIP only	Same as above Recovery: Same as above
VMG303	Jitter	Minor	QoS Alarm that is generated when IP message Jitter reaches a certain threshold	SLoIP only	Same as above Recovery: Same as above
VMG304	Latency	Minor	QoS Alarm that is generated when IP message Latency reaches a certain threshold	SLoIP only	Same as above Recovery: Same as above
nnMegacoFault (NORTEL-UEMG-MEGACO-MIB)					
VMG311	megacoTaskInput	Major	Application layer framing (ALF) alarm occurs when the MG 9000 is experiencing Megaco retransmissions greater than 50 % for a period of 5 minutes or more.		**Recovery:** Verify the MG 9000 is in service from the GWC perspective. Check the network connection between the GWC and the MG 9000.
VMG312	megacoALF	Major	Megaco task alarm indicates one or more of the Megaco Task's input buffers are over 90 % full for a period of 5 minutes or more.		**Recovery:** Check the following based on the inputsource: • line card - indicates the MG 9000 has a babbling line card. All line cards should be checked. • DSP - indicates the MG 9000 has a babbling DSP. If the alarm is not raised on the inactive ITP card, perform a SWACT of the ITP card. • GWC - indicates the GWC is flooding the MG 9000 with messages. Check the GWC for faults. • datasync - indicates the active ITP card is flooding the inactive ITP card with messages.
VMG313	megacoDspRes			Yes	

VMG322	vmgAdminStatus OutOfService	Critical	Admin State Out Of Service - Call Processing Out of Service	Yes	
VMG323	cardInitializing	Critical	VMG Initializing - Call Processing Out of Service	Yes	
VMG324	cardLocked	Critical	Card Locked - Call Processing Out of Service	Yes	
VMG325	cardDisabled	Critical	Card Disabled - Call Processing Out of Service	Yes	
VMG328	lineMtcNotReady	Critical	Line Maintenance Not Ready - Call Processing Out of Service	Yes	
VMG329	megacoMtcNotR eady	Critical	Megaco Maintenance Not Ready - Call Processing Out of Service	Yes	
VMG373	gwcUnreachable	Critical	GWC Unreachable - Call Processing Out of Service	Yes	
VMG374	noGwcReply	Critical	GWC Reachable But No Reply To Service Change - Check LGRP/GWC state - Call Processing Out of Service	Yes	
VMG376	aallBearerSubsys NotReady	Critical	AAL1 Bearer Not Ready - Call Processing Out of Service	Yes	
VMG377	ipBearerSubsysN otReady	Critical	IP Bearer Not Ready - Call Processing Out of Service	Yes	
Performance (NORTEL-UEMG-PERFMON-MIB)					
OVLD304	Performance Degraded	Minor/Major	Overload Detection Alarm that is generated whenever the MG9000 actually enters an overload condition.	Yes	
SCTP (NORTEL-UEMG-RELMSGING-MIB)					
OVLD808	relMsgLinkFail	Critical	An external messaging link has closed and cannot send/receive	Yes	
OVLD809	relMsgLinkSevDe graded	Major	Message loss is high enough such that the message link is in a degraded service state. For ABI, this would mean that some calls are failing and perhaps maintenance action are failing (e.g. static data download, etc)	Yes	
OVLD810	relMsgLinkDegra ded	Minor	Message retransmissions are high enough that system is starting to see performance degradation. Potentially, this could mean increased latency, reduced messaging through the system, buffer overflows and perhaps heading toward congestion.	Yes	
GIGE (NORTEL-UEMG-GIGE-MIB)					
GIGE301	LOS	Critical	Loss of Signal	Yes	
GIGE302	RFI	Critical	Remote Failure Indication	Yes	
GIGE303	TxF	Critical	Transmit Failure	Yes	
GIGE304	TEM	Critical	threshol exceeded	Yes	
GIGE305	POW	Critical	Low Power Indicated	Yes	
GIGE306	RxSD	Critical	Transmit Signal Degraded	Yes	
GIGE307	RxEER	Critical	Transmit Excessive Error Ratio	Yes	
GIGE308	TBC	Critical	Transmit Bias Current	Yes	
GIGE309	LINT	Critical	Link Initialization	Yes	
GIGE310	OPT	Critical	Transmit Optical Power	Yes	
GIGE311	OPR	Critical	Receive Optical Power	Yes	
GIGE312	GARP	Critical	GARP failure	Yes	
GIGE313	LKINT	Critical	Link Integrity Failure	Yes	
GIGE314	Auto negotiation	Critical	Auto negotiation Failure	Yes	
GIGE315	non preferred link	Critical	Non Preferred Link is active	Yes	
GIGE316	Link Invalid Status	Critical	Link Invalid Status	Yes	
GIGE317	No Protection Group	Critical	No Protection Group	Yes	
OMC300		Critical	Indicates that OM Collector failed to collect OM file from MG9K during a particular collection interval.	Yes	
IPSec (NORTEL-UEMG-IPSEC-MIB)					
IPSC300	ipsecMismatchSh aredKey	Critical	During negotiation, the key received did not match the one locally set	Yes	

IPSC301	ipsecIkePeerLinkExpired	Critical	Phase 1 security association has expired or not present	Yes	
IPSC302	ipsecSecurePeerLinkExpired	Critical	Phase 2 security association has expired or not present	Yes	
IPSC303	ipsecDoSCallp	Critical	Packets are being replayed to the call processing interface. Possible Denial of Service attack	Yes	
IPSC304	ipsecDoSMgmt	Critical	Packets are being replayed to the call processing interface. Possible Denial of Service attack	Yes	
IPSC305	ipsecMaxDiscardedPktRate	Minor	An inordinate percentage of the received/transmitted packets are being discarded as a result of current security policies. Indicates possible mis-configuration, or denial of service attack	Yes	
IPSC306	ipsecRadiusTimeout	Major	MG9K's requests sent to RADIUS server has timed out	Yes	

Supported in EM but not enabled at MG9000
New or changed in SN09

MG9000 Reported Event LOGs

LOG Subsystem (MIB)	LOG Id	LOG Type	Description	Supported/ Enabled	Procedure To Generate LOG
ATM Event (NORTEL-UEMG-ATM-MIB)	VC600	atmIntfPvcFailures-Trap	Indicates that one or more PVPLs or PVCLs on this interface has failed since the last atmPvcFailuresTrap was sent.	no	N/A
	VC800	nn5AtmIfThreshold	Generated when an ATM interface stat exceeds the specified threshold	no	N/A
	VC801	nnAtmStatsVcThreshTrap	Generated when the VC stat exceeds specified threshold.	no	N/A
Data Audit Event	MGAU600	AuditLogNotification	Generated my the MG9000 Manager when an Audit is started, stopped, a data missmatch was found between them MG9000 and the MG9000 Manager, or a communications failure occurred while the Audit was running	yes	Envoke the Reinitialize option on the OC3 card
Bandwidth Event (NORTEL-UEMG-BANDWIDTH-MIB)	BW800	nnBwSwitchFabricCongestion	A nnBwSwitchFabricCongestion Notification is generated when one of the input cellQueues Cross the configured threshold percentage.	yes	This fault is very difficult to produce during normal operations with a test set or manual action. The best way to generate this fault is using the following **Dshell** command. To do this "cd" to SNMP and use the "bwevents" command with the "swfabric" option. **Log Output Example:** NTL STD: RTPS BW800 JAN28 22:10:40 0462 THR MG9K BW Switch Fabric Congestion NE Number: 19 NE Name: CO_19 PhysLoc: Ne.ne19 Bandwidth Switch Fabric Congestion Type: CBR Switch Fabric Congestion Bandwidth Bandwith Notification Value: 70.0 % Bandwidth Current Total Queue Fill: 90.0 % SCC2: 10 BW 800 8936 THR MG9K BW Switch Fabric Congestion NE Number: 19 NE Name: CO_19 PhysLoc: Ne.ne19 Bandwidth Switch Fabric Congestion Type: CBR Switch Fabric Congestion Bandwidth Bandwith Notification Value: 70.0 % Bandwidth Current Total Queue Fill: 90.0 %
	BW801	nnBwBandwUtilizationCongestion	A nnBwBandwUtilization Notification is generated when the the total or dsl's cell rates Cross the configured threshold percentage.	yes	Set the DSL threshold (at BW Manager GUI an EM) to a low level, generate data traffic on a number of DSL lines until the LOG appears.
DS1 Carrier Event (NORTEL-UEMG-CARRIER-MIB)	MGCA500	dsx1LineStatus-Change	Trap is sent when the value of an instance dsx1Line Status changes.	yes	Remove the DS1 cable and replace
	MGCA600	apsTrapSwitchover	Sent when the value of an instance of apsChanSwitchover increments.	no	N/A
	MGCA601	apsTrapModeMis-match	Sent when the value of an instance of apsStatusModeMismatch increments	no	N/A
	MGCA602	apsProtSwitchRejectEvent		no	N/A
	MGCA800	norCarrThreshold	Sent when a Carrier exceeds the specified threshold on a given performance Measure.	yes	
BIP Input/Output State Change (NORTEL-UEMG-SHF-MIB)	SHLF501	nnShfInputOutputOperStatus	TRAP sent when any BIP Input/Output state change event occurs for an Input/Output with an alarm severity of indeterminate.	yes	Change any BIP Input/Output Alarm Severity setting to indeterminate and then follow test procedure for that alarm.
Test Event	TEST600	testComplete	Signifies that a test has completed for a particular entity	yes	Run a Line test or Run a Line card Diag
Link Event	LINK500	linkDown	Signifies that the SNMPv2 entity has detected that the ifOperStatus object is about to enter the down state.	yes	Take the ITP card pair Lock and Offline
	LINK501	linkUp	Signifies that the SNMP entity has detected that the ifOperStatus object left the down state.	yes	Take the ITP card pair online and Unlocked
Clock Sync Event (NORTEL-UEMG-CLOCKSYNC-MIB)	CLK500	ClockSyncChange	A change has occured for Clock Sync: timingModeChange (1), clockModeChange (2),	yes	Remove the Colck source cable to the ITX card
SLoA Event	SWL600	nnMtaTrapConnectionStatus	Sent when SNM indicates status of the connection	yes	Put line under test
MEGACO Event	MGC500	medGwyLinkStatus-Change	Indicates that status of media gateway control link has changed.	no	N/A
	MGC501	medGwyTermination-StatusChange	Sent when a termination changes Status.	no	N/A
SNMP Event	SNMP600	snmpEnableAuthen-Traps	Indicates permission to generate authentificationFailure traps.	no	N/A
	SNMP601	coldStart	Signifies that the SNMP entity is reinitializing itself and its configuration may have been altered.	yes	Initiate Coldstart from the MG9K LCI
	SNMP602	warmStart	Signifies that the SNMP entity is reinitializing itself such that its configuration is unaltered.	no	N/A
	NE500	norNodeSwact	Generated when the Node does a switch of activity.	yes	SWAC the OC3 card pair
	NE501	norNodeStateChange	Generated when the Node changes state.	yes	Take ITP OOS, put back inservice
	NE502	DS1SpareOperationEvent	Generated when a DS1 card is spared	yes	Manually spare a ds1 card
	NE503		ABI Switch Mastership	yes	
	NE504		ABI State Change	yes	
	NE600	entConfigChange	Generated when the value of entLastChangeTime changes.	yes	Plug in new line card
	NE601	norNodeRestartBegin	Generated when the Node is restarting.	yes	Restart ITP card

Network Element Event (NORTEL-UEMG-NODE-MIB)	**NE602**	norNodeRestart-Complete	Generated when the Node completes its Restart	yes	Same as above
	NE603	norNodeSWLoad-Complete	Generated when the Node completes its SoftwareLoad.	yes	Load an ITP with new SW load
	NE604	norNodeSWUpgrade-Complete	Generated when a SW Upgrade has completed	yes	Same as above
	NE605		Generated when a Network Element is deleted	yes	Delete a MG9K from the EM
	NE602		Generated when a Reinitialize Gateway event occurs	yes	Envoke the Reinitialize option on the OC3 card
	NE607	norNodeCardDeleted	Generated when a card is deleted	yes	Provision an MG9K card for deletion from the EM then pull the card from MG9K
	NE608	norNodeCardInserted	Generated when a card is inserted	yes	Insert a MG9K card at the MG9K
	NE609		generated whenever a user executes an image request	yes	
Alarm Reliability Event	**ALM998**	AlarmSequenceError	Generated when the MG9000 Manager detects it has missed Alarms from the MG9000	yes	Break connection (OC3) to MG9K, generate a number of alarms at MG9K, resetup MG9K connection.
	ALM999	AlarmSequenceRestored	Generated when the MG9000 Manager recovered the missing Alarms from the MG9000	yes	Same as above
DSL Event (NORTEL-UEMG-DSL-MIB)	**XDSL600**	adslAtucRateChangeTrap	The ATUCs transmit rate has changed (RADSL mode only)	no	N/A
	XDSL601	adslAtucInitFailureTrap	ATUC initialization failed	no	N/A
	XDSL602	adslAturRateChangeTrap	The ATURs transmit rate has changed (RADSL mode only)	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL800	adslAtucPerfLofsThreshTrap	Loss of Framing 15-minute interval threshold reached	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL801	adslAtucPerfLossThreshTrap	Loss of Signal 15-minute interval threshold reached	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL802	adslAtucPerfLprsThreshTrap	Loss of Power 15-minute interval threshold reached	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL803	adslAtucPerfESsThreshTrap	Errored Second 15-minute interval threshold reached	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL804	adslAtucPerfLolsThreshTrap	Loss of Link 15-minute interval threshold reached	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL805	adslAturPerfLofsThreshTrap	Loss of Framing 15-minute interval threshold reache	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL806	adslAturPerfLossThreshTrap	Loss of Signal 15-minute interval threshold reached	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL807	adslAturPerfLprsThreshTrap	LPRS 15-minute interval threshold reached	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL808	adslAturPerfESsThreshTrap	Errored Second 15-minute interval threshold reached	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
	XDSL809	nnDSLThreshold Trap	a nnDslThreshold notification is sent when a DSL Interface exceeds the specified threshold on a given performanceMeasure, specified by the nnDslThresholdNotifyType: atucfec (1), atuccrc (2), atucncd (3), atucocd (4), atuchec (5), atuclcd (6), aturfec (7), aturblockError (8), aturncd (9), aturocd (10), aturhec (11), aturlcd (12)	yes	Using an ADSL Modem **test set** inject large numbers of this type of error.
Manager Upgrade Event	**UPGD600**		indicating an upgrade is needed.	yes	Requires the customer to perform the upgrade or downgrade procedure. Follow MG9K EM upgrade procedutes
	UPGD601		indicating an export has started	yes	Requires no immediate action
	UPGD602		indicating an export has completed	yes	Same as above
	UPGD603		indicating an import has started	yes	Same as above
	UPGD604		indicating an import has completed	yes	Same as above
Manager Event	**MGEM687**		Indicates that an attempt to correct the database has failed for Line Circuit(s).	yes	
	MGEM688		Indicates that an attempt to correct the database has failed for Termination(s).	yes	
	MGEM89		Indicates that the Database is unavailable and correction failed.	yes	
	MGEM699		MG9K Discovery Status Event	yes	
	MGEM700		MG9000 Manager Server application Startup	yes	Telnet into the MG9000 Manager server and execute the shutdown procedure then execute following command "/opt/nortel/mg9ksrv_06/bin/mg9kimpl start"
	MGEM701		MG9000 Manager Server application Shutdown	yes	Telnet into the MG9000 Manager server and execute the following command "/opt/nortel/mg9ksrv_06/bin/mg9kimpl stop"
	MGEM702		MG9000 Manager Mid-Tier Server application Startup	yes	Telnet into the MG9000 Manager Mid-Tier server and execute the shutdown procedure then execute the following command "/opt/nortel/mg9kmtr_06/bin/mg9kmidtimpl start"
	MGEM703		MG9000 Manager Mid-Tier Server application Shutdown	yes	Telnet into the MG9000 Manager Mid-Tier server and execute the following command "/opt/nortel/mg9kmtr_06/bin/mg9kmidtimpl stop"
OM Collector Event	**OMC700**		MG9000 Manager Mid-Tier Server OM Collector application Startup	yes	Telnet into the MG9000 Manager Mid-Tier server and execute the shutdown procedure then execute the following command "/opt/nortel/omcltr_06/bin/OMimpl start"
	OMC701		MG9000 Manager Mid-Tier Server OM Collector application Shutdown	yes	Telnet into the MG9000 Manager Mid-Tier server and execute the following command "/opt/nortel/omcltr_06/bin/OMimpl stop"
Performance (NORTEL-UEMG-PERFMON-MIB)	**OVLD800**	ovIdRscMonPduRateFault	Pdu Rate Threshold crossed.	yes	
	OVLD801	ovIdRscMonCbvMsgRFault	Cbv Message Rate Overloaded Alarm	yes	
	OVLD802	ovIdRscMonConnQueFault	Connection Queue Overloaded Alarm.	yes	
	OVLD803	ovIdRscMonCpuUtilFault	PDU Rate Overloaded Alarm.	yes	
	OVLD804	ovIdRscMonCpuUtilFault	CPU Utilization Overloaded Alarm	yes	

	OVLD805	perfMonRamFault	RAM Utilization Overloaded Alarm	yes	
	OVLD806	perfMonFlashFault	Flash Utilization Overloaded Alarm	yes	
	OVLD807	perfMonChannFault	Chan Utilization Overloaded Alarm	yes	
	VMG600		Indicates that termination data was successfully provisioned in all appropriate areas except for the database.	yes	
	VMG601		Indicates that an attempt to correct termination data in the database has passed.	yes	
	REX600		Indicates the start or completion of REX on a card/card-pair. The cards under consideration are ITP, ITX and DCC.	yes	
	REX601		Indicates the success or failure of REX on a card/card-pair. The cards under consideration are ITP, ITX and DCC	yes	
	REX602		Indicates that the REX for the card/card-pair under consideration has been skipped. The card types considered are ITP, ITX and DCC.	yes	

New or changed in SN09

MG9000 Manager User Action Audit LOGs

LOG Subsystem	LOG Id	Description	Procedure To Generate LOG
	MGEM600	SWACT of ABI, ITP, ITX, OC3, or IMA card	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM601	Lock of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM602	Unlock of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM603	Force Lock of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM604	Force Unlock of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM605	Diag of ABI, ITP, ITX, OC3, IMA, DS1, MTA, WLC, SAA, XDSL, SIC card	See procedures in MG9000 FCAPS Document Fault Management section
	MGEM606	Create a VMG	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM607	Delete a VMG	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM608	ESA data configuration	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM609	Gateway data configuration	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM610	Create Termination	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM611	Bulk Termination creation	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM612	Create ESA Service Code	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM613	Delete ESA Service Code	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM614	Delete Termination	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM615	Bulk Termination deletion	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM616	Delete all termination on a card	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM617	Change Termination data	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM618	Create a PLoA Passive Endpoint	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM619	Create a PLoA Active Endpoint	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM620	Create a PLoA Hairpin connection	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM621	PLoA Connection Admin State change	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM622	PLoA Service Restart	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM623	PLoA Connection SVC test initiated	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM624	PLoA Connection SVC test abort	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM625	PLoA Connection Unlock test	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM626	Delete a PLoA Endpoint	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM627	Modify ADSL data circuit provisioning attributes	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM628	De-provision ADSL data circuit service	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM629	Add new ADSL data circuit	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM630	Change ADSL data circuit	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM631	Delete ADSL data circuit	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM632	Set links in DS1 IMA group	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM633	Start DS1 IMA group pattern test	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM634	Stop DS1 IMA group pattern test	See procedures in MG9000 FCAPS Document Configuration Management section

MG9000 Manager	**MGEM635**	Add DS1 IMA link to group	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM636	Remove DS1 IMA link from group	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM637	Set administration state on DS1 IMA link	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM638	Set configuration state on DS1 IMA link	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM639	OC3, DS1 IMA, DS1, DS0, carrier lock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM640	OC3, DS1 IMA, DS1, DS0, multiple carrier lock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM641	OC3, DS1 IMA, DS1, DS0, carrier unlock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM642	OC3, DS1 IMA, DS1, DS0, multiple carrier unlock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM643	OC3, DS1 IMA, DS1, DS0, forced carrier lock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM644	OC3, DS1 IMA, DS1, DS0, forced multiple carrier lock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM645	OC3, DS1 IMA, DS1, DS0, forced carrier unlock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM646	OC3, DS1 IMA, DS1, DS0, forced multiple carrier unlock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM647	OC3, DS1 IMA, DS1, DS0, carrier online	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM648	OC3, DS1 IMA, DS1, DS0, multiple carrier online	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM649	OC3, DS1 IMA, DS1, DS0, carrier offline	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM650	OC3, DS1 IMA, DS1, DS0, multiple carrier offline	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM651	WLC, ADSL Data/Line, SAA Line circuit lock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM652	WLC, ADSL Data/Line, SAA Line circuit multiple lock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM653	WLC, ADSL Data/Line, SAA Line circuit unlock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM654	WLC, ADSL Data/Line, SAA Line circuit multiple unlock	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM655	WLC, ADSL Data/Line, SAA Line circuit diagnostic check	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM656	WLC, ADSL Data/Line circuit abort diagnostic check	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM657	WLC, ADSL Data/Line, SAA Line circuit set end to end test port	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM658	WLC, ADSL Data/Line, SAA Line circuit set PAV test port	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM659	WLC, ADSL Data/Line, SAA Line circuit clear test	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM660	Create new LCI user	
	MGEM661	Delete existing LCI user	
	MGEM662	Modify existing LCI user data	
	MGEM663	Channelize DS1 carrier	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM664	Unchannelize DS1 carrier	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM665	Modify DS1 carrier provisioning attributes	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM666	Synchronize pre-provisioned bundles	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM667	Assign DS1 card spare	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM668	Rlease DS1 card spare	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM669	Revert DS1 card sparing activity	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM670	Initiate DS1 card sparing activity	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM671	Add DS1 card to protection group	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM672	Remove DS1 card from protection group	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM673	Provision DS0 bundle on DS1 carrier	See procedures in MG9000 FCAPS Document Configuration Management section

	MGEM674	Modify DS0 bundle	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM675	Set DS0 bundle ciruit identifier	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM676	Lock DS0 bundle	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM677	Unlock DS0 bundle	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM678	Delete DS0 bundle	See procedures in MG9000 FCAPS Document Configuration Management section
	MGEM679	ABI Card Switch Mastership requested	
	MGEM679	getCardType(+ restart requested	
	MGEM679	Frame location update requested	
	MGEM680	getCardType(+ configuration state (Online/Offline/Deprovision/Re-Initialize change requested	
	MGEM681	Provisioning Request	
	MGEM682	Carrier Modification Request	
	MGEM683	Frame Location Update Request	
	MGEM684	Restart Requested	
	MGEM685	Audit request for one NE	
	MGEM686	Software Download Requested-single card type	
	MGEM687	(See Event LOGs)	
	MGEM688	(See Event LOGs)	
	MGEM689	(See Event LOGs)	
	MGEM690	Reserved for G.729	
	MGEM691	Unused	
	MGEM692	Unused	
	MGEM693	Unused	
	MGEM694	WLC, ADSL Data/Line, SAA Line circuit Force lock	
	MGEM695	WLC, ADSL Data/Line, SAA Line circuit Force multiple lock	
	MGEM696	WLC, ADSL Data/Line, SAA Line circuit Force unlock	
	MGEM697	WLC, ADSL Data/Line, SAA Line circuit Force multiple unlock	
	MGEM698	IPSec notifications	
	MGEM699	(See Event LOGs)	
	MGEM700	(See Event LOGs)	
	MGEM701	(See Event LOGs)	
	MGEM702	(See Event LOGs)	
	MGEM703	(See Event LOGs)	
	MGEM704	Delete NE request	
	MGEM705	Force Deprovision	
	MGEM706	Provision/Create a DFAD Tap	
	MGEM707	Deprovision/Delete a DFAD Tap	
	MGEM708	Start & Stop - Sync Backup	
	MGEM709	Provision/Create an MTAP request	
	MGEM710	Deprovision/Delete an MTAP request	
	MGEM711	Upgrade VMG requested	
	MGEM712	Submit a request for audit	
	MGEM713	Discovery request	
	MGEM714	Upgrade Request	

Appendix F: CICM Logs and Alarms

The following table is the list of events that can be generated by the SAM21 blade-based CICM product in SN09. Some notes on the table's contents at the time of writing:

• All logs with a CICM Log Output Path of "Alarm_Trap_to_IEMS" or "/var/log/customerlog" are visible to a fault OSS at the IEMS northbound log interface. "Alarm_Trap_to_IEMS" logs are reporting the raising and clearing of alarms and are part of a set/clear pair of logs. (See exception below.) "/var/log/customerlog" logs are autonomous INFO logs with no severity and are not part of a set/clear pair. Output paths of "/var/log/auditlog" and "/var/log/securitylog" are not available at IEMS's northbound log interface.

• The CICM328 log (WindowsRestart alarm) has no identified clear in the table below. The WindowsRestart alarm occurs when CICM restarts. When the CICM application comes up, there is a cold start trap generated which is not documented in the table below. It may be possible to use this event as a "clear" for WindowsRestart.

• The CICM353 log events are unique to the SAM16-based CICM product and are not contained in the table below.

• Items highlighted in bold are changes one can expect from the previous release. At the time of writing, in SN09 only 1 new instance (SubtractConnectionAckFailed) of the CICM363 log is known. This is an autonomous INFO log which has no severity and is not part of a set/clear pair.

Log	CICM Log Output Path	Alarm	Log Severity	Component Id	Category	Description	Specific Problem
CICM300	/var/log/customerlog	LegacyError	None	Unknown ,/var/log/customerlog,Platform	environmental	Legacy Error Log.	Log details: XXX
CICM300	/var/log/customerlog	LegacyWarning	None	Unknown ,/var/log/customerlog,Platform	environmental	Legacy Warning Log.	Log details: XXX
CICM301	Alarm_Trap_to_IEMS	softwareMismatch	Minor	CICM=<nodename>;NodeType=Platform	environmental	Software Version Mismatch.	Version Mismatch. Local Version XXX. Mate Version XXX.
CICM301	Alarm_Trap_to_IEMS	softwareMismatch Clear	None	CICM=<nodename>;NodeType=Platform	environmental	Software Version Mismatch.	Version Mismatch. Local Version XXX. Mate Version XXX.
CICM302	/var/log/customerlog	RouteOrElementStateMismatch	None	Unknown ,/var/log/customerlog,Platform	communications	Route/element state mismatch	Resetting adapter, state= XXX mate=XXX
CICM303	/var/log/customerlog	CorruptVLCM	None	Unknown ,/var/log/customerlog,Platform	equipment	Corrupt VLCM.	VLCM name XXX is corrupt - in memory gateway already has id of XXX.
CICM304	/var/log/customerlog	UnableBindIP	None	Unknown ,/var/log/customerlog,Platform	communications	Unable to bind IP.	Unable to bind IP adress XXX to interface XXX.
CICM305	/var/log/customerlog	NoAdapterMib	None	Unknown ,/var/log/customerlog,Platform	processingError	Unable To Bind Adapter.	Unable to obtain dynamic adapter config from Mib - cannot bind adapter.
CICM306	/var/log/customerlog	NoAdminIPNodeA	None	Unknown ,/var/log/customerlog,Platform	processingError	No admin Ip for node A.	No admin address datafilled for node A
CICM306	/var/log/customerlog	NoAdminIPNodeB	None	Unknown ,/var/log/customerlog,Platform	processingError	No admin Ip for node B.	No admin address datafilled for node B
CICM306	/var/log/customerlog	NoAdminNetMask	None	Unknown ,/var/log/customerlog,Platform	processingError	No admin net mask.	No admin net mask datafilled
CICM306	/var/log/customerlog	InvalidAdminAddr	None	Unknown ,/var/log/customerlog,Platform	processingError	Invalid admin address.	Invalid admin ip address specified XXX
CICM306	/var/log/customerlog	InvalidAdminMask	None	Unknown ,/var/log/customerlog,Platform	processingError	Invalid admin mask.	Invalid admin mask specified XXX

CICM307	/var/log/customerlog	SkippingDisabledAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Skipping disabled adapter	Skipping disabled XXX adapter.
CICM308	/var/log/customerlog	UFTPSessionTimeout1	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPSessionTimeout.	Timed out after XXX secs - No request details received from client
CICM308	/var/log/customerlog	UFTPSessionTimeout2	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPSessionTimeout.	Timed out after XXX secs - No response from client
CICM308	/var/log/customerlog	UFTPSessionTimeout3	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPSessionTimeout.	Timed out after XXX secs - Terminated after error occured
CICM309	/var/log/customerlog	NoStreamsAvailable	None	Unknown ,/var/log/customerlog,Cicm	communications	NoStreamsAvailable.	No streams available for CreateConnection, XXX streams already allocated
CICM310	/var/log/customerlog	H248SendPortNotFoundInMIB	None	Unknown ,/var/log/customerlog,Cicm	communications	H248 Send Port Not Found in MIB.	XXX : H248 send port not found in MIB.Defaulting to XXX
CICM310	/var/log/customerlog	H248ListenPortNotFoundInMIB	None	Unknown ,/var/log/customerlog,Cicm	communications	H248 Listen Port Not Found in MIB.	XXX : H248 listen port not found in MIB.Defaulting to XXX
CICM311	/var/log/customerlog	CouldNotOpenRegKey	None	Unknown ,/var/log/customerlog,Platform	processingError	Could not open registry key.	Could not open XXX in registry. New hierarchy needs to be created. This event can be generated during initial configuration of the gateway.
CICM311	/var/log/customerlog	MibFailedOpenKey	None	Unknown ,/var/log/customerlog,Platform	processingError	Mib failed to open key.	Mib node error: failed to open key XXX.
CICM312	/var/log/customerlog	MIBCompatFailure	None	Unknown ,/var/log/customerlog,Platform	processingError	MIB compatibility failure.	MIB compatability failure. Could not find the MIB entries for release XXX
CICM312	/var/log/customerlog	MIBCompatRemFailure	None	Unknown ,/var/log/customerlog,Platform	processingError	MIB compatibility remote failure.	MIB compatability failure. Could not find the MIB entries for release XXX on remote node
CICM313	Alarm_Trap_to_IEMS	GWCConnectionLoss	Critical	CICM=<nodename>;NodeType=Cicm	communications	GWC Connection Loss	CICM has lost connection with the GWC
CICM313	Alarm_Trap_to_IEMS	GWCConnectionLossClear	None	CICM=<nodename>;NodeType=Cicm	communications	GWC Connection Loss	CICM has regained connection with GWC
CICM314	/var/log/customerlog	MibReadFailure	None	Unknown ,/var/log/customerlog,Platform	processingError	Mib Registry Read Failure.	Mib registry error: failed to read attribute XXX in key XXX. Probable cause is out of date config data.
CICM316	/var/log/customerlog	UnableCreateSocket	None	Unknown ,/var/log/customerlog,Platform	communications	Unable to create a socket.	Unable to create a socket. Error = XXX
CICM316	/var/log/customerlog	UnableBindSocketAddr	None	Unknown ,/var/log/customerlog,Platform	communications	Unable to Bind Socket to IP.	Unable to Bind Socket to IP address.

CICM316	/var/log/customerlog	AddrNotAvailable	None	Unknown ,/var/log/customerlog,Platform	communications	Addr not available.	Specified address is not available on the local host.
CICM316	/var/log/customerlog	AddrInUse	None	Unknown ,/var/log/customerlog,Platform	communications	Addr already in use.	Specified address is already in use.
CICM316	/var/log/customerlog	NoAsyncReadMode	None	Unknown ,/var/log/customerlog,Platform	communications	No async read mode	Unable to select asynchronous read mode. Error = XXX
CICM316	/var/log/customerlog	ErrorSetSocketTMO	None	Unknown ,/var/log/customerlog,Platform	communications	Error setting socket tmo	Error setting socket timeout.Error = XXX
CICM322	Alarm_Trap_to_IEMS	SystemShutdown	Critical	CICM=<nodename>;NodeType=Platform	processingError	System Shutdown	System is shutting down due to user command.
CICM322	Alarm_Trap_to_IEMS	SystemStartUp	None	CICM=<nodename>;NodeType=Platform	processingError	System Shutdown	System is starting up.
CICM323	/var/log/customerlog	SlaveAdapterReceivedNoPackets	None	Unknown ,/var/log/customerlog,Platform	communications	Slave adapter received no packets	Slave adapter XXX received no packets
CICM324	/var/log/customerlog	FatalStateError	None	Unknown ,/var/log/customerlog,Cicm	equipment	Fatal Error in state	Fatal error in state XXX.
CICM325	/var/log/customerlog	ElementNotConfigured	None	Unknown ,/var/log/customerlog,Cicm	processingError	Element Not Configured.	Element XXX is not configured.
CICM325	/var/log/customerlog	ElementNotConfigured2	None	Unknown ,/var/log/customerlog,Cicm	processingError	Config data missing.	Configuration data missing, service cannot start.
CICM326	/var/log/customerlog	UnableToGetPhysicalLinkStatusForDevice	None	Unknown ,/var/log/customerlog,Platform	communications	Unable to get physical link status	Unable to get physical link status for device XXX
CICM327	/var/log/customerlog	FailedStartNetObj	None	Unknown ,/var/log/customerlog,Cicm	equipment	Failed to start network status	Failed to start network status object, hr=0x XXX
CICM328	Alarm_Trap_to_IEMS	WindowsRestart	Critical	CICM=<nodename>;NodeType=Cicm	equipment	Windows restart	Auto reboot on failure is set. Initiating windows restart.
CICM329	/var/log/customerlog	AuditMateDown	None	Unknown ,/var/log/customerlog,Cicm	equipment	Audit Mate Node Down	Node initialisation: mate node is down
CICM329	/var/log/customerlog	AuditMateActive	None	Unknown ,/var/log/customerlog,Cicm	equipment	Audit Mate Node Down	Node initialisation: mate node is active in state XXX
CICM330	/var/log/customerlog	CantDoPhysicalCheckOnLink	None	Unknown ,/var/log/customerlog,Platform	communications	Can't do physical check on link	Can't do physical check on link XXX
CICM331	/var/log/customerlog	CompFailureShutdown	None	Unknown ,/var/log/customerlog,Cicm	equipment	Component failure : shutdown	Component XXX has failed. Initiating shutdown. XXX
CICM332	/var/log/customerlog	BadTransition	None	Unknown ,/var/log/customerlog,Cicm	equipment	Bad transition on mate node	Bad transition on mate node from XXX to XXX
CICM333	/var/log/customerlog	NoAccessRemoteName	None	Unknown ,/var/log/customerlog,CicmEM	communications	No access to remote name	No access to the remote name in the MIB.
CICM334	Alarm_Trap_to_IEMS	MateFailure	None	CICM=<nodename>;NodeType=Cicm	equipment	Audit: Mate Node Failed	Mate node failed - Broadcast failure and ask components to promote to Master.
CICM334	Alarm_Trap_to_IEMS	MateRecovered	None	CICM=<nodename>;NodeType=Cicm	equipment	Audit: Mate Node Failed	Mate node recovered.

CICM335	/var/log/customerlog	RouteElementInvalid	None	Unknown ,/var/log/customerlog,Platform	communications	Route Element Invalid	Local route element XXX or remote route element XXX is invalid
CICM336	/var/log/customerlog	NetworkRecovery	None	Unknown ,/var/log/customerlog,Cicm	communications	Network loss and recovery	Network has been lost and then recovered, mate (slave) must reboot.
CICM337	Alarm_Trap_to_IEMS	NoMessageToA	Major	CICM=<nodename>;NodeType=Cicm;Component=Chassis	equipment	Message To Node A Failed	Failed to send message to Node A.
CICM337	Alarm_Trap_to_IEMS	NoMessageToAClear	None	CICM=<nodename>;NodeType=Cicm;Component=Chassis	equipment	Message To Node A Failed	Clear Failed to send message to Node A.
CICM338	/var/log/customerlog	NetworkElementHasFailed	None	Unknown ,/var/log/customerlog,Platform	communications	Network Element Failed	Network Element XXX Failed
CICM339	Alarm_Trap_to_IEMS	NoMessageFromB	Major	CICM=<nodename>;NodeType=Cicm	equipment	No Message Received From B	Have not received a message from Node B for 1.5*ALARM_POLL_PERIOD Seconds. XXX
CICM339	Alarm_Trap_to_IEMS	NoMessageFromBClear	None	CICM=<nodename>;NodeType=Cicm	equipment	No Message Received From B	Clear: Have not received a message from Node B for 1.5*ALARM_POLL_PERIOD Seconds. XXX
CICM340	/var/log/customerlog	CantSetLocalAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Can't set local adapter	Can't set local adapter, invalid adapter specified
CICM341	Alarm_Trap_to_IEMS	BackupFail	Minor	CICM=<nodename>;NodeType=Platform	processingError	Backup Fail.	Scheduled/on-demand backup failed during last iteration.
CICM341	Alarm_Trap_to_IEMS	BackupFailClear	None	CICM=<nodename>;NodeType=Platform	processingError	Backup Fail.	Scheduled/on-demand backup failed during last iteration.
CICM342	/var/log/customerlog	UnableToBindAdminIPAddressToInterface	None	Unknown ,/var/log/customerlog,Platform	communications	Unable to bind admin IP address to interface	Unable to bind admin IP address to interface XXX - will continue to attempt to bind
CICM344	/var/log/customerlog	CantSetSlaveAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Can't set slave adapter	Can't set slave adapter, invalid adapter specified XXX
CICM345	/var/log/customerlog	EMMateDown	None	Unknown ,/var/log/customerlog,CicmEM	communications	EM MAte Down	Mate node down. Name: XXX. XXX
CICM346	/var/log/customerlog	EMMibWriteFail	None	Unknown ,/var/log/customerlog,CicmEM	communications	EM Mate Down	Couldn't write EM remote node status to Mib
CICM348	/var/log/customerlog	ChangingSlaveAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Changing slave adapter	Changing slave adapter from XXX to XXX
CICM350	/var/log/customerlog	GetInterfaceDeviceMapping	None	Unknown ,/var/log/customerlog,Platform	communications	Get Interface Device Mapping Failed	Get Interface Device Mapping Failed
CICM352	/var/log/customerlog	CantMapAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Can't map adapter	Can't map XXX to an NT device, link state won't be checked

CICM354	/var/log/customerlog	maxRudpSessionsNotPresent	None	Unknown ,/var/log/customerlog,Cicm	communications	maxRudpSessionsNotPresent.	Maximum sessions configuration not present
CICM354	/var/log/customerlog	UnableToSetMaxRUDPSessions	None	Unknown ,/var/log/customerlog,Cicm	communications	UnableToSetMaxRUDPSessions.	unable to set max RUDP sessions [may already be started]
CICM355	/var/log/customerlog	VmgIpAddressBindFailed	None	Unknown ,/var/log/customerlog,Cicm	communications	Bind UDP socket for vmg failed.	Failed to start UDP socket. hr XXX
CICM355	/var/log/customerlog	VmgTerminationInvalid	None	Unknown ,/var/log/customerlog,Cicm	communications	VMG termination invalid.	VMG XXX termination XXX invalid
CICM356	/var/log/customerlog	AdapterDown	None	Unknown ,/var/log/customerlog,Platform	communications	Adapter down	Adapter XXX is down - aborting start until all adapters are up
CICM357	/var/log/customerlog	EchoServerPortNotPresent	None	Unknown ,/var/log/customerlog,Cicm	communications	EchoServerPortNotPresent.	Echo server port configuration not present
CICM358	/var/log/customerlog	UnableToMapNETOInterfaceNumber	None	Unknown ,/var/log/customerlog,Platform	communications	Unable to map ne to an interface number	Unable to map ne XXX to an interface number
CICM359	Alarm_Trap_to_IEMS	MateNodeComFailure	Major	CICM=<nodename>;NodeType=Platform	communications	Mate Node COM Failure.	COM method failed to mate node (XXX).
CICM359	Alarm_Trap_to_IEMS	MateNodeComFailureClear	None	CICM=<nodename>;NodeType=Platform	communications	Mate Node COM Failure.	COM method succeeded to mate node.
CICM360	/var/log/customerlog	AutoBindAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Auto-bind adapter problem	Auto-bind adapter XXX XXX
CICM361	/var/log/customerlog	HostPortNotPresent	None	Unknown ,/var/log/customerlog,Cicm	communications	HostPortNotPresent.	Host port configuration not present
CICM362	/var/log/customerlog	SwactRequestRejected	None	Unknown ,/var/log/customerlog,Platform	communications	Swact request rejected	Swact request rejected XXX
CICM363	/var/log/customerlog	CreateConnectionAckFailed	None	Unknown ,/var/log/customerlog,Cicm	communications	Create ConnectionAck Failed.	CreateConnectionAck::can't determine destination for message
CICM363	/var/log/customerlog	ModifyConnectionAckFailed	None	Unknown ,/var/log/customerlog,Cicm	communications	Modify ConnectionAck Failed.	ModifyConnectionAck::can't determine destination for message
CICM363	/var/log/customerlog	noPtimeCanBeNegotiated	None	Unknown ,/var/log/customerlog,Cicm	communications	no ptime can be negotiated.	Ensure a common ptime exists between the GWC and the CICM terminal audio profile
CICM363	**/var/log/customerlog**	**SystemShutdown**	**None**	**Unknown ,/var/log/customerlog,Cicm**	**communications**	**Subtract ConnectionAck Failed.**	**SubtractConnectionAck::can't determine destination for message**
CICM363	/var/log/customerlog	noPtimeCanBeNegotiated	None	Unknown ,/var/log/customerlog,Cicm	communications	no ptime can be negotiated.	Ensure a common ptime exists between the GWC and the CICM terminal audio profile
CICM363	/var/log/customerlog	noCodecCanBeNegotiated	None	Unknown ,/var/log/customerlog,Cicm	communications	no codec can be negotiated.	Ensure a common codec exists between the GWC and the CICM terminal audio profile

CICM364	/var/log/customerlog	RegisterGatewayFailed	None	Unknown ,/var/log/customerlog,Cicm	communications	Register Gateway Failed	Register Gateway XXX Failed
CICM364	/var/log/customerlog	UnRegisterGatewayFailed	None	Unknown ,/var/log/customerlog,Cicm	communications	UnRegister Gateway Failed	UnRegister Gateway XXX Failed
CICM365	/var/log/customerlog	MibSyncMateFail	None	Unknown ,/var/log/customerlog,Cicm	equipment	Mib Sync Mate Failure	Mate node failed during MIB syncronisation. This node will start partially Synchronised.
CICM366	/var/log/customerlog	MibSyncSCMPollfail	None	Unknown ,/var/log/customerlog,Cicm	equipment	Mib Sync SCM Poll Failure	Opening Service Control Manager FAILURE.
CICM367	/var/log/customerlog	ErrorDatafillTones	None	Unknown ,/var/log/customerlog,Cicm	equipment	Error Datafilling Tones	Error encountered datafilling tones!.
CICM368	/var/log/customerlog	NoMaxSessions	None	Unknown ,/var/log/customerlog,Cicm	equipment	Max Sessions Not Present	Invalid config. Max Sessions not present.
CICM368	/var/log/customerlog	MaxSessionsNotPresent	None	Unknown ,/var/log/customerlog,Cicm	communications	MaxSessionsNotPresent.	Maximum sessions configuration not specified
CICM369	/var/log/customerlog	NoDomainLicense	None	Unknown ,/var/log/customerlog,Cicm	equipment	No Domain License	No network domain license for terminal at XXX
CICM370	Alarm_Trap_to_IEMS	MateFailure	Major	CICM=<nodename>;NodeType=Platform	communications	Mate Failure.	Admin reports mate node failure.
CICM370	Alarm_Trap_to_IEMS	MateStarting	Major	CICM=<nodename>;NodeType=Platform	communications	Mate Failure.	Admin reports Mate Node start.
CICM371	/var/log/customerlog	TerminalError	None	Unknown ,/var/log/customerlog,Cicm	equipment	An Error Occured on the Terminal	Terminal Error XXX
CICM372	/var/log/customerlog	UnableToMapAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Unable to map adapter	Unable to map XXX adapter XXX to an ip address.
CICM373	/var/log/customerlog	UFTPFirmwareFileOpenFailed	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPFirmwareFileOpenFailed.	Failed to open file XXX.
CICM373	/var/log/customerlog	UFTPFirmwareFileOpenFailedFatal	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPFirmwareFileOpenFailed.	Invalid directory or file XXX not found
CICM373	/var/log/customerlog	UFTPFirmwareFileReadError	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPFirmwareFileReadError.	Firmware file XXX read error
CICM373	/var/log/customerlog	UFTPCommandFileReadError	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPCommandFileReadError.	UFTPCommandFileReadError
CICM373	/var/log/customerlog	UFTPCommandFileCreationError	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPCommandFileCreationError.	Command = XXX
CICM373	/var/log/customerlog	UFTPBaseDirectoryMissing	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPBaseDirectoryMissing.	UFTP base directory missing from registry
CICM374	/var/log/customerlog	ReadPollPeriodFail	None	Unknown ,/var/log/customerlog,CicmEM	communications	Poll Period Read Fail	Couldn't read gwPollPeriod from mib. Defaulting to 30 seconds.
CICM375	Alarm_Trap_to_IEMS	SAM21VersionMismatch	Minor	CICM=<nodename>;NodeType=Platform	processingError	SAM21 Version Mismatch.	SAM21 Version Mismatch. Version XXX

CICM375	Alarm_Trap_to_IEMS	SAM21VersionMismatchClear	None	CICM=<nodename>;NodeType=Platform	processingError	SAM21 Version Mismatch.	SAM21 Version Mismatch. Version XXX
CICM376	/var/log/customerlog	ShuttingDownTerminals	None	Unknown ,/var/log/customerlog,Cicm	communications	ShuttingDownTerminals.	Shutdown counter set to zero minutes, shutting down terminals immediately
CICM376	/var/log/customerlog	TerminalShutDownAborted	None	Unknown ,/var/log/customerlog,Cicm	communications	TerminalShutDownAborted.	Terminal shutdown aborted
CICM377	Alarm_Trap_to_IEMS	SyslogFailure	Major	CICM=<nodename>;NodeType=Platform	communications	Syslog Failure.	Syslog failure. Last stream in failure XXX.
CICM377	Alarm_Trap_to_IEMS	SyslogFailureClear	None	CICM=<nodename>;NodeType=Platform	communications	Syslog Failure.	Syslog failure clear.
CICM378	/var/log/customerlog	ExcessNodes	None	Unknown ,/var/log/customerlog,CicmEM	communications	Excessive Nodes on EM	More than 100 nodes present, unrecommended configuration
CICM379	/var/log/customerlog	RegisterSessionFailed	None	Unknown ,/var/log/customerlog,Cicm	communications	Register Session Failed	Register Session Failed on Gateway XXX
CICM379	/var/log/customerlog	RegisterSessionFailedRange	None	Unknown ,/var/log/customerlog,Cicm	communications	Register Gateway Failed	Register Gateway XXX Failed termination XXX is out of range
CICM379	/var/log/customerlog	RegisterSessionFailedInvalid	None	Unknown ,/var/log/customerlog,Cicm	communications	Register Gateway Failed	Register Gateway XXX Failed termination XXX is invalid
CICM379	/var/log/customerlog	CouldntStartAuditTimer	None	Unknown ,/var/log/customerlog,Cicm	communications	Couldn't start audit timer	Couldn't start audit timer
CICM380	Alarm_Trap_to_IEMS	FailedPollMG	None	CICM=<nodename>;NodeType=Platform	communications	Fail Poll MG	Failed to Poll Media Gateway XXX.
CICM380	Alarm_Trap_to_IEMS	FailedPollMGClear	None	CICM=<nodename>;NodeType=Platform	communications	Fail Poll MG	Failed to Poll Media Gateway XXX.
CICM381	Alarm_Trap_to_IEMS	NetworkLoss	Critical	CICM=<nodename>;NodeType=Platform	communications	Network Loss.	Critical network connection loss on adapter XXX
CICM381	Alarm_Trap_to_IEMS	ClearNetworkLoss	None	CICM=<nodename>;NodeType=Platform	communications	Network Loss.	Critical network connection loss cleared on adapter XXX
CICM381	Alarm_Trap_to_IEMS	NetworkLossMajor	Major	CICM=<nodename>;NodeType=Platform	communications	Network Loss.	Major network connection loss on adapter XXX
CICM381	Alarm_Trap_to_IEMS	ClearNetworkLossMajor	None	CICM=<nodename>;NodeType=Platform	communications	Network Loss.	Major network connection loss cleared on adapter XXX
CICM381	Alarm_Trap_to_IEMS	NetworkRedundancyLoss	Major	CICM=<nodename>;NodeType=Platform	communications	Network Redundancy Loss.	Network redundancy lost to the mate node
CICM381	Alarm_Trap_to_IEMS	ClearNetworkRedundancyLoss	None	CICM=<nodename>;NodeType=Platform	communications	Network Redundancy Loss.	Network redundancy restored to the mate node
CICM382	Alarm_Trap_to_IEMS	RemoteHostFail	Minor	CICM=<nodename>;NodeType=Platform	communications	Remote Host Fail.	Disabling client XXX with interface XXX.
CICM382	Alarm_Trap_to_IEMS	RemoteHostFailClear	None	CICM=<nodename>;NodeType=Platform	communications	Remote Host Fail.	Enabling client XXX with interface XXX.
CICM383	/var/log/customerlog	FirmwareUpgradeNotSupportedUFTPOverUnistim	None	Unknown ,/var/log/customerlog,Cicm	communications	FirmwareUpgradeNotSupportedUFTPOverUnistim.	Firmware upgrade is not supported via UFTP over Unistim. File XXX

CICM383	Alarm_Trap_to_IEMS	FirmwareUpgradeFail	None	CICM=<nodename>;NodeType=Cicm;Component=Terminals	communications	Firmware upgrade failure.	Firmware upgrade failure.
CICM383	Alarm_Trap_to_IEMS	FirmwareUpgradeFailClear	None	CICM=<nodename>;NodeType=Cicm;Component=Terminals	communications	Firmware upgrade failure.	Firmware upgrade failure.
CICM384	/var/log/customerlog	NodeIsolatedForcingTransitionFromMasterToSlave	None	Unknown ,/var/log/customerlog,Platform	communications	Node Isolated - Forcing transition from master to slave	Node Isolated - Forcing transition from master to slave
CICM385	/var/log/customerlog	SlaveNodeIsolated	None	Unknown ,/var/log/customerlog,Platform	communications	Slave Node isolated	Slave Node isolated
CICM386	/var/log/customerlog	UFTPmaxSessionsMIBDataFatal	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPmaxSessions value in the mib is incorrect	UFTPmaxSessions must be at least one. Value XXX is invalid
CICM386	/var/log/customerlog	UFTPmaxSessionsMIBDataNonFatal	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPmaxSessions value is missing from the mib	UFTPmaxSessions missing using default value XXX
CICM387	Alarm_Trap_to_IEMS	CommsFailedCicm	Major	CICM=<nodename>;NodeType=CICMEM;Cicm=<node IP address>	communications	CICM Poll Failed	Failed to Poll CICM Node XXX.
CICM387	Alarm_Trap_to_IEMS	CommsFailedCicmClear	None	CICM=<nodename>;NodeType=CICMEM;Cicm=<node IP address>	communications	CICM Poll Failed	Failed to Poll CICM Node XXX.
CICM388	/var/log/customerlog	UFTPtimerTimeoutMIBDataNonFatal	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTPtimerTimeout value is missing from the mib	UFTPtimerTimeout missing using default value XXX
CICM389	/var/log/customerlog	UFTPInvalidClientMessage	None	Unknown ,/var/log/customerlog,Cicm	communications	UFTP_INVALID_CLIENT_MESSAGE	UFTP_INVALID_CLIENT_MESSAGE XXX value XXX is invalid
CICM390	Alarm_Trap_to_IEMS	FailedPAMConn	Major	CICM=<nodename>;NodeType=CicmEM	communications	Failed To Connect PAM server	PAM server XXX is not responding to authentication requests
CICM390	Alarm_Trap_to_IEMS	FailedPAMConnClear	None	CICM=<nodename>;NodeType=CicmEM	communications	Failed To Connect PAM server	PAM server XXX is now responding to authentication requests
CICM391	/var/log/customerlog	ProcessNetworkStateTransitionStateError	None	Unknown ,/var/log/customerlog,Platform	communications	Invalid transition	ProcessNetworkStateTransition() called with invalid transition XXX
CICM392	/var/log/customerlog	PAMServerTMO	None	Unknown ,/var/log/customerlog,CicmEM	communications	PAM Server TMO	Timeout occurred whilst awaiting response from PAM server XXX
CICM393	/var/log/customerlog	TakeoverManualAbortedIsNotImplemented	None	Unknown ,/var/log/customerlog,Platform	communications	Takeover manual aborted, is not implemented	Takeover manual aborted, is not implemented
CICM394	/var/log/customerlog	FailedToUnbindAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Fatal error: Unable to unbind adapter	Fatal error: Unable to unbind adapter.
CICM395	/var/log/customerlog	MateNodeFailedTemporarily	None	Unknown ,/var/log/customerlog,Platform	communications	Mate node failed temporarily	Mate node failed temporarily for XXX iterations
CICM396	/var/log/customerlog	TakeoverAbort	None	Unknown ,/var/log/customerlog,Platform	communications	Takeover aborted, reverting to Master	Takeover aborted, reverting to Master
CICM397	/var/log/customerlog	MateNodeLostForcingTransitionFromSlaveToMaster	None	Unknown ,/var/log/customerlog,Platform	communications	Mate node lost - Forcing transition from slave to master	Mate node lost - Forcing transition from slave to master
CICM398	/var/log/customerlog	MateNodeLost	None	Unknown ,/var/log/customerlog,Platform	communications	Mate node lost	Mate node lost

CICM399	/var/log/customerlog	RouteMapError	None	Unknown ,/var/log/customerlog,Platform	communications	Route map error	Resetting adapter, state= XXX mate=XXX
CICM500	/var/log/customerlog	StateChange	None	Unknown ,/var/log/customerlog,Platform	processingError	State Change.	Admin reports a state change to XXX for component XXX.
CICM503	/var/log/customerlog	NetAccessStateChange	None	Unknown ,/var/log/customerlog,CicmEM	communications	Network Access State Change	Netork access state change to XXX
CICM504	/var/log/customerlog	EMNetworkChange	None	Unknown ,/var/log/customerlog,CicmEM	communications	EM Network State Change	Network connectivity XXX. hr=XXX
CICM505	/var/log/customerlog	StopMonitoring	None	Unknown ,/var/log/customerlog,CicmEM	communications	Stop Monitoring	Stopped monitoring node XXX
CICM506	/var/log/auditlog	MonitorStart	None	Unknown ,/var/log/auditlog,CicmEM	communications	Start Monitoring	Started to monitor node XXX.
CICM507	/var/log/auditlog	ConnectToPAMServer	None	Unknown ,/var/log/auditlog,CicmEM	environmental	Connect to PAM.	Connect to PAM.
CICM508	/var/log/customerlog	SlaveInstructedToChangeToInvalidAdapter	None	Unknown ,/var/log/customerlog,Platform	communications	Slave instructed to change to invalid adapter, selecting default	Slave instructed to change to invalid adapter, selecting default
CICM509	Alarm_Trap_to_IEMS	ProcessStateChange	Critical	CICM=<nodename>;NodeType=Platform;SoftwareComponent=<component id>	processingError	Critical Process State Change.	Critical Process XXX is not running.
CICM509	Alarm_Trap_to_IEMS	ProcessStateChangeClear	None	CICM=<nodename>;NodeType=Platform;SoftwareComponent=<component id>	processingError	Critical Process State Change.	Critical Process XXX is running.
CICM509	Alarm_Trap_to_IEMS	ServiceStateChange	Major	CICM=<nodename>;NodeType=Platform;SoftwareComponent=<component id>	processingError	Service State Change.	Service XXX is not running.
CICM509	Alarm_Trap_to_IEMS	ServiceStateChangeClear	None	CICM=<nodename>;NodeType=Platform;SoftwareComponent=<component id>	processingError	Service State Change.	Service XXX is running.
CICM510	/var/log/auditlog	EMMateUp	None	Unknown ,/var/log/auditlog,CicmEM	environmental	EM Mate Up.	EM Mate Up. Name: XXX.
CICM512	/var/log/customerlog	StartSWACT	None	Unknown ,/var/log/customerlog,Platform	processingError	Start SWACT.	Admin reports a request to start SWACT.
CICM512	/var/log/customerlog	PromoteToMaster	None	Unknown ,/var/log/customerlog,Platform	processingError	Promote to Master.	Admin reports a request to promote to Master.
CICM512	/var/log/customerlog	DemoteToSlave	None	Unknown ,/var/log/customerlog,Platform	processingError	Demote to Slave.	Admin reports a request to demote to slave.
CICM513	/var/log/auditlog	ChangingLocalAdapter	None	Unknown ,/var/log/auditlog,Platform	communications	Changing local adapter	Changing local adapter from XXX to XXX
CICM603	/var/log/customerlog	InvalidEventReport	None	Unknown ,/var/log/customerlog,Platform	processingError	Invalid Event Report.	Invalid report received from Admin.
CICM604	/var/log/customerlog	MateSyncErrState	None	Unknown ,/var/log/customerlog,Platform	processingError	Mate sync error state.	request for mate synchronisation received in state XXX.
CICM605	/var/log/customerlog	GWRegBadState	None	Unknown ,/var/log/customerlog,Platform	equipment	GW Reg in Bad State.	Gateway registration received in state XXX.

CICM606	/var/log/customerlog	PremSlaveGWReg	None	Unknown ,/var/log/customerlog,Platform	equipment	Premature reg slave gw.	Premature registration of the slave gateway.
CICM607	/var/log/customerlog	SwactReqRemoteMGM	None	Unknown ,/var/log/customerlog,Platform	equipment	Swact Request from Remote MGM.	Swact request received from the remote MGM.
CICM608	/var/log/customerlog	RetransRUDPMessagesThrottled	None	Unknown ,/var/log/customerlog,Platform	communications	Retransmitted RUDP messages.	Retransmitted XXX RUDP messages, XXX retransmissions were throttled.
CICM609	/var/log/customerlog	RetransRUDPMessages	None	Unknown ,/var/log/customerlog,Platform	communications	Retransmitted RUDP messages.	Retransmitted XXX RUDP messages.
CICM610	/var/log/customerlog	LossOfLogs	None	Unknown ,/var/log/customerlog,Platform	communications	Loss of logs.	XXX logs have been lost due to buffering.
CICM610	/var/log/customerlog	LossOfTraps	None	Unknown ,/var/log/customerlog,Platform	communications	Loss of traps.	XXX traps have been lost due to buffering.
CICM611	Alarm_Trap_to_IEMS	ThresholdReached	Major	CICM=<nodename>;NodeType=Platform	qualityOfService	Resource Threshold Crossed	Resource XXX is near or above its threshold of XXX
CICM611	Alarm_Trap_to_IEMS	ThresholdReachedClear	None	CICM=<nodename>;NodeType=Platform	qualityOfService	Threshold Crossed	Resource XXX is near or above its threshold value of XXX
CICM612	/var/log/customerlog	AuditStart	None	Unknown ,/var/log/customerlog,Cicm	environmental	Start Audit.	Starting the daily audit.
CICM612	/var/log/customerlog	AuditEnd	None	Unknown ,/var/log/customerlog,Cicm	environmental	Audit Complete	Daily audit completed.
CICM614	/var/log/customerlog	MsgFromInvalidComp	None	Unknown ,/var/log/customerlog,Cicm	equipment	Message from invalid component	Message received from invalid component type = 0x XXX
CICM615	/var/log/customerlog	NodeForcedMaster	None	Unknown ,/var/log/customerlog,Cicm	equipment	Node forced to master	Node is being forced to become master.
CICM615	/var/log/customerlog	NodeForcedSlave	None	Unknown ,/var/log/customerlog,Cicm	equipment	Node forced to slave	Node is being forced to become slave.
CICM617	/var/log/customerlog	MibSyncPollFail	None	Unknown ,/var/log/customerlog,Cicm	equipment	Mib Sync Poll Failure	Network status remote state query returned hr=0x XXX.
CICM618	/var/log/customerlog	NoLineID	None	Unknown ,/var/log/customerlog,Cicm	equipment	No Line ID	User XXX has no LineId attribute in the mib.
CICM619	/var/log/customerlog	NoToneset	None	Unknown ,/var/log/customerlog,Cicm	equipment	No Toneset Found	Toneset XXX not found A standard tone will be used in place of all toneIDs
CICM620	/var/log/customerlog	InvalidToneIndex	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Tone Component Index	Invalid tone component index toneset XXX toneid XXX
CICM621	/var/log/customerlog	NoVolume	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Volume Datafilled	No volume datafilled for toneset XXX toneid XXX
CICM622	/var/log/customerlog	Invalidtone	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Tone Frequency	Invalid tone frequency count toneset XXX toneid XXX

CICM623	/var/log/customerlog	NoFrequency	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Frequency Datafilled	No frequency datafilled for toneset XXX toneid XXX
CICM624	/var/log/customerlog	InvalidCadenceCount	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Cadence Count	Invalid tone cadence count toneset XXX toneid XXX
CICM625	/var/log/customerlog	NoCadenceOff	None	Unknown ,/var/log/customerlog,Cicm	equipment	No Cadence Off	No Cadence off datafilled for toneset XXX toneid XXX
CICM625	/var/log/customerlog	NoCadenceOn	None	Unknown ,/var/log/customerlog,Cicm	equipment	No Cadence On	No Cadence on datafilled for toneset XXX toneid XXX
CICM627	/var/log/customerlog	InvalidConnMap	None	Unknown ,/var/log/customerlog,Cicm	equipment	Connection mapped to invalid line	Connection XXX is mapped to line XXX which isn't valid.
CICM628	/var/log/customerlog	ConnNonE1	None	Unknown ,/var/log/customerlog,Cicm	equipment	Connection mapped not in E1_CONN state	Connection XXX is mapped to line XXX which isn't in E1_CONNECTION state.
CICM629	/var/log/customerlog	ResetNoConn	None	Unknown ,/var/log/customerlog,Cicm	equipment	Reset Connection isn't in NO_CONNECTION state	Resetting connection for line XXX which isn't in NO_CONNECTION state.
CICM630	/var/log/customerlog	CreateConFail	None	Unknown ,/var/log/customerlog,Cicm	equipment	Create Connection Fail	Create connection failed. Call type = XXX, result = XXX
CICM631	/var/log/customerlog	DelConFail	None	Unknown ,/var/log/customerlog,Cicm	equipment	Delete Connection Fail	Delete connection failed.
CICM632	/var/log/customerlog	NoLineObject	None	Unknown ,/var/log/customerlog,Cicm	equipment	No line object	Create Connection: Could not find line object for conflicting connection XXX with lineid = XXX
CICM633	/var/log/customerlog	CorruptConnMap	None	Unknown ,/var/log/customerlog,Cicm	equipment	Corrupt Connection Map	Connection map is corrupt, or media control is reusing handles, connection id XXX is already in use my lineid XXX.
CICM634	/var/log/customerlog	NoConIDMap	None	Unknown ,/var/log/customerlog,Cicm	equipment	No Connection Id map	Connection map is corrupt, or media control is reusing handles, connection id XXX could not be found in the map.
CICM635	/var/log/customerlog	UnableChangeLoss	None	Unknown ,/var/log/customerlog,Cicm	equipment	Unable Change Rx Loss	Unable to change rx loss for connection XXX
CICM636	/var/log/customerlog	TooManyFeatures	None	Unknown ,/var/log/customerlog,Cicm	equipment	Too Many Features	Terminal type has too many features on the main set (max is XXX).
CICM637	/var/log/customerlog	TooManyFeaturesExt	None	Unknown ,/var/log/customerlog,Cicm	equipment	Too Many Features	Terminal type has too many features on the extension set (max is XXX).
CICM638	/var/log/securitylog	AuthUserProblem	None	Unknown ,/var/log/securitylog,Cicm	equipment	Auth User Failed	User XXX
CICM639	/var/log/securitylog	LogoutSuccess	None	Unknown ,/var/log/securitylog,Cicm	equipment	Logout Success	User XXX

CICM639	/var/log/securitylog	LoginSuccess	None	Unknown ,/var/log/securitylog,Cicm	equipment	Login Success	User XXX
CICM641	/var/log/securitylog	ChangePassword	None	Unknown ,/var/log/securitylog,Cicm	equipment	Change Password Attempt	User XXX
CICM642	/var/log/securitylog	ReleaseAuth	None	Unknown ,/var/log/securitylog,Cicm	equipment	Release Authentication	
CICM643	/var/log/customerlog	InvalidFirmwarePrOt	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Firmware Protocol	Invalid FirmwareProtocol for TerminalType= XXX
CICM644	/var/log/customerlog	InvalidFWLevel	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Firmware Level	Invalid Firmware level for TerminalType= XXX
CICM645	/var/log/customerlog	NoFWLevel	None	Unknown ,/var/log/customerlog,Cicm	equipment	No Firmware Level	Terminal has no firmware level recorded in the MIB
CICM646	/var/log/customerlog	InvalidUFTHost	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid UFTP Host	Invalid UFTP host port
CICM647	/var/log/customerlog	InvalidUnistimHost	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Unistim Host	Invalid Unistim host address
CICM648	/var/log/customerlog	InvalidFWTFTPAddr	None	Unknown ,/var/log/customerlog,Cicm	equipment	Invalid Firmware TFPT Address	Invalid Firmware TFTP Address for TerminalType=XXX
CICM649	/var/log/auditlog	ConfigDataChange	None	Unknown ,/var/log/auditlog,Platform	processingError	Config Data Change.	Admin reports a configuration data change.
CICM650	/var/log/auditlog	InitialisingAsMaster	None	Unknown ,/var/log/auditlog,Platform	communications	Initialising as master	Initialising as master
CICM650	/var/log/auditlog	InitialisingAsMasterNoSlave	None	Unknown ,/var/log/auditlog,Platform	communications	Initialising as master (no slave)	Initialising as master (no slave)
CICM650	/var/log/auditlog	InitialisingAsSlave	None	Unknown ,/var/log/auditlog,Platform	communications	Initialising as slave	Initialising as slave
CICM650	/var/log/auditlog	StartingTakeover	None	Unknown ,/var/log/auditlog,Platform	communications	Starting takeover	Starting takeover
CICM650	/var/log/auditlog	TakeoverSucceedNowSlave	None	Unknown ,/var/log/auditlog,Platform	communications	Takeover succeeded, now slave	Takeover succeeded, now slave
CICM650	/var/log/auditlog	TakeoverSucceedNowMaster	None	Unknown ,/var/log/auditlog,Platform	communications	Takeover succeeded, now Master	Takeover succeeded, now Master
CICM650	/var/log/auditlog	ForcingTransitionFromSlaveToMaster	None	Unknown ,/var/log/auditlog,Platform	communications	Forcing transition from slave to master	Forcing transition from slave to master
CICM650	/var/log/auditlog	ForcingTransitionFromMasterToSlave	None	Unknown ,/var/log/auditlog,Platform	communications	Forcing transition from master to slave	Forcing transition from master to slave
CICM650	/var/log/auditlog	MateNodeRecoveredForcingtransitionFromSlaveToMaster	None	Unknown ,/var/log/auditlog,Platform	communications	Mate Node Recovered - Forcing transition from slave to master	Mate Node Recovered - Forcing transition from slave to master
CICM650	/var/log/auditlog	ProcessingSwact	None	Unknown ,/var/log/auditlog,Platform	communications	Processing Swact	Processing Swact request
CICM652	/var/log/auditlog	addGateway	None	Unknown ,/var/log/auditlog,CicmEM	communications	Adding a gateway	Gateway XXX has been added.
CICM653	/var/log/auditlog	deleteGateway	None	Unknown ,/var/log/auditlog,CicmEM	communications	Deleting a gateway	Deleting gateway XXX
CICM654	/var/log/auditlog	addProfile	None	Unknown ,/var/log/auditlog,CicmEM	communications	Adding a profile	Adding a XXX profile for gateway XXX
CICM655	/var/log/auditlog	delProfile	None	Unknown ,/var/log/auditlog,CicmEM	communications	Deleting a profile	Deleting XXX profile for gateway XXX
CICM656	Alarm_Trap_to_IEMS	maxRxRateExceed	Minor	CICM=<nodename>;NodeType=Platform	processingError	Max Rx Rate Exceeded.	Max rx rate of XXX has been exceeded by rate XXX.

CICM656	Alarm_Trap_to_IEMS	maxRxRateExceedClear	None	CICM=<nodename>;NodeType=Platform	processingError	Max Rx Rate Exceeded.	Clear max rx rate of XXX has been exceeded.
CICM657	Alarm_Trap_to_IEMS	maxCreateAttempts	Minor	CICM=<nodename>;NodeType=Platform	communications	Max Creation Attempts.	Reached the max creation attempts for the session.
CICM657	Alarm_Trap_to_IEMS	maxCreateAttemptsClear	None	CICM=<nodename>;NodeType=Platform	communications	Max Creation Attempts.	Reached the max creation attempts for the session.
CICM658	/var/log/auditlog	MateNodeRecovered	None	Unknown ,/var/log/auditlog,Platform	communications	Mate node recovered	Mate node recovered
CICM659	/var/log/auditlog	SlaveAdapterRecovered	None	Unknown ,/var/log/auditlog,Platform	communications	Slave adapter recovered	Slave adapter XXX recovered
CICM660	/var/log/securitylog	SuccessfulPAMAuthentication	None	Unknown ,/var/log/securitylog,CicmEM	environmental	Successful PAM Authentication.	User XXX has started a session on the CICM-EM
CICM661	/var/log/securitylog	PAMAuthenticationFailure	None	Unknown ,/var/log/securitylog,CicmEM	processingError	PAM Authenication Failure.	User XXX authentication failure
CICM662	/var/log/securitylog	UserRevoked	None	Unknown ,/var/log/securitylog,CicmEM	environmental	User Privileges Revoked.	Privileges revoked
CICM663	/var/log/securitylog	UserUpgraded	None	Unknown ,/var/log/securitylog,CicmEM	environmental	User Privileges upgraded.	Privileges upgraded
CICM664	/var/log/securitylog	InactiveUserTMO	None	Unknown ,/var/log/securitylog,CicmEM	environmental	Inactive User Timeout.	User XXX is no longer active on the CICM-EM
CICM665	/var/log/auditlog	NetworkElementHasRecovered	None	Unknown ,/var/log/auditlog,Platform	communications	Network Element recovered	Network Element XXX recovered
CICM668	Alarm_Trap_to_IEMS	MaxNoSessions	None	CICM=<nodename>;NodeType=Cicm	processingError	Reached the maximum number of sessions.	Current number of active sessions has reached the maximum of XXX.
CICM668	Alarm_Trap_to_IEMS	MaxNoSessionsClear	None	CICM=<nodename>;NodeType=Cicm	processingError	Reached the maximum number of sessions.	Current number of active sessions is below the maximum of XXX.
CICM680	/var/log/auditlog	RegisterGatewaySucceeded	None	Unknown ,/var/log/auditlog,Cicm	communications	Register Gateway Succeeded	Register Gateway XXX Succeeded
CICM681	/var/log/auditlog	ConfigurationChange	None	Unknown ,/var/log/auditlog,CicmEM	communications	Configuration change	XXX
CICM682	/var/log/auditlog	ProvisioningChange	None	Unknown ,/var/log/auditlog,CicmEM	communications	Provisioning change	XXX
CICM749	/var/log/securitylog	AccountDisabled	None	Unknown ,/var/log/securitylog,Cicm	equipment	Account Disabled	User XXX
CICM750	/var/log/securitylog	ChangePasswordFail	None	Unknown ,/var/log/securitylog,Cicm	equipment	Change Password Attempt	User XXX
CICM801	Alarm_Trap_to_IEMS	bhhcaMinorAlarm	Minor	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Minor Alarm	BHHCA is close to maximum value.
CICM801	Alarm_Trap_to_IEMS	bhhcaMinorAlarmClear	None	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Minor Alarm	BHHCA is close to maximum value.
CICM802	Alarm_Trap_to_IEMS	bhhcaMajorAlarm	Major	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Major Alarm	BHHCA is at Maximum Limit. Calls may not succeed.
CICM802	Alarm_Trap_to_IEMS	bhhcaMajorAlarmClear	None	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Major Alarm	BHHCA is at Maximum Limit. Calls may not succeed.
CICM803	Alarm_Trap_to_IEMS	bhhcaCriticalAlarm	Critical	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Critical Alarm	BHHCA is well above Maximum Limit. Calls will be Throttled.

CICM803	Alarm_Trap_to_IEMS	bhhcaCriticalAlarm Clear	None	CICM=<nodename>;NodeType=Cicm	qualityOfService	BHHCA Critical Alarm	BHHCA is well above Maximum Limit. Calls will be Throttled.
CICM804	Alarm_Trap_to_IEMS	registryFlushAlarm	Minor	CICM=<nodename>;NodeType=Platform	equipment	Registry Flush Minor Alarm	Registry has not been flushed for 1 hour. Registry data could be lost if power outage occurs.
CICM804	Alarm_Trap_to_IEMS	registryFlushAlarm Clear	None	CICM=<nodename>;NodeType=Platform	equipment	Registry Flush Minor Alarm	Registry has not been flushed for 1 hour. Registry data could be lost if power outage occurs.

Appendix G: Ethernet Routing Switch 8600 Trap List

<?xml version="1.0" encoding="ISO-8859-1" ?>

- <!--

```
    severity = 6|5|4|3|2|1
Critical = 1
Major = 2
Minor = 3
Warning = 4
Clear = 5
Info = 6
```

-->

- <TRAPS>

- <TRAP oid="**.1.3.6.1.2.1.16.0.1**" name="**risingAlarm**">

- <PROPERTIES>

<eventprop name="**severity**" value="**3**" />

<eventprop name="**logName**" value="**PP**" />

<eventprop name="**logNumber**" value="**310**" />

<eventprop name="**eventType**" value="**TBL**" />

<eventprop name="**eventLabel**" value="**PP Fault**" />

<eventprop name="**category**" value="**qualityOfService**" />

<eventprop name="**entity**" value="**$ip_alarmStatus_$1**" />

<eventprop name="**componentID**" value="**PP8600=$ip; alarmIndex=$1**" />

<eventprop name="**alarmClear**" value="**3**" />

<eventprop name="**probableCause**" value="**Threshold crossed.**" />

<eventprop name="**description**" value="**Threshold Crossed: alarmIndex= $1(Threshold= $2 alarmValue= $3)**" />

<eventprop name="**specificProblem**" value="**Rising threshold crossed**" />

</PROPERTIES>

- <VARBINDS>

<varbind name="**.1.3.6.1.2.1.16.3.1.1.1**" property="**$1**" />

<varbind name="**.1.3.6.1.2.1.16.3.1.1.7**" property="**$2**" />

<varbind name="**.1.3.6.1.2.1.16.3.1.1.5**" property="**$3**" />

</VARBINDS>

</TRAP>

- <TRAP oid="**.1.3.6.1.2.1.16.0.2**" name="**fallingAlarm**">

- <PROPERTIES>

<eventprop name="**severity**" value="**5**" />

<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**311**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**qualityOfService**" />
<eventprop name="**entity**" value="**$ip_alarmStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; alarmIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Threshold crossed**" />
<eventprop name="**description**" value="**Threshold Crossed: alarmIndex = $1(Threshold = $2 alarmValue = $3)**" />
<eventprop name="**specificProblem**" value="**Falling threshold crossed**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.16.3.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.16.3.1.1.8**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.16.3.1.1.5**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.6.3.1.1.5.1.0**" name="**coldStart**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**313**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**operator**" />
<eventprop name="**entity**" value="**$ip_coldStart**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Agent reinitialized itself with default settings**" />
<eventprop name="**description**" value="**A coldStart trap signifies that the snmp agent is reinitializing itself with default settings.**" />
<eventprop name="**specificProblem**" value="**Agent reinitialized itself with default settings**" />
</PROPERTIES>

</TRAP>

- <TRAP oid="**.1.3.6.1.6.3.1.1.5.2.0**" name="**warmStart**">

- <PROPERTIES>

<eventprop name="**severity**" value="**5**" />

<eventprop name="**logName**" value="**PP**" />

<eventprop name="**logNumber**" value="**315**" />

<eventprop name="**eventType**" value="**INFO**" />

<eventprop name="**eventLabel**" value="**PP Fault**" />

<eventprop name="**category**" value="**operator**" />

<eventprop name="**entity**" value="**$ip_warmstart**" />

<eventprop name="**componentID**" value="**PP8600=$ip**" />

<eventprop name="**alarmClear**" value="**3**" />

<eventprop name="**probableCause**" value="**Agent reinitialized itself with its configuration unaltered.**" />

<eventprop name="**description**" value="**A warmStart trap signifies that the SNMPv2 agent is reinitializing itself such that its configuration is unaltered.**" />

<eventprop name="**specificProblem**" value="**Agent reinitialized itself with its configuration unaltered.**" />

</PROPERTIES>

</TRAP>

- <TRAP oid="**.1.3.6.1.6.3.1.1.5.3.0**" name="**linkDown**">

- <PROPERTIES>

<eventprop name="**severity**" value="**2**" />

<eventprop name="**logName**" value="**PP**" />

<eventprop name="**logNumber**" value="**317**" />

<eventprop name="**eventType**" value="**TBL**" />

<eventprop name="**eventLabel**" value="**PP Fault**" />

<eventprop name="**category**" value="**communications**" />

<eventprop name="**entity**" value="**$ip_linkStatus_$1**" />

<eventprop name="**componentID**" value="**PP8600=$ip; ifIndex=$1**" />

<eventprop name="**alarmClear**" value="**3**" />

<eventprop name="**probableCause**" value="**loss of communication**" />

<eventprop name="**description**" value="**Link Down: ifIndex = $1(AdminStatus = $2 OperationStatus = $3 Port = $p Slot = $s)**" />

<eventprop name="**specificProblem**" value="**Generic Link Status**" />

</PROPERTIES>

- <VARBINDS>

<varbind name="**.1.3.6.1.2.1.2.2.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.2.2.1.7**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.2.2.1.8**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.6.3.1.1.5.4.0**" name="**linkUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**318**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_linkStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ifIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**communication regained**" />
<eventprop name="**description**" value="**Link Up: ifIndex = $1(AdminStatus = $2 OperationStatus = $3 Port = $p Slot = $s)**" />
<eventprop name="**specificProblem**" value="**Generic Link Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.2.2.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.2.2.1.7**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.2.2.1.8**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.6.3.1.1.5.5.0**" name="**authenticationFailure**">
- <PROPERTIES>
<eventprop name="**severity**" value="**4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**319**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**security**" />
<eventprop name="**entity**" value="**$ip_authenticationFailure**" />

<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**6**" />
<eventprop name="**probableCause**" value="**Authentication failure**" />
<eventprop name="**description**" value="**Authentication failure occured**" />
<eventprop name="**specificProblem**" value="**Authentication failure**" />
</PROPERTIES>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.6**" name="**rcnChasPowerSupplyDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**322**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcnSupplyStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SupplyId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Power Supply down**" />
<eventprop name="**description**" value="**Power Supply Status: SupplyId = $1(OperationStatus = $2)**" />
<eventprop name="**specificProblem**" value="**Power Supply Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.8.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.8.1.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.6**" name="**rcChasPowerSupplyDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**322**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />

<eventprop name="**entity**" value="**$ip_rcSupplyStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SupplyId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Power supply down**" />
<eventprop name="**description**" value="**Power Supply Status: SupplyId = $1(OperationStatus = $2)**" />
<eventprop name="**specificProblem**" value="**Power Supply Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.8.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.8.1.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.14**" name="**rcChasPowerSupplyUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**323**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcSupplyStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SupplyId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Power supply up**" />
<eventprop name="**description**" value="**Power Supply Status: SupplyId = $1(OperationStatus = $2)**" />
<eventprop name="**specificProblem**" value="**Power Supply Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.8.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.8.1.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.14**" name="**rcnChasPowerSupplyUp**">
- <PROPERTIES>

<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**323**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcnSupplyStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SupplyId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Power supply up**" />
<eventprop name="**description**" value="**Power Supply Status: SupplyId = $1(OperationStatus = $2)**" />
<eventprop name="**specificProblem**" value="**Power Supply Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.8.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.8.1.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.7**" name="**rcnChasFanDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**324**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcnFanStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; fanId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Fan status down**" />
<eventprop name="**description**" value="**Fan Down: fanId= $1(OperationStatus = $2)**" />
<eventprop name="**specificProblem**" value="**Fan down**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.7.1.1.1**" property="**$1**" />

<varbind name="**.1.3.6.1.4.1.2272.1.4.7.1.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.7**" name="**rcChasFanDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**324**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcFanStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; fanId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Fan Status Down**" />
<eventprop name="**description**" value="**Fan Down: fanId= $1(OperationStatus = $2)**" />
<eventprop name="**specificProblem**" value="**Fan down**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.7.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.7.1.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.21**" name="**rcnChasFanUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**325**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcnFanStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; fanId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Fan Status Up**" />
<eventprop name="**description**" value="**Fan Up: fanId= $1(OperationStatus = $2)**" />

<eventprop name="**specificProblem**" value="**Fan Up**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.7.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.7.1.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.21**" name="**rcChasFanUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**325**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcFanStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; fanId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Fan Status Up**" />
<eventprop name="**description**" value="**Fan Up: fanId= $1(OperationStatus = $2)**" />
<eventprop name="**specificProblem**" value="**Fan Up**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.7.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.7.1.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.11**" name="**rcn2kCardDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**326**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcn2KCardStatus_$1**" />

<eventprop name="**componentID**" value="**PP8600=$ip; cardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Rc 2k Card Down**" />
<eventprop name="**description**" value="**Card Down: cardIndex = $1(AdminStatus = $2 OperationStatus = $3)**" />
<eventprop name="**specificProblem**" value="**RC 2k Card Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.4**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.5**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.11**" name="**rc2kCardDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**326**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rc2KCardStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; cardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Rc 2k Card Down**" />
<eventprop name="**description**" value="**Card Down: cardIndex = $1(AdminStatus = $2 OperationStatus = $3)**" />
<eventprop name="**specificProblem**" value="**RC 2k Card Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.4**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.5**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.12**" name="**rcn2kCardUp**">

- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**327**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcn2KCardStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; cardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Card status Up**" />
<eventprop name="**description**" value="**Card Up: cardIndex = $1(AdminStatus = $2 OperationStatus = $3)**" />
<eventprop name="**specificProblem**" value="**RC 2k Card Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.4**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.5**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.12**" name="**rc2kCardUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**327**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rc2KCardStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; cardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Card Up**" />
<eventprop name="**description**" value="**Card Up: cardIndex = $1(AdminStatus = $2 OperationStatus = $3)**" />
<eventprop name="**specificProblem**" value="**RC 2K Card Status**" />

</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.4**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.5**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.13**" name="**rcn2kTemperature**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**328**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcn2kTemperature**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Over-heating of the chassis detected**" />
<eventprop name="**description**" value="**Chassis over-heating: rc2kChassisTemperature = $1**" />
<eventprop name="**specificProblem**" value="**RC 2K Chassis Temperature**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.1.2**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.3**" name="**rcnErrorNotification**">
- <PROPERTIES>
<eventprop name="**severity**" value="**$1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**329**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_ErrorNotification**" />

<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Error condition occured**" />
<eventprop name="**description**" value="**Error occured: Error Level = $1(Error Code = $2 Error Text = $3)**" />
<eventprop name="**specificProblem**" value="**RC 2K Error**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.20.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.20.2**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.20.3**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.8**" name="**rcnLinkOscillation**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**330**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_linkOscillation_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; portIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Link Oscillation detected**" />
<eventprop name="**description**" value="**LinkOscillation: portIndex = $1**" />
<eventprop name="**specificProblem**" value="**RC Link Oscillation**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.9**" name="**rcnMacViolation**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />

<eventprop name="**logNumber**" value="**331**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_MacViolation_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; portIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**RC Mac Violation**" />
<eventprop name="**description**" value="**RC Mac Violation: portIndex= $1(rcErrorText = $2)**" />
<eventprop name="**specificProblem**" value="**RC Mac violation**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.20.3**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.10**" name="**rcnSonetTrap**">
- <PROPERTIES>
<eventprop name="**severity**" value="**4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**332**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_ SonetTrap_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; portIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Sonet port status change**" />
<eventprop name="**description**" value="**Sonet Trap: portIndex = $1(TrapType = $2 TrapIndication = $3)**" />
<eventprop name="**specificProblem**" value="**Sonet port status change**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.26.5.1**" property="**$2**" />

<varbind name="**.1.3.6.1.4.1.2272.1.26.5.2**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.4**" name="**rcnStpNewRoot**">
- <PROPERTIES>
<eventprop name="**severity**" value="**4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**333**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_StpNewRoot _$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; stgId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Stp New Root**" />
<eventprop name="**description**" value="**Stp New Root: stgId = $1**" />
<eventprop name="**specificProblem**" value="**Stp New Root**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.13.4.1.1**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.5**" name="**rcnStpTopologyChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**334**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_ StpTopoChange_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; stgId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Stp Topology change**" />
<eventprop name="**description**" value="**Stp Topology change: stgId= $1(portIndex = $2)**"
/>

<eventprop name="**specificProblem**" value="**Stp Topology change**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.13.4.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.16**" name="**rcnStpTCN**">
- <PROPERTIES>
<eventprop name="**severity**" value="**4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**335**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_StpTCN_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; portIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Stp TCN**" />
<eventprop name="**description**" value="**Stp TCN: portIndex= $1(stgId= $2 BridgeAddress= $3)**" />
<eventprop name="**specificProblem**" value="**Stp TCN**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.13.4.1.1**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.13.4.1.4**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.15**" name="**rcn2kAtmPvcLinkStateChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**$4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**336**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />

<eventprop name="**category**" value="**environmental**" />
<eventprop name="**entity**" value="**$ip_LinkState_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rc2kAtmPvcIfIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**PVC link status change**" />
<eventprop name="**description**" value="**Atm Pvc Link State Change: AtmPvcIfIndex = $1(AtmPvcVpi = $2 AtmPvcVci = $3 AtmPvcOamVcStatus = $4)**" />
<eventprop name="**specificProblem**" value="**PVC link status change**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.9.3.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.9.3.1.2**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.9.3.1.3**" property="**$3**" />
<varbind name="**.1.3.6.1.4.1.2272.1.100.9.3.1.18**" property="**$4**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.17**" name="**rcnSmltIstLinkUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**337**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_SplitLinkStatus**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Split MLT link status up**" />
<eventprop name="**description**" value="**Split MLT link status up**" />
<eventprop name="**specificProblem**" value="**Split MLT link status up**" />
</PROPERTIES>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.18**" name="**rcnSmltIstLinkDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />

<eventprop name="**logNumber**" value="**338**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_SplitLinkStatus**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Split MLT Link Status Down**" />
<eventprop name="**description**" value="**Split MLT Link Status Down**" />
<eventprop name="**specificProblem**" value="**Split MLT Link Status Down**" />
</PROPERTIES>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.19**" name="**rcnSmltLinkUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**339**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_rcnSmltLinkStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcMltSmltId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Split SMLT link up**" />
<eventprop name="**description**" value="**Split SMLT link up: rcMltSmltId = $1**" />
<eventprop name="**specificProblem**" value="**Split SMLT Link status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.17.10.1.13**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.19**" name="**rcSmltLinkUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**339**" />

<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_rcSmltLinkStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcMltSmltId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Split SMLT link up**" />
<eventprop name="**description**" value="**Split SMLT link up: rcMltSmltId = $1**" />
<eventprop name="**specificProblem**" value="**Split SMLT Link status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.17.10.1.13**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.20**" name="**rcnSmltLinkDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**340**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_rcnSmltLinkStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcMltSmltId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Split SMLT Link down**" />
<eventprop name="**description**" value="**Split SMLT link down: rcMltSmltId = $1**" />
<eventprop name="**specificProblem**" value="**Split SMLT link status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.17.10.1.13**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.20**" name="**rcSmltLinkDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />

<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**340**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_rcSmltLinkStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcMltSmltId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Split SMLT link down**" />
<eventprop name="**description**" value="**Split SMLT link down: rcMltSmltId = $1**" />
<eventprop name="**specificProblem**" value="**Split SMLT Link status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.17.10.1.13**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.22**" name="**rcnPasswordChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**341**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**security**" />
<eventprop name="**entity**" value="**$ip_CLIPasswordChanged**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**CLI password changed**" />
<eventprop name="**description**" value="**CLI password changed (PasswordChange = $1 PassChangeResult = $2)**" />
<eventprop name="**specificProblem**" value="**CLI password has been changed**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.19.17**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.19.18**" property="**$2**" />
</VARBINDS>

```
</TRAP>
- <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.25" name="rcnPcmciaCardRemoved">
- <PROPERTIES>
<eventprop name="severity" value="1" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="342" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_PCMCIARemoved" />
<eventprop name="componentID" value="PP8600=$ip" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="PCMCIA card is being removed." />
<eventprop name="description" value="PCMCIA card is being removed." />
<eventprop name="specificProblem" value="PCMCIA card removed." />
</PROPERTIES>
</TRAP>
- <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.26" name="rcnSmartCpldTimerFired">
- <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="343" />
<eventprop name="eventType" value="TBL" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_cpldTimerFired_$1" />
<eventprop name="componentID" value="PP8600=$ip; CardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="cpld timer fired" />
<eventprop name="description" value="cpld timer fired: CardIndex = $1" />
<eventprop name="specificProblem" value="cpld timer fired" />
</PROPERTIES>
- <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.100.6.1.1" property="$1" />
</VARBINDS>
</TRAP>
```

- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.27**" name="**rcnCardCpldNotUpDate**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**344**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_cpldNotUpDate_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; CardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**cpld is not up to date**" />
<eventprop name="**description**" value="**cpld is not up to date: CardIndex = $1**" />
<eventprop name="**specificProblem**" value="**cpld not up to date**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.1**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.28**" name="**rcnIgapLogFileFull**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**345**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**processingError**" />
<eventprop name="**entity**" value="**$ip_IgapLogFileFull**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Igap Log file full**" />
<eventprop name="**description**" value="**Igap accounting time-out Log File reach the maximum.**" />
<eventprop name="**specificProblem**" value="**Igap Log file full**" />
</PROPERTIES>
</TRAP>

<TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.29**" name="**rcnCpLimitShutDown**">
<PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**346**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_CPLimitShutDown_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; PortIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**cp limit for the port is shutting down**" />
<eventprop name="**description**" value="**Cp limit for port is shutting down: PortIndex= $1(AdminStatus = $2 OperStatus = $3 CpLimitShutDown = $4)**" />
<eventprop name="**specificProblem**" value="**cp limit for the port is shutting down**" />
</PROPERTIES>
<VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.2.2.1.7**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.2.2.1.8**" property="**$3**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.50**" property="**$4**" />
</VARBINDS>
</TRAP>
<TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.30**" name="**rcnSshServerEnabled**">
<PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**347**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_SshServerStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SshGlobalPort=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**SSH server is enabled**" />
<eventprop name="**description**" value="**SSH server is enabled: SshGlobalPort = $1**" />

<eventprop name="**specificProblem**" value="**SSH server enabled**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.34.1.2**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.31**" name="**rcnSshServerDisabled**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**348**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_SshServerStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SshGlobalPort=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**SSH server is disabled**" />
<eventprop name="**description**" value="**SSH server is disabled: SshGlobalPort = $1**" />
<eventprop name="**specificProblem**" value="**SSH server disabled**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.34.1.2**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.32**" name="**rcnSshSessionLogin**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**349**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_SshSessionStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SshGlobalHostIpAddr=$1**" />
<eventprop name="**alarmClear**" value="**3**" />

<eventprop name="**probableCause**" value="**SSH Session login**" />
<eventprop name="**description**" value="**SSH session login occured: SshGlobalHostIpAddr = $1**" />
<eventprop name="**specificProblem**" value="**SSH Session login**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.34.1.12**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.33**" name="**rcnSshSessionLogout**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**350**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_SshSessionStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SshGlobalHostIpAddr=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**SSH session logout**" />
<eventprop name="**description**" value="**SSH session logout occured: SshGlobalHostIpAddr = $1**" />
<eventprop name="**specificProblem**" value="**SSH session logout**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.34.1.12**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.34**" name="**rcnSshUnauthorizedAccess**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**351**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />

<eventprop name="**category**" value="**security**" />
<eventprop name="**entity**" value="**$ip_SshUnauthorizedAccess_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; SshGlobalHostIpAddr=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Unauthorized access**" />
<eventprop name="**description**" value="**Unauthorized access occured: SshGlobalHostIpAddr = $1**" />
<eventprop name="**specificProblem**" value="**Unauthorized access**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.34.1.12**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.35**" name="**rcnHaCpuState**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**352**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_HaCpuState_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; CardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**State of the HA-CPU**" />
<eventprop name="**description**" value="**State of the HA-CPU: CardIndex = $1 (HaCpuState = $2)**" />
<eventprop name="**specificProblem**" value="**State of the HA-CPU**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.32.1**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.36**" name="**rcnInsufficientMemory**">
- <PROPERTIES>

<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**353**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**environmental**" />
<eventprop name="**entity**" value="**$ip_InsufficientMemory_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; CardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Insufficient memory on CPU blade for proper operation**" />
<eventprop name="**description**" value="**Insufficient memory: CardIndex = $1**" />
<eventprop name="**specificProblem**" value="**Insufficient memory on CPU**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.1**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.37**" name="**rcnSaveConfigAction**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**354**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**processingError**" />
<eventprop name="**entity**" value="**$ip_SaveConfig**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Switch run time or boot configuration is saved**" />
<eventprop name="**description**" value="**Switch configuration saved: SysAction = $1**" />
<eventprop name="**specificProblem**" value="**Switch configuration saved**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.1.8**" property="**$1**" />

</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.38**" name="**rcnLoopDetectOnPort**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**355**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_LoopOnPort_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; PortIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Loop detected on port. The vlan on that port will be disabled**" />
<eventprop name="**description**" value="**Loop detected on port: PortIndex = $1 (rcVlanId = $2)**" />
<eventprop name="**specificProblem**" value="**Loop detected on port.**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.3.2.1.1**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.46.1.3.0.3.0**" name="**vrrpTrapStateTransition**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**356**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_TrapStateTransition_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ifIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**State transition has occurred on vrrp interface**" />

<eventprop name="**description**" value="**State Transition: ifIndex = $1 (TransitionType = $2 TransitionCause = $3 Port = $p Slot = $s)**" />
<eventprop name="**specificProblem**" value="**Trap state transition**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.2.2.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.46.1.1.14**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.46.1.1.15**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.23**" name="**rcnEmError**">
- <PROPERTIES>
<eventprop name="**severity**" value="**4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**357**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_EmError_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; CardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Em error detected**" />
<eventprop name="**description**" value="**Em error: CardIndex = $1 (Em Error = $2)**" />
<eventprop name="**specificProblem**" value="**Em error detected**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.100.6.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.23**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.14.16.2.1**" name="**ospfVirtIfStateChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**$4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**358**" />
<eventprop name="**eventType**" value="**TBL**" />

<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**environmental**" />
<eventprop name="**entity**" value="**$ip_IfStateChange_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ospfRouterId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**OSPF virtual interface state change**" />
<eventprop name="**description**" value="**OSPF virtual interface state change: ospfRouterId = $1 (AreaId = $2 Neighbor = $3 State = $4)**" />
<eventprop name="**specificProblem**" value="**OSPF virtual interface state change**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.14.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.14.9.1.1**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.14.9.1.2**" property="**$3**" />
<varbind name="**.1.3.6.1.2.1.14.9.1.7**" property="**$4**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.14.16.2.2**" name="**ospfNbrStateChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**$4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**359**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_NbrStateChange_$1_$3**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ospfRouterId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Non-virtual neighbor state change**" />
<eventprop name="**description**" value="**Non-virtual neighbor state change: RouterId = $1 (NbrIpAddr = $2 NbrRouter = $3 State = $4)**" />
<eventprop name="**specificProblem**" value="**Non-virtual OSPF neighbor state change**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.14.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.14.10.1.1**" property="**$2**" />

<varbind name="**.1.3.6.1.2.1.14.10.1.3**" property="**$3**" />
<varbind name="**.1.3.6.1.2.1.14.10.1.6**" property="**$4**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.14.16.2.3**" name="**ospfVirtNbrStateChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**$4**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**360**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**environmental**" />
<eventprop name="**entity**" value="**$ip_VirtNbrStateChange_$1_$3**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ospfRouterId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Virtual OSPF neighbor state change**" />
<eventprop name="**description**" value="**Virtual neighbor state change: RouterId = $1 (NbrArea = $2 NbrRouter = $3 State = $4)**" />
<eventprop name="**specificProblem**" value="**Virtual OSPF neighbor state change**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.14.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.14.11.1.1**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.14.11.1.2**" property="**$3**" />
<varbind name="**.1.3.6.1.2.1.14.11.1.5**" property="**$4**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.14.16.2.4**" name="**ospfIfConfigError**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**361**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_IfConfigError**" />

<eventprop name="**componentID**" value="**PP8600=$ip; ospfRouterId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Configuration error**" />
<eventprop name="**description**" value="**IfConfig Error: ospfRouterId = $1 (IpAddress = $2)**" />
<eventprop name="**specificProblem**" value="**configuration error**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.14.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.14.7.1.1**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.14.16.2.5**" name="**ospfVirtIfConfigError**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**362**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_VirtIfConfigError_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ospfRouterId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Virtual interface configuration error**" />
<eventprop name="**description**" value="**VirtIfConfigError: ospfRouterId = $1 (AreaId = $2 Neighbor = $3 ErrorType =$4)**" />
<eventprop name="**specificProblem**" value="**Virtual interface configuration error**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.14.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.14.9.1.1**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.14.9.1.2**" property="**$3**" />
<varbind name="**.1.3.6.1.2.1.14.16.1.2**" property="**$4**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.14.16.2.6**" name="**ospfIfAuthFailure**">

- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**363**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**security**" />
<eventprop name="**entity**" value="**$ip_IfAuthFailure_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ospfRouterId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**ospf If authentication failure**" />
<eventprop name="**description**" value="**ospf If authentication failure: ospfRouterId = $1 (ConfigErrorType =$2)**" />
<eventprop name="**specificProblem**" value="**ospf If authentication failure**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.14.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.14.16.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.14.16.2.7**" name="**ospfVirtIfAuthFailure**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**364**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**security**" />
<eventprop name="**entity**" value="**$ip_VirtIfAuthFailure_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ospfRouterId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**ospf virtual interface authentication failure**" />
<eventprop name="**description**" value="**ospfVirtIfAuthFailure: ospfRouterId = $1 (AreaId = $2 Neighbor = $3 ErrorType =$4)**" />
<eventprop name="**specificProblem**" value="" />
</PROPERTIES>

- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.14.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.14.9.1.1**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.14.9.1.2**" property="**$3**" />
<varbind name="**.1.3.6.1.2.1.14.16.1.2**" property="**$4**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.14.16.2.16**" name="**ospfIfStateChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**$3**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**365**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_ifStateChange_$1_$2**" />
<eventprop name="**componentID**" value="**PP8600=$ip; ospfRouterId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Non-virtual OSPF interface state change**" />
<eventprop name="**description**" value="**Non-virtual OSPF interface state change: ospfRouterId = $1 (IpAddress = $2 State =$3)**" />
<eventprop name="**specificProblem**" value="**Non-virtual OSPF interface state change**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.14.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.14.7.1.1**" property="**$2**" />
<varbind name="**.1.3.6.1.2.1.14.7.1.12**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.1**" name="**rcnCardDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**366**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />

<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcnCardStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcCardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**RC Card status down**" />
<eventprop name="**description**" value="**RC card status down: CardIndex = $1 (AdminStatus = $2 OperStatus = $3)**" />
<eventprop name="**specificProblem**" value="**RC Card status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.5**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.6**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.1**" name="**rcCardDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**2**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**366**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_rcCardStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcCardIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**RC Card Status down.**" />
<eventprop name="**description**" value="**RC card status down: CardIndex = $1 (AdminStatus = $2 OperStatus = $3)**" />
<eventprop name="**specificProblem**" value="**RC Card Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.5**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.6**" property="**$3**" />
</VARBINDS>

```
</TRAP>
- <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.2" name="rcnCardUp">
- <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="367" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcnCardStatus_$1" />
<eventprop name="componentID" value="PP8600=$ip; rcCardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="RC card status up" />
<eventprop name="description" value="RC card status up: CardIndex = $1 (AdminStatus = $2 OperStatus = $3)" />
<eventprop name="specificProblem" value="RC Card Status" />
</PROPERTIES>
- <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.1" property="$1" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.5" property="$2" />
<varbind name=".1.3.6.1.4.1.2272.1.4.9.1.1.6" property="$3" />
</VARBINDS>
</TRAP>
- <TRAP oid=".1.3.6.1.4.1.2272.1.21.2" name="rcCardUp">
- <PROPERTIES>
<eventprop name="severity" value="5" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="367" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="equipment" />
<eventprop name="entity" value="$ip_rcCardStatus_$1" />
<eventprop name="componentID" value="PP8600=$ip; rcCardIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="RC card status up" />
<eventprop name="description" value="RC card status up: CardIndex = $1 (AdminStatus
```

= $2 OperStatus = $3)" />
<eventprop name="**specificProblem**" value="**RC Card Status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.5**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.4.9.1.1.6**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.39**" name="**rcnbgpEstablished**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**368**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_bgpEstablished_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; PeerIpAddress=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**BGP FSM entered the ESTABLISHED state**" />
<eventprop name="**description**" value="**BGP FSM entered ESTABLISHED state: PeerIpAddress = $1 (PeerLastError = $2 PeerState = $3)**" />
<eventprop name="**specificProblem**" value="**BGP FSM entered the ESTABLISHED state**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.8.101.9.1.2**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.101.9.1.26**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.101.9.1.25**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.40**" name="**rcnbgpBackwardTransition**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />

<eventprop name="**logNumber**" value="**369**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_bgpBackwardTransition_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcIpBgpPeerIpAddress=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**BGP FSM backward transition**" />
<eventprop name="**description**" value="**BGP FSM backward transition: PeerIpAddress = $1 (PeerLastError = $2 PeerState = $3)**" />
<eventprop name="**specificProblem**" value="**BGP FSM backward transition**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.8.101.9.1.2**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.101.9.1.26**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.101.9.1.25**" property="**$3**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.41**" name="**rcnAggLinkUp**">
- <PROPERTIES>
<eventprop name="**severity**" value="**5**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**370**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_AggLinkStatus_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcMltId=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Aggregator up**" />
<eventprop name="**description**" value="**Aggregator up: rcMltId = $1**" />
<eventprop name="**specificProblem**" value="**Aggregator status**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.17.10.1.1**" property="**$1**" />
</VARBINDS>

```
</TRAP>
- <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.42" name="rcnAggLinkDown">
- <PROPERTIES>
<eventprop name="severity" value="2" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="371" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_AggLinkStatus_$1" />
<eventprop name="componentID" value="PP8600=$ip; rcMltId=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="Aggregator Down" />
<eventprop name="description" value="Aggregator Down: rcMltId = $1" />
<eventprop name="specificProblem" value="Aggregator status" />
</PROPERTIES>
- <VARBINDS>
<varbind name=".1.3.6.1.4.1.2272.1.17.10.1.1" property="$1" />
</VARBINDS>
</TRAP>
- <TRAP oid=".1.3.6.1.4.1.2272.1.21.0.43" name="rcnIgmpNewGroupMember">
- <PROPERTIES>
<eventprop name="severity" value="6" />
<eventprop name="logName" value="PP" />
<eventprop name="logNumber" value="372" />
<eventprop name="eventType" value="INFO" />
<eventprop name="eventLabel" value="PP Fault" />
<eventprop name="category" value="communications" />
<eventprop name="entity" value="$ip_GroupMember_$1" />
<eventprop name="componentID" value="PP8600=$ip; rcIgmpGroupIfIndex=$1" />
<eventprop name="alarmClear" value="3" />
<eventprop name="probableCause" value="New Group member in interface" />
<eventprop name="description" value="New Group member in interface:
rcIgmpGroupIfIndex = $1 (GroupIpAddress = $2 Port = $3 Members $4)" />
<eventprop name="specificProblem" value="New Group member in interface" />
</PROPERTIES>
```

- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.8.6.1.5**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.6.1.1**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.6.1.3**" property="**$3**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.6.1.2**" property="**$4**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.44**" name="**rcnIgmpLossGroupMember**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**373**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_GroupMember_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; rcIgmpGroupIfIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Group member lost on interface**" />
<eventprop name="**description**" value="**Group member lost on interface: rcIgmpGroupIfIndex = $1 (GroupIpAddress = $2 Port = $3 Members $4)**" />
<eventprop name="**specificProblem**" value="**Group member lost on interface**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.8.6.1.5**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.6.1.1**" property="**$2**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.6.1.3**" property="**$3**" />
<varbind name="**.1.3.6.1.4.1.2272.1.8.6.1.2**" property="**$4**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.45**" name="**rcnIgmpNewQuerier**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**374**" />
<eventprop name="**eventType**" value="**INFO**" />

<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_Querier_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; igmpInterfaceIfIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**New Querier in interface**" />
<eventprop name="**description**" value="**New Querier in interface: igmpInterfaceIfIndex = $1 (igmpInterfaceQuerier = $2)**" />
<eventprop name="**specificProblem**" value="**New Querier in interface**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.3.59.1.1.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.3.59.1.1.1.1.5**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.46**" name="**rcnIgmpQuerierChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**375**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_QuerierChange_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; igmpInterfaceIfIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Querier changed**" />
<eventprop name="**description**" value="**Querier changed: igmpInterfaceIfIndex = $1 (NewQuerier = $2 igmpInterfaceQuerier = $3)**" />
<eventprop name="**specificProblem**" value="**Querier changed**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.3.59.1.1.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.30.1.1.25**" property="**$2**" />
<varbind name="**.1.3.6.1.3.59.1.1.1.1.5**" property="**$3**" />
</VARBINDS>

</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.47**" name="**rcnDvmrpIfStateChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**376**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_DvmrpStateChange_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; dvmrpInterfaceIfIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**DVMRP interface state change**" />
<eventprop name="**description**" value="**DVMRP interface state change: dvmrpInterfaceIfIndex = $1 (OperState = $2)**" />
<eventprop name="**specificProblem**" value="**DVMRP interface state change**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.3.62.1.1.3.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.3.62.1.1.3.1.3**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.48**" name="**rcnDvmrpNewNbrChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**377**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_NbrChange_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; dvmrpNeighborIfIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**New neighbor is up on DVMRP interface**" />
<eventprop name="**description**" value="**New neighbor is up on DVMRP interface: dvmrpNeighborIfIndex = $1 (NeighborAddress = $2)**" />

<eventprop name="**specificProblem**" value="**New neighbor is up on DVMRP interface**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.3.62.1.1.4.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.3.62.1.1.4.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.49**" name="**rcnDvmrpNbrLossChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**378**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_NbrChange_$1**" />
<eventprop name="**componentID**" value="**PP8600=$ip; dvmrpNeighborIfIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Neighbor gone down on DVMRP interface**" />
<eventprop name="**description**" value="**Neighbor gone down on DVMRP interface: dvmrpNeighborIfIndex = $1 (NeighborAddress = $2)**" />
<eventprop name="**specificProblem**" value="**Neighbor gone down on DVMRP interface**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.3.62.1.1.4.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.3.62.1.1.4.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.59**" name="**rcnFdbProtectViolation**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**379**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />

<eventprop name="**entity**" value="**$ip_FdbProtect_$1_$2**" />
<eventprop name="**componentID**" value="**PP8600=$ip; PortIndex=$1**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**fdb-entries limit violation**" />
<eventprop name="**description**" value="**fdb-entries limit violation: PortIndex = $1 (VlanId = $2)**" />
<eventprop name="**specificProblem**" value="**fdb-entries limit violation**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.3.2.1.1**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.60**" name="**rcnLogMsgControl**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**380**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_Log**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Log Message control trap**" />
<eventprop name="**description**" value="**rcnLogMsgControl: SysMsgLogFrequency = $1 (SysMsgLogText = $2)**" />
<eventprop name="**specificProblem**" value="**Log Message control trap**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.1.66**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.1.67**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.61**" name="**rcnSaveConfigFile**">
- <PROPERTIES>

<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**381**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**equipment**" />
<eventprop name="**entity**" value="**$ip_SaveConfig**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Run time / boot config saved on switch**" />
<eventprop name="**description**" value="**Config saved on switch: SysAction = $1 (SysConfigFileName = $2)**" />
<eventprop name="**specificProblem**" value="**Run time / boot config saved on switch**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.4.1.2272.1.1.8**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.1.34**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.62**" name="**rcnDNSRequestResponse**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**382**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_DNSResponse**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Request/Response from DNS server**" />
<eventprop name="**description**" value="**Request sent to or response got from DNS server: DnsServerListIpAddr = $1 (DnsRequestType = $2)**" />
<eventprop name="**specificProblem**" value="**Request/Response from DNS server**" />
</PROPERTIES>
- <VARBINDS>

<varbind name="**.1.3.6.1.4.1.2272.1.1.71**" property="**$1**" />
<varbind name="**.1.3.6.1.4.1.2272.1.1.72**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.80.0.1.0**" name="**pingProbeFailed**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**383**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_ProbeFailed**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Probe failure is detected**" />
<eventprop name="**description**" value="**Probe failure is detected: (ping TargetAddress = $1)**" />
<eventprop name="**specificProblem**" value="**Probe failure is detected**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.80.1.2.1.4**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.80.0.2.0**" name="**pingTestFailed**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**384**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_pingTestFail**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Ping test failed**" />

<eventprop name="**description**" value="**Ping test failed: (ping TargetAddress = $1)**" />
<eventprop name="**specificProblem**" value="**Ping test failed**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.80.1.2.1.4**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.80.0.3.0**" name="**pingTestCompleted**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**385**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_pingTestComp**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Ping test completed**" />
<eventprop name="**description**" value="**Ping test completed: (ping TargetAddress = $1)**" />
<eventprop name="**specificProblem**" value="**Ping test completed.**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.80.1.2.1.4**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.81.0.1.0**" name="**traceRoutePathChange**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**386**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_traceRouteChange**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />

<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**The path to a target has changed**" />
<eventprop name="**description**" value="**The path to a target has changed: (TargetAddress = $1)**" />
<eventprop name="**specificProblem**" value="**The path to a target has changed**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.81.1.2.1.4**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.81.0.2.0**" name="**traceRouteTestFailed**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**387**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_RouteTestFail**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Could not determine the path to a target**" />
<eventprop name="**description**" value="**Could not determine the path to a target: (TargetAddress = $1)**" />
<eventprop name="**specificProblem**" value="**Could not determine the path to a target**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.81.1.2.1.4**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.2.1.81.0.3.0**" name="**traceRouteTestCompleted**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**388**" />
<eventprop name="**eventType**" value="**INFO**" />

<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_RouteTestComplete**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**The path to a target has just been determined.**" />
<eventprop name="**description**" value="**The path to a target has just been determined: (TargetAddress = $1)**" />
<eventprop name="**specificProblem**" value="**The path to a target has just been determined.**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.81.1.2.1.4**" property="**$1**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.562.42.5.1.3.2.2**" name="**UDPEapSessionEndTrap**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**389**" />
<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_UDPEapSessionEnd**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Session end trap**" />
<eventprop name="**description**" value="**UDPEapSession end trap**" />
<eventprop name="**specificProblem**" value="**Session end trap**" />
</PROPERTIES>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.562.42.5.1.3.2.1**" name="**UDPEapSessionStartTrap**">
- <PROPERTIES>
<eventprop name="**severity**" value="**6**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**390**" />

<eventprop name="**eventType**" value="**INFO**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**other**" />
<eventprop name="**entity**" value="**$ip_UDPEapSessionSart**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**Session start trap**" />
<eventprop name="**description**" value="**UDPEapSession start trap**" />
<eventprop name="**specificProblem**" value="**Session start trap**" />
</PROPERTIES>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.63**" name="**rcnDuplicateIpAddress**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />
<eventprop name="**logName**" value="**PP**" />
<eventprop name="**logNumber**" value="**391**" />
<eventprop name="**eventType**" value="**TBL**" />
<eventprop name="**eventLabel**" value="**PP Fault**" />
<eventprop name="**category**" value="**communications**" />
<eventprop name="**entity**" value="**$ip_DuplicateIp**" />
<eventprop name="**componentID**" value="**PP8600=$ip**" />
<eventprop name="**alarmClear**" value="**3**" />
<eventprop name="**probableCause**" value="**More than one host with the same IP address have been detected on a subnet.**" />
<eventprop name="**description**" value="**Duplicate IP address detected on subnet: NetAddress=$1 (PhysicalAddress=$2)**" />
<eventprop name="**specificProblem**" value="**Duplicate IP address detected on the subnet.**" />
</PROPERTIES>
- <VARBINDS>
<varbind name="**.1.3.6.1.2.1.4.22.1.3**" property="**$1**" />
<varbind name="**.1.3.6.1.2.1.4.22.1.2**" property="**$2**" />
</VARBINDS>
</TRAP>
- <TRAP oid="**.1.3.6.1.4.1.2272.1.21.0.64**" name="**rcnLoopDetectPortDown**">
- <PROPERTIES>
<eventprop name="**severity**" value="**1**" />

<eventprop name="**logName**" value="**PP**" />

<eventprop name="**logNumber**" value="**392**" />

<eventprop name="**eventType**" value="**TBL**" />

<eventprop name="**eventLabel**" value="**PP Fault**" />

<eventprop name="**category**" value="**communications**" />

<eventprop name="**entity**" value="**$ip_LoopDetect_$1**" />

<eventprop name="**componentID**" value="**PP8600=$ip; portIndex=$1**" />

<eventprop name="**alarmClear**" value="**3**" />

<eventprop name="**probableCause**" value="**A network configuration error is creating a loop between ports in a vlan**" />

<eventprop name="**description**" value="**Loop detected on port: PortIndex=$1 (AdminStatus=$2 OperStatus=$3)**" />

<eventprop name="**specificProblem**" value="**Loop detected on a port and port is going to shut down**" />

</PROPERTIES>

- <VARBINDS>

<varbind name="**.1.3.6.1.4.1.2272.1.4.10.1.1.1**" property="**$1**" />

<varbind name="**.1.3.6.1.2.1.2.2.1.7**" property="**$2**" />

<varbind name="**.1.3.6.1.2.1.2.2.1.8**" property="**$3**" />

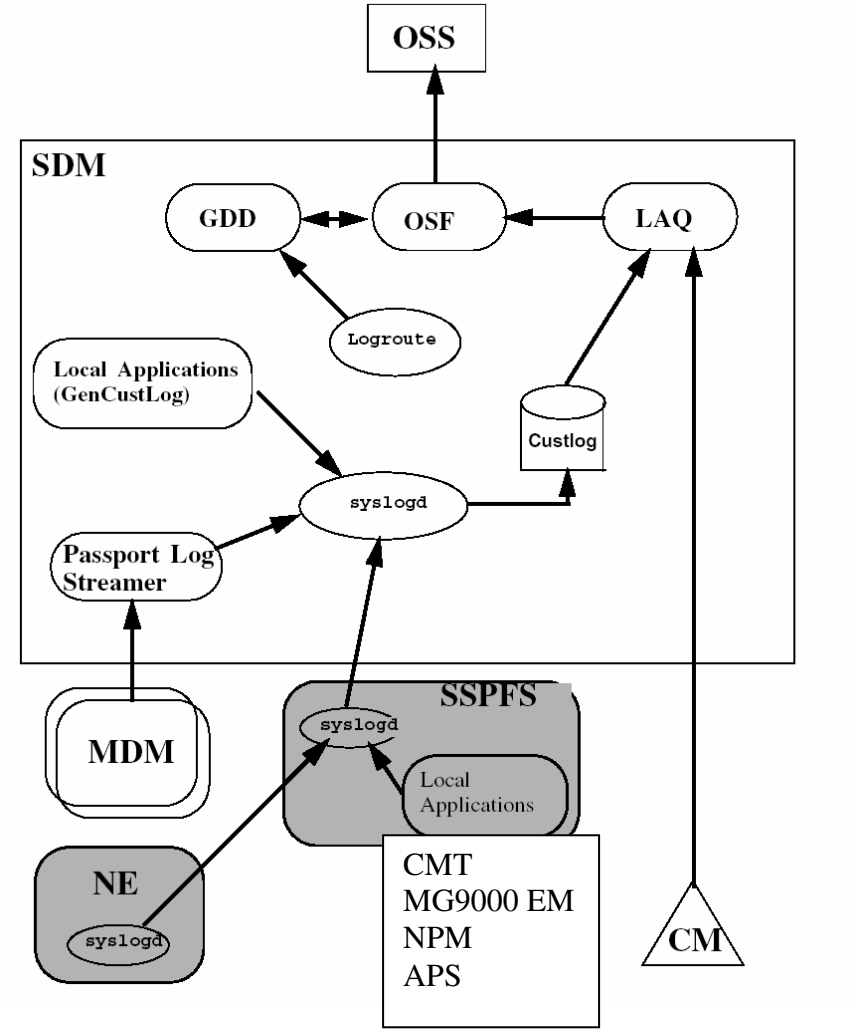
</VARBINDS>

</TRAP>

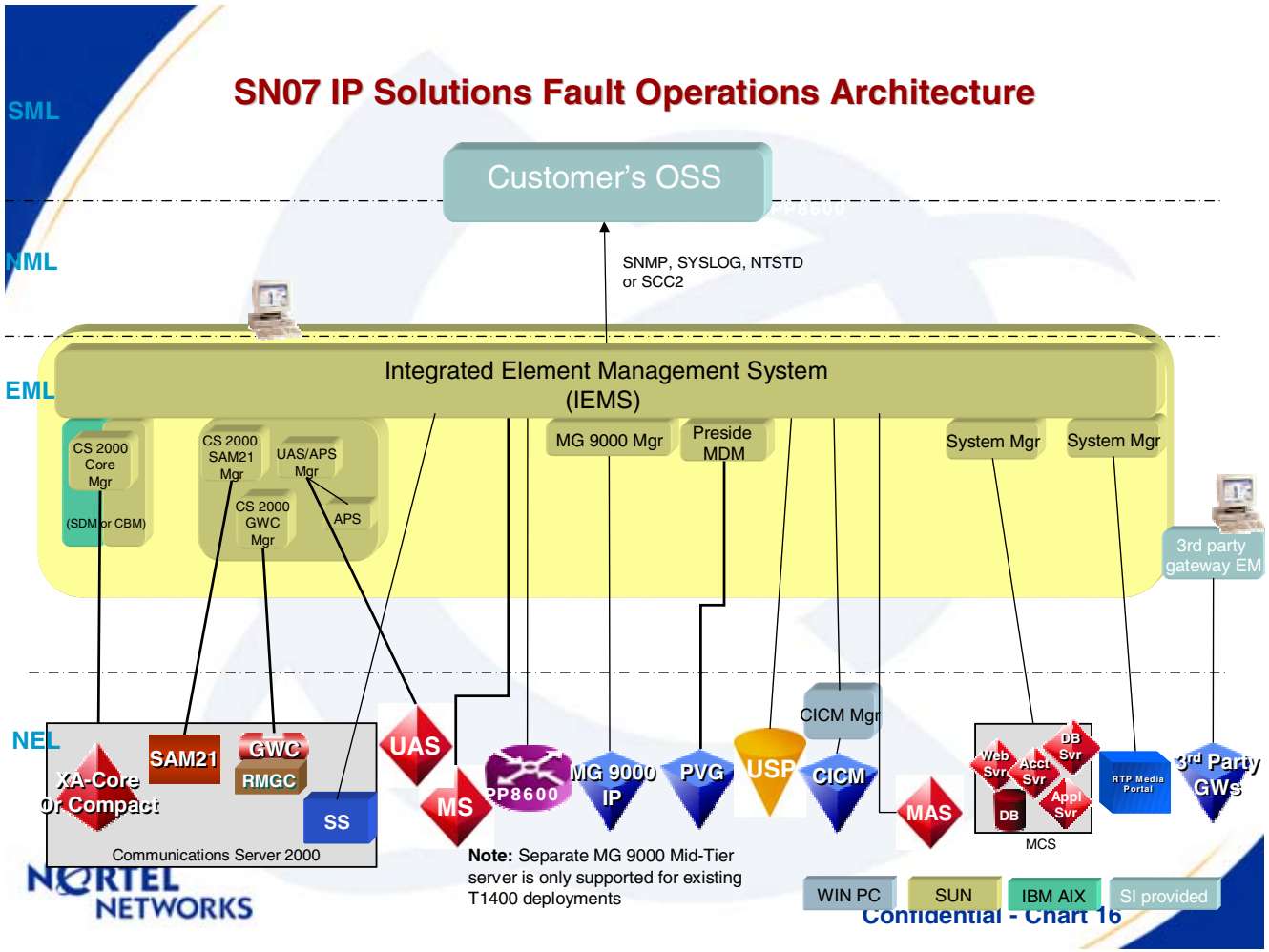
</TRAPS>

Appendix H: IEMS Fault Transparency with SDM/CBM

Prior to IEMS, which had its first Generally Available release in SN07, Succession supported sending faults and events from network elements via Syslog to the SDM/CBM. This feature, SYSLOG Consolidation for Succession, then allows the SDM/CBM to convert these logs to SCC2 or NTSTD to forward to the OSS. See the Figure below.



The fault feeds, delivered via IEMS supports SCC2 & NTSTD to the OSS, as did SDM/CBM. The implementation with IEMS used a more robust interfaces between the NE/EMS to IEMS and thus on a NE by NE basis there may be changes in the SCC2 log feed versus the SDM/CBM implementation. To understand fault diagram with IEMS see the diagram below.



This document is updated as new or changed information with respect to SDM/CBM and IEMS log transparency is learned. To understand the differences between the IEMS implementation and the SDM implementation see the tables below.

On NT STD and SCC2 Log Format Delimiters (SDM/CBM or IEMS to Fault OSS)

Table 1- **ASCII Character Legend**

ASCII Character Legend			
Character Name	**Hexidecimal**	**Decimal**	**Control Character**
Line Feed:	0A	10	^J
Carriage Return:	0D	13	^M
End of Message:	19	25	^Y
Null:	00	00	^@
Space:	20	32	space

Table 2 - **STD and SCC2 Log Delimiter Comparison between SDM/CBM and IEMS**

STD and SCC2 Log Delimiter Comparison Between SDM/CBM and IEMS				
Last Updated:	**Sept. 8, 2005**			
SDM/CBM Load:	**SN07/SN08: final compile & patch current; SN09: pre final compile 22.18.1.0**			
IEMS Load:	**SN07/SN08: final compile & patch current; SN09: IEMS_090_0531_1**			
Platform/Product:	**SDM/CBM**	**IEMS**	**SDM/CBM**	**IEMS**
Log Format:	**STD/STD_OLD**	**STD**	**SCC2/SCC2_OLD**	**SCC2**
Start of Log String:	0A 0D	0D (pre-SN09); 0A 0D (SN09+)	0A 0D	0A 0D
End of Line String:	0A 0D	0A 0D	0A 0D	0A 0D
End of Log String:	20 0A 0D 0A 0D 00	0A 0D 00 0A	0A 19 0A 0D	0A 0D 0A 19 0A

Comments on Table 2:

- The Log Delimiter String data applies to releases SN07 through to SN09 for the loads indicated as of the Last Updated date.
- **Last known change: IEMS NT STD Start of Log String has been changed from just 0D to 0A0D in SN09.**
- Previous change: IEMS SCC2 Start of Log String was changed to 0D to 0A0D to in SN09 and it was patched back to SN08 and SN07.
- Future changes: None planned. Through currently the End of Log String does differ between SDM/CBM and IEMS.
- The spaces between the hexadecimal numbers in Table 2 are there just to enhance readability. ie. 0D immediately follows 0A in the Start of Log String for SDM/CBM.
- In the SDM/CBM, the logroute interface allows customers to modify, if desired (but not recommended), the:
    - Start of Log String (default value: 0A 0D in hex)
    - End of Line String (default value: 0A 0D in hex) and the provisionable portions of the:

- End of Log String (default value: 20 0A 0D 0A 0D 00 where the first 0A 0D is the currently provisioned value in logroute for the End of Line string and the second 0A 0D sequence is the currently provisioned value logroute for the End of Log string.")

- The log delimiters of IEMS are not provisionable in any release as of the Last Updated date.
- IEMS was first generally available to customers (GA) in SN07. There was an SN06.2 beta where the delimiters for IEMS may have been different.
- SDM log stream delimiters have been the same since at least SN05. An OSS should consider the potential requirement of having to support multiple Nortel software releases concurrently. As well as SDM/CBM and IEMS concurrently.

Table 3 - **NE/EM Comparision**

<table>
<tr><th>NE/EM & SCC2 Transparency</th><th>Difference or Notes</th><th>OSS Impacting</th></tr>
<tr>
<td>CS2000, & Peripherals, IW-SPM, MG4000, SDM, CBM, cCS2000 –

Transparent with the following Notes</td>
<td>
Differences:

a) IEMS mandatory indent rule - IEMS has a mandatory indent rule where if it comes across a log from the CS2K/SDM that is not indented appropriately in its view, it will add 8 spaces to the beginning of the line. Very few logs (such as BOOT201 below) are believed to be affected by this issue. With well written OSS templates and the fix in place, the affected logs should not be adversely affected when it comes to OSS parsing.
<table>
<tr><th>SDM SCC2 Samples:</th><th>IEMS SCC2 Sample:</th></tr>
<tr>
<td><pre>* 08 BOOT201 INFO Bootp log report
Mac Address : 0001af0bc772
          MAC addr to node_id lookup failure : 11
          INM permisssion to boot failure   : 0
          Core IP address lookup failure   : 0
          SEND_UDP_MSG failure   : 0</pre></td>
<td><pre>* 08 BOOT201 INFO Bootp log report
        Mac Address : 0001af0bc772
          MAC addr to node_id lookup failure : 11
          INM permisssion to boot failure   : 0
          Core IP address lookup failure   : 0
          SEND_UDP_MSG failure   : 0</pre></td>
</tr>
</table>
Notes:
a) Certain logs generated by the CS2K such as OMAU, OMGA, and the protologs (SWER, TRAP, INIT and so on) have no log number, just blank spaces. This is how they look on the CS2K and SDM/CBM. In an SN07 office where the SDM is feeding CS2K logs to IEMS, IEMS adds 000 for a log number. Eg. SWER000. In SN08, a resolution was implemented in IEMS whereby the 000 log number was no longer added to these SDM/CBM logs and the 3 spaces are maintained as it is received. Resolved in SN08 via CR Q00980472.

b) When IEMS receives logs from managed components, it implements an 80 character per line rule for log bodies. If 80 characters is exceeded, an End of Line String is inserted at the 80th character and the remainder of the line is put onto the next line. In the case of logs from the SDM/CBM, where rows often exceed 80 characters, this wrap rule could result in visual or transparency differences between what the log looks like on SDM/CBM and IEMS. In some cases, trailing whitespace in a row could potentially be wrapped resulting in a blank line being created. In order to maintain transparency and avoid parsing issues with blank lines and so on, the 80 character wrap rule has been removed from the incoming feed to IEMS from SDM/CBM. Resolved in SN07 via patch IEM05O7D

c) Certain CS2K logs such as CARR and PM support an optional field called Equipment Identifier that shows up at the end
</td>
<td>a) No Impact</td>
</tr>
</table>

<table>
<tr><td></td><td>of the log header after the Event Label. The CS2K has a "newline" rule (which the SDM/CBM implements as well) where the Equipment Identifier is removed from the header line in that it has its own line immediately following the header. The SDM/CBM's Log Delivery Service at SN07 final compile in its implementation of the 65 character newline rule incorrectly took into consideration the 9 characters for the optional ECORE_FORMAT field. (Even when ECORE is set to OFF in the SDM/CBM log device in logroute). This results in the Equipment Identifer field being "newlined" when the CS2K normally would not. (A transparency difference between what the log looks like on the CS2K and on the SDM/CBM). The end result of all this is that templates parsing CARR and PM logs (and any other Equipment Identifier-supporting logs) may no longer be able to parse these logs properly prior to implementation of the patch for this CR. Resolved in SN07 via patches SDM_BASE.logs-20.82.7.10.tape, SDM_BASE.gdd-20.82.7.3.tape for SDM and NTLOGS208208-15.patch, NTGDD208208-03.patch for CBM.

d) SDM / CBM transparency issue. In the SN07 CBM product, some applications had started to communicate their failure events via an alarmd process. The resultant log looks different than the original (as seen on SDM). For failure events common to both SDM and CBM platforms, this created 2 versions of the log. 1 for SDM and 1 for CBM. Known logs affected were SDM327/SDM627. This second CBM version was undone in that . Resolved in SN07 CBM patch CR Q01001000-01</td><td></td></tr>
<tr><td>STORM
Partially Transparent</td><td>Differences:
a) Log name/numbers are retained but log formats are different. Believed to affect approx. 8 logs. See example below.

<table><tr><th>SDM SCC2 Samples:</th><th>IEMS SCC2 Sample:</th></tr><tr><td>* 59 STM 803 5090 THR Threshold exceeded
Status: Alarm raised. Number of zombie(s) is 1.
Minor alarm threshold value is 1.</td><td>* 40 STM 803 0088 FLT STM Fault
Location: 172.18.17.6
Notification Id: 56
State: Raised
Category: qualityOfService
Cause: thresholdCrossed
Time: Sep 07 09:40:17 2004
Component Id: STORMIA=storm0
Specific Problem:
Description: Status: Alarm raised. Number of zombie(s) is 1. Minor alarm threshold value is 1.</td></tr></table></td><td>a) No Impact if no existing OSS support for STM logs. Otherwise, the template would have to change.</td></tr>
</table>

NE/EM & SCC2 Transparency	Difference or Notes	OSS Impacting
GWC and GWC EM Partial Transparency	**Differences:** **a)** GWC3XX set logs. (Approx. 17 logs). The syntax of the Category and Cause fields in the log body are different (spaces and Upper case characters). **b)** GWC399 (the clear log for the GWC3XX set logs) is not transparent. IEMS version of the log has 2 extra lines. (mainly for human interpretation). Note: The Component Id structure difference in the example below is tracked by CR Q00976754 and resolved in SN07 patch ZOD41O7D. It is not an SDM / IEMS transparency issue.	**a)** No Impact. **b)** No Impact. A single OSS template should be able to handle both versions these GWC logs.

<table>
<tr><td></td><td>
<table>
<tr><th>SDM SCC2 Samples:</th><th>IEMS SCC2 Sample:</th></tr>
<tr><td>**16 GWC 301 5129 TBL GWC Fault
Location: GWC-1-UNIT-1
NotificationID: 1
State: Raise
Category: Quality of Service
Cause: Underlying resource unavailable
Time: Sep 01 13:16:11 2004
Component Id: GWC-1-UNIT-1
Specific Problem: Unit Out of Service: Unit is system disabled; Service
is not available
Description: Standby unit disabled.</td><td>**28 GWC 301 0036 TBL GWC Fault
Location: GWC-0-UNIT-1
NotificationID: 1
State: Raise
Category: qualityOfService
Cause: underlyingResourceUnavailable
Time: Aug 27 13:28:43 2004
Component Id: GWC=GWC-?~UNIT-?;Version=GN070CB;Unit=unit_1;Software=NODE MTC
Specific Problem: Unit Out of Service: Unit is system disabled; Service is not available
Description: Standby unit disabled.</td></tr>
<tr><td>16 GWC 399 5155 INFO GWC Fault
Location: GWC-1-UNIT-1
NotificationID: 1
State: Clear
Time: Sep 01 13:16:21 2004</td><td>30 GWC 399 0050 INFO GWC Fault
Location: GWC-0-UNIT-1
NotificationID: 1
State: Clear
Time: Aug 27 13:30:45 2004
Component Id: GWC=GWC-?~UNIT-?;Version=GN070CB;Unit=unit_1;Software=NODE MTC
Description: Standby unit disabled.</td></tr>
</table>
</td><td></td></tr>
<tr><td>MG9K ATM/IP & MG9000 EM
Partial Transparency</td><td>Differences:
a) For all MG9000 logs having a format which includes the Category and State fields (generally alarm logs - approx. 200 in SN07, and 40 more in SN08), you will find that the syntax of the field value between SDM and IEMS can be slightly different. This is due to the MG9K EM outputting syslog to SDM and Corba to IEMS.
Example for SDM:
State: cleared
Category: Equipment Alarm
Example for IEMS:
State: Cleared
Category: equipment

Notes:
a) In SN07, the MG9000 Element Manager in an IEMS implementation was duplicating alarm logs sent to IEMS by including them in the syslog feed in addition to the Corba feed to IEMS. Application of the MG9000 EM patch will de-activate sending alarm logs to syslog remove the duplication. Resolved in SN07 via patch IEM08O7D for IEMS and 9K EM patch ZOD50</td><td>a) No Impact</td></tr>
<tr><td>SAM21
Transparent</td><td>Differences:
a) Some SAM21 logs (worst case 19 SCU logs) indent the event label 1 character (space). When IEMS processes this, the leading space in the Event Label is removed. SDM maintains the leading space.</td><td>a) No Impact</td></tr>
</table>

NE/EM & SCC2	Difference or Notes	OSS Impacting

<table>
<tr><th>Transparency</th><th></th><th></th></tr>
<tr><td>Passport 8600
Not transparent</td><td>
Differences: (SN07)
a) The logs reporting Passport 8600 SNMP trap events are completely different between SDM/CBM and IEMS. In SN07, the SDM uses the PPES300-307 log name/number set and obtains the data for these logs from MDM. IEMS listens to SNMP traps directly from the Passport 8600 and implements the PP398 log for the sets and PP399 for the clears.
<table>
<tr><th>SN07 SDM SCC2 Samples:</th><th>SN07 IEMS SCC2 Sample:</th></tr>
<tr><td>**20 PPES300 1486 TBL
time: 2003 11 14 12 17 03
event: set
compId: PP8600 BATMAN IF 72
severity: major
faultCode: C0000002
alarmType: communications
commentData: Link down trap interface: 72</td><td>** PP398 SEP08 21:37:57 9992 TBL PP Fault
Location: 10.102.15.130
State: Raise
Specific Problem: Generic Link Status
Description: Link Down: ifIndex = 167
(AdminStatus = up OpeationStatus = down)</td></tr>
<tr><td>20 PPES307 1487 TBL
time: 2003 11 14 12 17 06
event: clear
compId: PP8600 BATMAN IF 72
severity: cleared
faultCode: C0000002
alarmType:
commentData: Explicited CLEAR Alarm generated by GMDR.</td><td>38 PP399 SEP08 21:38:00 9994 INFO PP Fault
Location: 10.102.15.130
State: Clear
Specific Problem: Generic Link Status
Description: Link Up: ifIndex = 167
(AdminStatus = up OpeationStatus = up)</td></tr>
<tr><td>20 PPES300 1488 TBL
time: 2003 11 14 12 17 06
event: clear
compId: PP8600 BATMAN IF 72
severity: cleared
faultCode: C0000002
alarmType: communications
commentData: Link up trap interface: 72</td><td></td></tr>
</table>
b) IEMS only supported a limited set of Passport 8600 traps in SN07. (The ones listed below). The unsupported Passport 8600 SNMP traps are treated by IEMS as unknown and reported northbound to the OSS as IEMS602 (Unknown Trap from Known Device).
<table>
<tr><th>Alarm Name</th><th>Trap OID (v2c)</th><th>Log</th></tr>
<tr><td>coldStart</td><td>1.3.6.1.6.3.1.1.5.1.0</td><td>PP399</td></tr>
<tr><td>coldStart</td><td>1.3.6.1.4.1.2272.0.99001</td><td>PP398</td></tr>
<tr><td>warmStart</td><td>1.3.6.1.6.3.1.1.5.2.0</td><td>PP399</td></tr>
</table>
</td><td>
SN07:
a) No impact – OSS coding support challenges may be present with extracting data from the Specific Problem and Description fields and being able to correlate the sets with the clears.
b) Impact Major - A customer is either other going to ignore all IEMS602s or mark all critical – either way, it is going to be problem in SN07.
c) Impact Major - There is insufficient information (only an IP address) to determine what is causing the fault and what needs to be corrected.

SN08:
a) No impact – The above SN07 issues are resolved in SN08 and as with any new logs in a release, new templates will have to be written to support them. With the current flexibility of the IEMS aging policy and that of an OSS, a working fault management system should be possible between the two of them.
</td></tr>
</table>

warmStart	1.3.6.1.4.1.2272.0.99002	PP398
linkDown	1.3.6.1.6.3.1.1.5.3.0	PP398
linkUp	1.3.6.1.6.3.1.1.5.4.0	PP399
rcChasPowerSupplyDown	1.3.6.1.4.1.2272.1.21.6.0	PP398
rcChasPowerSupplyUp	1.3.6.1.4.1.2272.1.21.14.0	PP399
rcChasFanDown	1.3.6.1.4.1.2272.1.21.7.0	PP398
rcChasFanUp	1.3.6.1.4.1.2272.1.21.21.0	PP399
rc2kCardDown	1.3.6.1.4.1.2272.1.21.11.0	PP398
rc2kCardUp	1.3.6.1.4.1.2272.1.21.12.0	PP399
rcSmltLinkUp	1.3.6.1.4.1.2272.1.21.19.0	PP399
rcSmltLinkDown	1.3.6.1.4.1.2272.1.21.20.0	PP398

• Exception: PP368 and PP369 are the SN08 logs which have been patched back to SN07. (Only these 2 logs to date have been patched back).

```
59 IEMS602 7505 INFO
    Location: 10.102.15.131
    Event: .1.3.6.1.4.1.2272.1.21.8.0
    Varbind0: .1.3.6.1.2.1.1.3.0: 203 days, 23 hours, 11 minutes, 22 seconds
    .
    Varbind1: .1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.4.1.2272.1.21.8.0
    Varbind2: .1.3.6.1.4.1.2272.1.4.10.1.1.1.0: 267
```

c) IEMS Location Field has only an IP address.

Notes: (SN08)

a) SN08 feature A00007343 was created to help address the above issues in 8600 fault management via IEMS. With the feature, a new set of logs (PP310 -> PP392) was created to addresses log format/content issues [a) and c)] and PP398/399 is no longer used. Full SNMP trap support as of SN08 was implemented as well [b)] and hence no IEMS602 logs would be seen for unsupported 8600 SNMP traps. This feature does not result in transparency between SDM and IEMS but it does clean up the IEMS log situation. See the SN08 IEMS log samples below for Passport 8600. PP317 is cleared by PP318 when the Component ID matches. At the time of writing, two SN08 IEMS logs for Passport 8600 (PP368 and PP369) have been patched back to SN07.

IEMS PP317 SN08 SCC2 Sample:

Specific Problem: Generic Link Status
Description: Link Down: ifIndex = 72(AdminStatus = up OperationStatus = down)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.3.0
.1.3.6.1.2.1.1.3.0: 73 days, 5 hours, 35 minutes, 4 seconds.

IEMS PP318 SN08 SCC2 Sample:

01 PP 318 0120 INFO PP Fault
Location: PP8600A;10.102.15.130
State: Cleared
Category: communications
Cause: communication regained
Time: Feb 10 16:01:48 2005
Component ID: PP8600=10.102.15.130; ifIndex=72
Specific Problem: Generic Link Status
Description: Link Up: ifIndex = 72(AdminStatus = up OperationStatus = up)
.1.3.6.1.6.3.1.1.4.1.0: .1.3.6.1.6.3.1.1.5.4.0
.1.3.6.1.2.1.1.3.0: 73 days, 5 hours, 35 minutes, 6 seconds.

Differences: (SN08)

a) One noted difference between SN08 IEMS 8600 trap/log fault management and that of SDM/CBM via MDM is that MDM has implemented a per alarm aging mechanism where a trap is not part of a set/clear pair. (There are a lot of 8600 SNMP traps like this.) After a certain period of time, one of these autonomous logs (that has severity) will be cleared automaticly. IEMS as of SN08 does not have a per alarm aging mechanism. In order to prevent a situation in IEMS where these autonomous logs are being raised but never cleared, an 8600 device alarm clearing policy has been implemented by default in the SN08 load. If any 8600 alarm has been present in IEMS for 7 days, it will automaticly be cleared by this policy. The clear notification will be an IEMS608 log which will contain information required in order to clear the previous set log for the alarm. While clearing 8600 alarms related to hardware such as fan or link down after 7 days is undesirable it was felt better than having no clear for the multitude of 8600 autonomous traps. Note: An OSS does not have to take action on aging clears if it does not want to. Or it can take action on only a subset of them. The 8600 aging policy in IEMS can also be disabled or modified to be something other than 7 days.

<table>
<tr><th>NE/EM & SCC2 Transparency</th><th>Difference or Notes</th><th>OSS Impacting</th></tr>
<tr>
<td>MSS15000, MG15000, MDM
Partial Transparency</td>
<td>
Notes:
Between IEMS and SDM/CBM, MSS15000/MG15000/MDM log names are the same and appears to use the same mapping scheme. (Where the log prefix is determined by what the first 4 digits of the fault code is). Names are PPEM, MDM and CA. Log Body tags all the same.

Differences: (SN07 and SN08)
a) Log numbers are maintained except that it would appear IEMS doesn't use PPEM/CA/MDM307 for explicit clears and instead uses a 000 number. OSS templates for PPEM000/CA000/MDM000 should be identical to PPEM307/CA307/MDM307 (explicit clear varieties). Inappropriate use of the 000 log number for explicit clears from MDM was discontinued in SN08. Resolved in SN08 via CR Q00980484.
<table>
<tr><th>SN07 SDM/CBM Explicit Clear Sample:</th><th>SN07 IEMS Explicity Clear Sample:</th></tr>
<tr><td>08 PPEM307 9380 TBL
time: 2004 09 09 12 09 11
event: clear
compId: EM P15KE LP 12 SONET 1 STS 0
severity: cleared
faultCode: 70115261
alarmType:
commentData: Explicited CLEAR Alarm generated by GMDR.</td><td>46 PPEM000 8088 TBL
time: 2004 09 09 12 46 42
event: clear
compId: EM P15KE LP 12 SONET 1 STS 0
severity: cleared
faultcode: 70115261
alarmType: other
commentData: Explicited CLEAR Alarm generated by GMDR.</td></tr>
</table>
b) IEMS has changed the field values of alarmType in some cases so that it aligns with a standard list of X.733 alarm categories. Where there was no equivalent alarm type in X.733, IEMS uses "other". (See table below). When logs come out of SDM/CBM, the original alarmtype as provided by MDM is maintained.
<table>
<tr><th>SN07/08 SDM/CBM alarmtype SCC2 Sample:</th><th>SN07/SN08 IEMS alarmtype SCC2 Sample:</th></tr>
<tr><td>**13 PPEM305 7877 TBL
time: 2005 03 08 16 13 14
event: message
compId: EM P15KL NMIS $ FMIP $ SESSION 9
severity: major
faultCode: 70060006
alarmType: security
commentData: 9 contiguous FMIP login attempts failed,</td><td>**41 PPEM305 8756 TBL
time: 2005 03 08 14 40 41
event: message
compId: EM P15KL NMIS $ FMIP $ SESSION 9
severity: major
faultcode: 70060006
alarmType: other
commentData: 9 contiguous FMIP login attempts failed,</td></tr>
</table>
</td>
<td>
a) Minor impact - Log numbers of 000 are usually invalid. Customers who have written templates for CA/MDM/PPEM3XX would have to add an additional line for PPEM000. The template logic would read something like; if you get an alarm raised with a PPEM3xx look for a PPEM3xx or PPEM307 or PPEM000 with the same compID and faultCode.
b) No Impact
c) No Impact
d) Minor impact – Fault OSS log parsing code for these logs would have to be coded to accommodate the capitalization differences.
e) Minor impact – Only if fault OSS parses out the values of the alarmType field. In such a case, the log parsing code would need to accommodate “processing” or “processingError”. Having a 307 number instead of 302 should be no impact given the same format structure of all the logs.
</td>
</tr>
</table>

last failure from 10.102.4.4 to userid: DEBUG	last failure from 10.102.13.16 to userid: DEBUG

c) In SN07, when the alarmType value is qualityOfService, SDM reports the log number as 301 whereas IEMS reports it as 307. (Log format of 300-307 are all the same). In SN08, this is no longer the case. **Resolved in SN08 via unknown CR.**

SN07 SDM/CBM SCC2 Sample:	**SN07 IEMS SCC2 Sample:**
04 **PPEM301** 5272 TBL time: 2004 08 23 11 04 25 event: clear compId: EM P15KL COL DEBUG AG 1 severity: cleared faultCode: 70030001 alarmType: qualityOfService commentData: currentQueueSize fell back to 500f maximum. 48 records discarded since the Set alarm.	**36 **PPEM307** 3736 TBL time: 2004 09 23 10 36 17 event: set compId: EM P15KH COL DEBUG AG 0 severity: major faultcode: 70030001 alarmType: qualityOfService commentData: currentQueueSize exceeded 75% of maximum.
SN08 SDM/CBM SCC2 Sample:	**SN08 IEMS SCC2 Sample:**
12 **PPEM301 8786 TBL time: 2005 02 23 14 47 02 event: set compId: EM P15KE LP 2 ENG $ AALIST $ severity: major faultCode: 70030007 alarmType: qualityOfService commentData: current list size exceeded 750f maximum	**49 **PPEM301** 5863 TBL time: 2005 02 11 13 49 03 event: set compId: EM P15KL COL DEBUG AG 15 severity: major faultcode: 70030001 alarmType: qualityOfService commentData: currentQueueSize exceeded 75% of maximum.

d) In SN07 and SN08, IEMS had a tag of “faultcode” whereas in SDM, it was “faultCode”. **Resolved in SN09 via CR Q01176407.**

e) In SN07 and SN08, IEMS was mapping the alarmType value of “processing” to “other” whereas in SDM, it “processing”. In SN09, IEMS started mapping “processing” to “processingError” in order to comply with X.733 values. Also, the IEMS log number was improperly coming out as 307 instead of 302 like SDM. In SN09, IEMS started to properly report processing errors as 302 log numbers. **Each Implemented/Resolved in SN09 via CR Q01176412.**

Summary of Transparency Differences Between SDM & IEMS (in bold text) for c), d) & e):

SDM alarmTpe	SDM log number	IEMS alarmType	IEMS log number
communications	300	communications	300

	qualityOfService	301	qualityOfService	**307 (SN07)** / 301 (SN08)	
	processing	302	**other (SN07/08)/processingError (SN09)**	**307 (SN07/SN08)** / 302 (SN09)	
	equipment	303	equipment	303	
	environmental	304	environmental	304	
	security	305	**other (SN07/08)**	305	
	debug	600	(unknown)	(unknown)	
	operator	306	**other (SN07/08)**	306	
	unknown	307 (set log)	**other (SN07/08)**	307	
	(blank)	307 (explicit clear)	**other (SN07/08)**	**000 (SN07)** / 307 (SN08)	

<table>
<tr><th>NE/EM & SCC2 Transparency</th><th>Difference or Notes</th><th>OSS Impacting</th></tr>
<tr><td>CMT- SESM
Partial Transparency</td><td>
Differences:
a) CMT399 is not transparent. IEMS version of this log has 2 extra lines.
b) Partial transparency amongst all CMT3XX set logs (approx. 4 logs): Syntax of Category, and Cause fields are different. (See samples below).
c) In CMT302 failure scenarios, it appears that IEMS uses an inconsistent Location field value between the set and clear. In SDM, SNMP_NE_Poller is consistently used. Resolution involves making the IEMS clear have SNMP_NE_Poller. Resolved in SN08 via CR Q01078502 and CR Q01078502-02. Plans to patch back to SN07.
<table>
<tr><th>SDM SCC2 Samples:</th><th>IEMS SCC2 Sample:</th></tr>
<tr><td>**14 CMT 302 9000 TBL CMT Fault
Location: SNMP_NE_Poller
NotificationID: 1
State: Raise
Category: Communications
Cause: Communications subsystem failure
Time: Aug 31 13:34:14 2004
Component Id: SESM=SNMP Device Poller;Device=GWC-6-UNIT-1;DeviceID=0x00000063000000a10a660f43
Specific Problem: SNMP Timeout
Description: CMT Unable to communicate with managed device</td><td>**29 CMT 302 5875 TBL GWC Fault
Location: SNMP_NE_Poller
NotificationID: 4
State: Raise
Category: communications
Cause: communicationsSubsystemFailure
Time: Sep 27 13:29:37 2004
Component Id: SESM=SNMP Device Poller;Device=GWC-5-UNIT-0;DeviceID=0x00000063000000a10a660f3e
Specific Problem: SNMP Timeout
Description: CMT Unable to communicate with managed device</td></tr>
<tr><td>15 CMT 399 9946 INFO CMT Fault
Location: SNMP_NE_Poller
NotificationID: 1
State: Clear
Time: Aug 31 13:28:15 2004</td><td>38 CMT 399 6002 INFO GWC Fault
Location: GWC-5-UNIT-0
NotificationID: 4
State: Clear
Time: Sep 27 13:38:22 2004
Component Id: SESM=SNMP Device Poller;Device=GWC-5-UNIT-0;DeviceID=0x00000063000000a10a660f3e
Description: CMT Reestablished communications with managed device</td></tr>
</table>
</td><td>a) No Impact.
b) No Impact.
c) Impact Major – Customer may be unable to clear the alarm until the CR issue is resolved.</td></tr>
<tr><td>CMT-QCA
Partial Transparency</td><td>Differences:
a) IEMS implements an 80 character log body line length for all managed components except the logs from SDM/CBM. Some of the QCA logs as output to /var/log/customerlog on the CMT have a Description field value that exceeds 80 characters. IEMS puts the excess onto a new line whereas SDM/CBM does not when it receives it from syslog.</td><td>a) No Impact</td></tr>
</table>

	Notes: SN08 introduced feature A00008338 to address certain general log supportability concerns for the OSS. This corrective content feature will be patched back to SN07.	
CMT-NPM Transparent	**Differences:** **a)** Some NPM logs (11 logs worst case) indent the event label 1 character (space). When IEMS processes this, the leading space in the Event Label is removed. SDM/CBM maintains the leading space.	**a)** No Impact
CMT-IEMS (general northbound feed comparison with SDM)	**Differences:** **a)** For NT STD and SCC2 log formats, the characters contained within the "Start of Log" and "End of Log" string delimiters are different. See Table 1 at the beginning of this Appendix. **b)** When IEMS re-syncs its alarm list with devices that support re-sync, IEMS creates clear logs for when discrepancies are found. ie Alarms it thought were there but went away. These clear logs used the original log name/number for the alarm in the database and the content of the "re-sync clear" was not necessarily the same. Resolution of this CR has resulted in the creation of a new IEMS log for re-sync raises/clears. (IEMS607). SDM/CBM has no such re-sync capability. **Resolved in SN07 via IEM10O7D patch** **Notes:** SN07 CR Q01001051 tracked the fact that the "end of log string" for SDM differs depending on whether ECORE_FORMAT is on or off in the device. This is not an SDM/IEMS transparency but an SDM/SDM one. (ECORE_FORMAT is not supported in Succession.) This issue has been resolved through the SN07 SDM/CBM patches. The End of Log string is now the same whether ECORE format is ON or OFF. (ECORE format is not supported in Succession and should be turned off for the SDM/CBM log device for IEMS fault communication).	**a)** No Impact. **b)** No Impact. A new template would have to be created for the IEMS607 log as is the case for any new log.

<table>
<tr><th>NE/EM & SCC2 Transparency</th><th>Difference or Notes</th><th>OSS Impacting</th></tr>
<tr><td>CMT–UAS
Partial Transparency</td><td>
Differences:
a) Minor difference in the syntax of the Cause field values. Eg. "outOfMemory" in IEMS vs "Out of memory" in SDM as per the example below.
b) Minor difference in the syntax of the Category field values. Eg. "processingError" in IEMS vs "Processing Error" in SDM as per the example below.
c) UAS399 not transparent. (Similar in fashion to GWC399 and CMT399). UAS399 is the clear log for all UAS3xx and 8xx raises. The IEMS version has 2 extra rows of information in the clear. See example below.
<table>
<tr><th>SDM SCC2 Samples:</th><th>IEMS SCC2 Sample:</th></tr>
<tr><td>**19 UAS 353 1227 TBL UAS Fault
Location: msh10uas-a
NotificationID: 81924
State: Raise
Category: Processing Error
Cause: Out of memory
Time: May 22 11:19:13 2003
Component Id: UAS;UASUnit=msh10uas-a;Software=LocalResourceManager_0
Specific Problem: 81924
Description: [mem_usage_high_major] Memory usage high. (803554284552sed)</td><td>**10 UAS 353 9836 TBL UAS Fault
Location: cablabuas
NotificationID: 81924
State: Raise
Category: processingError
Cause: outOfMemory
Time: Aug 30 15:10:48 2004
Component Id: UAS;UASUnit=cablabuas;Software=LocalResourceManager_0
Specific Problem: 81924
Description: [mem_usage_high_major] Memory usage high. (91% used)"</td></tr>
<tr><td>19 UAS 399 1228 INFO UAS Fault
Location: msh10uas-a
NotificationID: 81924
State: Clear
Time: May 22 11:19:14 2003</td><td>53 UAS 399 0642 INFO UAS Fault
Location: UAS_RTPU_TST
NotificationID: 49154
State: Clear
Time: May 11 10:53:37 2004
Component Id:
Description:</td></tr>
</table>
</td><td>a) No Impact
b) No Impact
c) No Impact</td></tr>
<tr><td>CMT –APS</td><td>At this time there are no known methods for an APS set log to be transmitted northbound to the OSS.</td><td>No Impact</td></tr>
<tr><td>CICM, MCS5200, USP, USPc, RTP Portal, Session Server, MS20x0, SPC

Not supported via SDM</td><td>N/A</td><td>No Impact</td></tr>
</table>

Appendix I: MCS Alarms and Logs

1 Fault Management Overview

1.1 Introduction

This document shall be considered an "amendment" to the previous release's (MCS 4.0) Logs and Alarms Description document. In other words, the MCS 4.0 document will act as the "base" document with all adds/changes/deletes captured in this amendment.

The MCS 4.0 Logs and Alarms Description document can be found in Livelink at http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7698565&objAction=browse&sort=name.

2 MCS Alarms

2.1 SM Service Address (SVCA) Alarm

2.1.1 SVCA 801

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This alarm is raised when the service address of System Manager is changed from the Management Console.

Format

Table 1: SVCA801 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SVCA/SMSVCADR
Alarm Name	SM Service Address Changes
Event Type	ADMIN
Severity:	Critical

Problem Text	System Manager service address changed.
Corrective Action:	Redeploy System Manager
Clear Condition:	System Manager is redeployed.

Action

If SM service address is changed, SM needs to be redeployed to take the IP Address change. If the administrator cannot login to SM from the Management Console after SM is redeployed, contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

2.2 Threshold (THLD) Alarms

2.2.1 EPMTC 401

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This alarm is raised on the Session Manager when the configured percentage of unreachable static clients has been reached.

Format

Table 2: EPMTC 401 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMTC/EPMTC
Alarm Name	Unreachable Static Clients.
Event Type:	THRESHOLD
Severity:	Warning
Problem Text	The number of unreachable static clients has exceeded the configured percentage of [X] % ... currently there are [Y] unreachable clients.
Corrective Action:	Collect the audit logs and service the affected clients as soon as possible.

Clear Condition:	Manual acknowledgement of the alarm by the craftsperson. If no manual acknowledgement has occurred, the start of the next audit will clear the raised alarm.

Table 3: EPMTC 401 Field descriptions

Field	Value	Description
[X]	Integer	The configured percentage of unreachable static clients when the alarm will be raised.
[Y]	Integer	The number of unreachable static clients.

Example:

```
The number of unreachable static clients has exceeded the configured
percentage of 100 % … currently there are 10010 unreachable clients
```

Action

Service the affected subscribers. Make sure the subscribers' clients are connected and registered.

Associated Operational Measurements or Performance Measurements

Not applicable

2.2.2 SIP 401

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

There is a SIP protocol alarm for call failures. This alarm is raised on the crossing of a threshold that is defined for OM group SIP_Inbound_Response_Report. This OM group counts SIP response messages which are received in response to outgoing SIP request messages. One response message in particular, "500 Server Internal Error" is designated as the call failure indication. There are three configurable thresholds for the SIP 500 response for minor, major, and critical alarms. The thresholds specify the 500 responses as a percentage of total responses. For example, if the minor threshold is set to the value 5, a minor alarm will be raised if, in any Office Transfer Period, the number of 500 responses reaches 5% of the total responses. The thresholds are configured in the Configuration Parameters of the network element.

In OM group SIP_Inbound_Response_Report there is one 500 register (and one set of configurable thresholds) for each supported SIP request message (INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PUBLISH, REFER, REGISTER, SUBSCRIBE, and UPDATE). Threshold checking (and resulting alarm generation, modification, or clearing) are performed at the end of each Office Transfer Period. Threshold checking is performed on each transaction type independently of all others. In order to prevent erroneous alarms behavior, threshold checking is subject to a minimum transaction count. There must be at least 100 transactions for threshold checking to be performed. This means that if an alarm is raised in one Office Transfer Period and fewer than 100 transactions occur in a subsequent Office Transfer Period, the alarm will persist regardless of the number of 500 responses.

In addition to the standard alarm fields, the OM threshold alarm will contain a Response Code Dump of recently received 500 response messages, which can be used to determine the source of the 500 responses. The format of each entry is similar to that shown below:

Format

Table 4: SIP 401 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SIP/SIPPRTCL
Alarm Name	OM threshold for SIP inbound 500 responses exceeded.
Event Type:	THRESHOLD_CROSSED
Severity:	Minor, Major, Critical
Problem Text	The number of 500 Server Internal Error responses to SIP <transaction> requests in OM group SIP_Inbound_Response_Report exceeds the specified percentage of responses.
Corrective Action:	Using the Response Code Dump of recent 500 responses in the alarm description, locate the network element that is responding with 500. Examine logs on the network element to determine if there is a SWER or other log which indicates that an error condition is causing the 500 responses. If there is no SWER or log which clearly identifies the problem and resolution, contact your next level of support.
Clear Condition:	Cleared when the number of 500 Server Internal Error responses falls below the specified percentage for the minor threshold.
Other:	Response Code Dump (see SIP 401 Field Descriptions).

Table 5: SIP 401 Field Descriptions

Field	Value	Description
transaction	String	The SIP

		transaction type for which the 500 response threshold was exceeded, which will be one of the following: INFO, INVITE, MESSAGE, NOTIFY, OPTIONS, PUBLISH, REFER, REGISTER, SUBSCRIBE, or UPDATE.
Response Code Dump	Example entry: Response Code [500] Dump: Queue Depth: 20 Queue Elements: 13 [0] Sat Mar 05 14:31:50 CST 2005 (1110054710931) ***INBOUND*** Source: IPDestination [INETADDR: **47.102.116.63**][PORT:5095][TRNSPRT: UDP] SIP/2.0 500 Server Internal Error to: "user 1001" <sip:9726851001@dt1.com>;tag=666777888 from: "user 1002" <sip:u1002@dt1.com>;tag=1244863008 call-id: 02746aac3a1d9280316ea896c1883d32577cea3@47.102.117.7 cseq: 5557 INVITE via: SIP/2.0/UDP 47.102.117.7:5065;branch=z9hG4bK-2a5a2-a57030d-1ad7fef0	Use the entries in the list to determine the network element which is sending the 500 responses. The example shows the IP address of the network element in bold text.

Action

Attached to each alarm report is a Response Code Dump, which contains a list of the most recently received 500 response messages. In each response message, the Source field identifies the source of the 500 response. Specifically, it contains the IP address of the network element which sent the 500 response. A 500 Server Internal Error response message is typically associated with a SWER report on the network element which sent the 500 response, and the SWER report will typically be accompanied by descriptive text indicating what corrective action should be taken. In the absence of such a descriptive text, the operator or craftperson should collect the SWER report and contact the next level of support.

Associated Operational Measurements or Performance Measurements

SIP_Delay_Report

SIP_Outbound_Response_Report

SIP_Transaction_Report

2.3 Database Communications (DBCM) Alarms

No changes

2.4 License Key (LKEY) Alarms

No changes

2.5 Recording System (RTA) Alarms

No changes

2.6 System (SYS) Alarms

2.6.1 SYS 707

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This alarm is raised when a fault tolerant network element instance requests synchronization from it's peer but is rejected.

Format

Table 6: SYS 707 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SYS/SYSTEM
Alarm Name	Synchronization request rejected
Event Type	ABNORMAL
Severity:	Major
Problem Text	System Manager service address changed.

Corrective Action:	Request to receive synchronization from peer rejected.
Clear Condition:	Restart network element instance.

Action

If problem reoccurs after restart or happens frequently, contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

2.7 SM Proxy (SMCM) Alarms

No changes

2.8 Security (SEC) Alarms

No changes

2.9 FTP (FTP) Alarms

No changes

2.10 Audiocode Gateway (AC) Alarms

No changes

2.11 Resource Management (RESM) Alarms

No changes

2.12 NE Proxy (NECM, SYNC) Alarms

No changes

2.13 Loads Directory (LOADS) Alarms

No changes

2.14 Server (SRVR) Alarms

No changes

2.15 Database Monitor (DBMN) Alarms

No changes

2.16 Keycode Resource (KCRE) Alarms

No changes

2.17 Media Application Server Provisioning (MAS) Alarms

No changes

2.18 Media Application Server Platform (MAS) Alarms

No changes

2.19 RTP Media Portal (RTP) Alarms

New MCS09 RTP Media Portal alarms are described in the following sections.

2.19.1 RTP 804

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This log/alarm is generated when difficulties are encountered when attempting to initialize/configure an RTP Media Portal (e.g. RTP Media Packet Engine is not loaded, cluster configuration is incorrect, error encountered configuring Fault Tolerance HA Layer, attempting to configure a CPX8216-T based RTP Media Portal as a cluster - or a BladeCenter-T based RTP Media Portal as a non-cluster)

Once set, this alarm condition remains set until the causing condition(s) is/are rectified and the RTP Media Portal is restarted.

Format

Table 7: RTP 804 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RTPB/RTPBLADE
Alarm Name	RTP Media Portal Configuration/Initialization Error

Event Type:	*CONFIG_OR_CUSTOMIZATION_ERROR*
Severity:	Critical
Problem Text	An error occurred during initialization. $1. The RTP Media Portal is NOT operational.
Corrective Action:	Please contact your next level of technical support.
Clear Condition:	Correct the configuration issue and restart the RTP Media Portal.

Table 8: RTP 804 Field descriptions

Field	Value	Description
$1	Text	Additional text describing the cause of the error condition

Example:

"An error occurred during initialization. **An error occurred while attempting to configure the HA Layer**. The RTP Media Portal is NOT operational.".

Action

Verify RTP Media Portal configuration.

Contact your next level of support.

Associated Operational Measurements or Performance Measurements

N/A.

2.19.2 RTP 805

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This informational alarm is generated to indicate that the corresponding service node is hosting the Standby Service Instance (ready to become active in the event of a failure).

Once set, this alarm condition remains set until the corresponding blade becomes active or is shutdown.

Format

Table 9: RTP 805 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RTPB/RTPBLADE
Alarm Name	RTP Media Portal Blade Standby Message
Event Type:	*UNSPECIFIED_REASON*
Severity:	*WARNING*
Problem Text	The RTP Media Portal Blade in slot $1 is in $2
Corrective Action:	This is informational only. No user action is required.
Clear Condition:	This alarm is cleared when the blade becomes active.

Table 10: RTP 805 Field descriptions

Field	Value	Description
$1	integer	Slot number in chassis
$2	String	State – Standby or Standby-Sync

Example:

```
"The RTP Media Portal Blade in slot 2 is in Standby".
```

Action

This alarm is informational only. No corrective action is required.

Associated Operational Measurements or Performance Measurements

standbyInstances (Integer): Meter showing number of standby Service Instances in the Service Cluster.

2.19.3 RTP 806

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This log/alarm is generated to indicate that the RTP Media Portal Cluster is in an invalid cluster configuration. The Cluster currently exists in a state different from how it is configured.

Once set, this alarm condition remains set until the cluster nodes are operational.

Format

Table 11: RTP 806 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RTPB/RTPBLADE
Alarm Name	HA Layer Invalid Cluster Configuration
Event Type:	*UNDERLYING_RESOURCE_UNAVAILABLE*
Severity:	*Critical*
Problem Text	Cluster is in a $1+$2 configuration with $3 node(s) shutting down and should be in a $4+$5 configuration
Corrective Action:	Ensure all nodes within the cluster are operational. If not, may need to restart the cluster nodes.
Clear Condition:	This alarm will clear when all nodes are operational.

Table 12: RTP 806 Field descriptions

Field	Value	Description
$1	Integer	Number of active nodes present in the cluster
$2	Integer	Number of standby nodes present in the cluster
$3	Integer	Number of nodes commanded to shutdown
$4	Integer	Number of nodes configured to be active
$5	Integer	Number of nodes configured to be standby

Example:

```
"Cluster is in a 7+0 configuration with 0 node(s) shutting down and
should be in a 7+1 configuration".
```

Action

Ensure all nodes of the cluster are operational. If necessary, restart the non-operational nodes.

Contact your next level of support.

Associated Operational Measurements or Performance Measurements

activeInstances (Integer): Meter showing number of active Service Instances in the Service Cluster.

standbyInstances (Integer): Meter showing number of standby Service Instances in the Service Cluster.

2.19.4 RTP 815

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This log/alarm is generated when a change to "Media Portal Cluster" data is detected to indicate that Live Update of Media Portal Cluster Configuration Parameters Data is NOT supported.

If Media Portal Cluster Configuration Parameters Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster then this alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

Format

Table 13: RTP 815 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RTPB/RTPBLADE
Alarm Name	RTP Media Portal does NOT support Live MPCluster Configuration Update
Event Type:	*CONFIG_OR_CUSTOMIZATION_ERROR*
Severity:	Minor

Problem Text	Live Update of Media Portal Cluster Configuration Parameters Data is NOT supported.
Corrective Action:	MPCluster Configuration Data change will take effect and the alarm will clear when the Media Portal is restarted.
Clear Condition:	Restart the RTP Media Portal to clear the alarm.

Action

Verify if the MPCluster Configuration Parameters data change is necessary and correct. If yes, then restart all RTP Media Portal NEs associated with this Service Cluster. If no, contact your next level of support.

Associated Operational Measurements or Performance Measurements

N/A

2.19.5 RTP 816

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This log/alarm is generated when a change to "Media Portal Cluster" data is detected to indicate that Live Update of Media Portal Cluster Fault Tolerance Data is NOT supported.

If Media Portal Cluster Fault Tolerance Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

Format

Table 14: RTP 816 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RTPB/RTPBLADE
Alarm Name	RTP Media Portal does NOT support Live MPCluster Configuration Update

Event Type:	*CONFIG_OR_CUSTOMIZATION_ERROR*
Severity:	Minor
Problem Text	Live Update of Media Portal Cluster Fault Tolerance Data is NOT supported.
Corrective Action:	MPCluster Configuration Data change will take effect and the alarm will clear when the Media Portal is restarted.
Clear Condition:	Restart the RTP Media Portal to clear the alarm.

Action

Verify if the Media Portal Cluster Fault Tolerance data change is necessary and correct. If yes, then restart all RTP Media Portal NEs associated with this Service Cluster. If no, contact your next level of support.

Associated Operational Measurements or Performance Measurements

N/A

2.19.6 RTP 817

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This log/alarm is generated when a change to "Media Portal Cluster" data is detected to indicate that Live Update of Media Portal Cluster Gateway Controllers Data is NOT supported.

If Media Portal Cluster Gateway Controllers Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

Format

Table 15: RTP 817 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RTPB/RTPBLADE

Alarm Name	RTP Media Portal does NOT support Live MPCluster Configuration Update
Event Type:	*CONFIG_OR_CUSTOMIZATION_ERROR*
Severity:	Minor
Problem Text	Live Update of Media Portal Cluster Gateway Controllers Data is NOT supported.
Corrective Action:	MPCluster Configuration Data change will take effect and the alarm will clear when the Media Portal is restarted.
Clear Condition:	Restart the RTP Media Portal to clear the alarm.

Action

Verify if the MPCluster Gateway Controllers data change is necessary and correct. If yes, then restart all Media Portals in the cluster. If no, contact your next level of support.

Associated Operational Measurements or Performance Measurements

N/A

2.19.7 RTP 818

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This log/alarm is generated when a change to "Media Portal Cluster" data is detected to indicate that Live Update of Media Portal Cluster Session Managers Data is NOT supported.

If Media Portal Cluster Session Managers Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

Format

Table 16: RTP 818 Attributes

Attribute Name	Attribute Value

Family Name (S/L)	RTPB/RTPBLADE
Alarm Name	RTP Media Portal does NOT support Live MPCluster Configuration Update
Event Type:	*CONFIG_OR_CUSTOMIZATION_ERROR*
Severity:	Minor
Problem Text	Live Update of Media Portal Cluster Session Managers Data is NOT supported.
Corrective Action:	MPCluster Configuration Data change will take effect and the alarm will clear when the Media Portal is restarted.
Clear Condition:	Restart the RTP Media Portal to clear the alarm.

Action

Verify if the MPCluster Session Managers data change is necessary and correct. If yes, then restart all Media Portals in the cluster. If no, contact your next level of support.

Associated Operational Measurements or Performance Measurements

N/A

2.19.8 RTP 819

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This log/alarm is generated when a change to "Media Portal Cluster" data is detected to indicate that Live Update of Media Portal Cluster Static Routes Data is NOT supported.

If Media Portal Cluster Static Routes Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

Format

Table 17: RTP 819 Attributes

Attribute Name	Attribute Value

Family Name (S/L)	RTPB/RTPBLADE
Alarm Name	RTP Media Portal does NOT support Live MPCluster Configuration Update
Event Type:	*CONFIG_OR_CUSTOMIZATION_ERROR*
Severity:	Minor
Problem Text	Live Update of Media Portal Cluster Static Routes Data is NOT supported.
Corrective Action:	MPCluster Configuration Data change will take effect and the alarm will clear when the Media Portal is restarted.
Clear Condition:	Restart the RTP Media Portal to clear the alarm.

Action

Verify if the MPCluster Static Routes data change is necessary and correct. If yes, then restart all Media Portals in the cluster. If no, contact your next level of support.

Associated Operational Measurements or Performance Measurements

N/A

2.19.9 RTP 820

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This log/alarm is generated when a change to "Media Portal Cluster" data is detected to indicate that Live Update of Media Portal Cluster Service Instances Data is NOT supported.

If Media Portal Cluster Service Instances Data is changed or deleted from the System Manager Console while the data is in use by any ACTIVE Media Portal(s) in the cluster. This alarm will be raised on all the RTP Media Portal NEs that are using the cluster data.

Once set, this alarm condition remains set until all RTP Media Portal NE's associated with the Service Cluster are restarted.

Format

Table 18: RTP 820 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RTPB/RTPBLADE
Alarm Name	RTP Media Portal does NOT support Live MPCluster Configuration Update
Event Type:	*CONFIG_OR_CUSTOMIZATION_ERROR*
Severity:	Minor
Problem Text	Live Update of Media Portal Cluster Service Instances Data is NOT supported.
Corrective Action:	MPCluster Configuration Data change will take effect and the alarm will clear when the Media Portal is restarted.
Clear Condition:	Restart the RTP Media Portal to clear the alarm.

Action

Verify if the MPCluster Service Instances data change is necessary and correct. If yes, then restart all Media Portals in the cluster. If no, contact your next level of support.

Associated Operational Measurements or Performance Measurements

N/A

2.20 H323 Gatekeeper (H3GK) Alarms

No changes

2.21 I/O (TCF) Alarms

No Changes

2.22 Terminal Server (TSVR) Alarms

No changes

2.23 H323 Maintenance (H323) Alarms

No changes

2.24 IMDB (IMDB) Alarms

No changes

2.25 Overload Control (OLC) Alarms

No changes

2.26 NCAS Alarms

2.26.1 NCAS 101

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This alarm is raised when the NCAS link to the CS2K Core has been disconnected.

Format

Table 19: NCAS 101 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	NCAS/NCAS
Alarm Name	NCAS
Event Type:	COMM
Severity:	Minor
Problem Text	NCAS Link to [X] disconnected.
Corrective Action:	Check network connectivity.
Clear Condition:	Connection to 2K Core established.

Table 20: NCAS 101 Field descriptions

Field	Value	Description
[X]	IP Address	IP address of the CS2K Core

Example:

```
NCAS Link to 47.104.117.22 disconnected.
```

Action

Verify network connectivity between the System Manager and the CS2K Core. Ensure Scplite is able to bring up an SCTP connection to the CS2K Core. Ensure the CS2K Core is available and accepting SCTP client connections.

Associated Operational Measurements or Performance Measurements

NCAS OM

2.27 R6 Application Server

2.27.1 R6AS0

Add/Modify/Delete

This alarm is being **added** for MCS09.

Explanation

This alarm is raised when the R6AS servertype configuration item of a Session Manager is modified.

Format

Table 21: R6AS0 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	R6AS/R6AS
Alarm Name	R6AS Configuration Modification
Event Type	ABNORMAL
Severity:	MAJOR
Problem Text	R6AS configuration modified while instance is not offline
Corrective Action:	Reboot the network element
Clear Condition:	Session Manager restarted

Action

The alarm can only be cleared by restarting the Session Manager which raised it.

Associated Operational Measurements or Performance Measurements

Not applicable

3 MCS Logs

3.1 Software Error (SWER) Logs

3.1.1 SWER 801

Add/Modify/Delete

This log is being **updated** for MCS09

Explanation

This log indicates that a software error has occurred and that an alarm has been raised.

Format

Table 22: SWER 801 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SWER/SWERR
Event Type	ABNORMAL
Severity	MINOR
Report Text	One or more Software Errors have occurred. The first one is captured below. Please collect the SWERs and the surrounding logs from the log file. SWER Reported:<swer_text>

Table 23: SWER 799 Field descriptions

Field	Value	Description
Swer_text	String	Description of software error provided by application along with an exception stack trace.

Action

Contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

3.2 Address (ADDR) Logs

3.2.1 ADDR 801

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that IP Address is changed.

Format

Table 24: ADDR 801 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	ADDR/ADDRESS
Event Type	ADMIN
Severity	INFO
Report Text	<<Logical Name>> IPAddress changed from <<oldAddr> to <newAddr>>

Table 25: ADDR 801 Field descriptions

Field	Value	Description
Logical Name	String	Logical Name of the IPAddress being changed
oldAddr	String	Old IPAddress
newAddr	String	New IPAddress

Action

There is no action required.

Associated Operational Measurements or Performance Measurements

Not applicable

3.3 Session Manager Accounting (ACAT) Logs

3.3.1 ACAT 201

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log is generated when setting a Session Manager's AM from <none> to a valid AM.

Format

Table 26: ACAT 201 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	ACAT/ACTAGENT
Event Type	Resource Availability
Severity	INFO
Report Text	Accounting is enabled upon this NE.

Action

There is no action required.

Associated Operational Measurements or Performance Measurements

On all instances of this Session Manager, the <NE_Inst>:<AM>:STD:acct OM row in the StdRecordStream group will appear and start counting the recording units sent to the configured AM.

On the configured AM, the <NE_inst>:acct OM rows in RECSTRMCOLL group will appear and start counting the recording units received from this Session Manager's instances.

3.3.2 ACAT 202

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log is generated when setting a Session Manager's AM from a valid AM to <none>.

Format

Table 27: ACAT 202 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	ACAT/ACTAGENT
Event Type	Resource Availability
Severity	ALERT
Report Text	Accounting is disaabled upon this NE.

Action

If you do not intend for the Session Manager to produce accounting records, then no action is required. If you do intend for the Session Manager to produce accounting records, then you should set the Session Manager's AM to a valid AM.

Associated Operational Measurements or Performance Measurements

On all instances of this Session Manager, the <NE_Inst>:<AM>:STD:acct OM row in the StdRecordStream group that matched the previous datafilled AM will disappear.

On the previously configured AM, the <NE_inst>:acct OM rows in RECSTRMCOLL group will disappear.

3.4 Network Interface (NIF) Logs

No changes

3.5 OM Collection (OM) Logs

No changes

3.6 Scheduler (SCHD) Logs

No changes

3.7 Database Communications (DBCM) Logs

3.7.1 DBCM 204

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that no database instance is available for initialization. This condition may be due to all database instances being out of service, or due to network connectivity problems preventing communication.

Format

Table 28: DBCM 204 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	DBCM/DBCOMM
Event Type	ABNORMAL
Severity	ALERT
Report Text	No suitable database instance is available for initialization

Action

Bring database instances back into service, or clear network connectivity problems preventing communication with the database instances.

Example

DBCM/DBCOMM 204 ALERT APR18 14:42:35
No suitable database instance is available for initialization

Associated Operational Measurements or Performance Measurements

Not applicable

3.7.2 DBCM 704

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that one of the database instances configured against a release that is incompatible with the release in the intializing network element instance. Connection to a database instance with an incompatible release is prohibited.

Format

Table 29: DBCM 704 Attributes

Attribute Name	Attribute Value

Family Name (S/L)	DBCM/DBCOMM
Event Type	ABNORMAL
Severity	ALERT
Report Text	Connection to <db-instance> with configured release <configured-release> from an NE instance running incompatible release <running-release> is prohibited

Table 30: DBCM 704 Field descriptions

Field	Value	Description
<db-instance>	DB Instance 0 or DB Instance 1	The database instance to which the network element instance tried to connect.
<configured-release>	a load in the mcp/loads directory	The load configured against the database instance
<running-release>	a load in the mcp/loads directory	The load configured against the initializing network element instance.

Action

No action is required – this log is for informational purposes.

Example

DBCM/DBCOMM 704 ALERT APR18 14:42:35
Connection to DB Instance 0 with configured release 9.2.0.0 from an NE instance running incompatible release 9.1.1.1 is prohibited

Associated Operational Measurements or Performance Measurements

Not applicable

3.8 Alarm Agent (ALM) Logs

No changes

3.9 Log Agent (LGAT) Logs

No changes

3.10 License Key (LKEY) Logs

No changes

3.11 Network Element Communication (NEC) Logs

No changes

3.12 Recording System (RECS, RTA) Logs

No changes

3.13 Sync System (CHKP) Logs

No changes

3.14 System (SYS) Logs

3.14.1 SYS 706

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the inactive network element instance of a fault pair of instances has experienced a drop and the sync channel (not due to peer failure), has been unable to re-establish the channel within a reasonable amount of time and is thus to far out of sync to proceed. The instance will restart and attempt to synchronize in the process.

Format

Table 31: SYS 706 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SYS/SYSTEM
Event Type	ABNORMAL
Severity	ALERT
Report Text	Hot activation no longer possible. Synchronization information is stale.

Action

If instance repeatedly restarts, contact the next level of support.

3.14.2 SYS 813

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates the state of the send side of the synchronization channel between peer fault tolerant network element instances.

The send side is the active network element instance.

Format

Table 32: SYS 813 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SYS/SYSTEM
Event Type	ADMIN
Severity	INFO
Report Text	Synchronization send status: <status>.

Table 33: SYS 813 Field descriptions

Field	Value	Description
<status>	"Starting", "Terminating" or "Terminated".	"Starting" when sync channel established, "Terminating" when channel begins takedown sequence, "Terminated" when sync channel is gone.

Action

None.

3.14.3 SYS 814

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates the state of the receive side of the synchronization channel between peer fault tolerant network element instances.

The receive side is the inactive network element instance.

Format

Table 34: SYS 814 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SYS/SYSTEM
Event Type	ADMIN
Severity	INFO
Report Text	Synchronization receive status: <status>.

Table 35: SYS 814 Field descriptions

Field	Value	Description
<status>	"Starting", "Terminating" or "Terminated".	"Starting" when sync channel established, "Terminating" when channel begins takedown sequence, "Terminated" when sync channel is gone.

Action

None.

3.15 Security (SEC) Logs

No changes

3.16 FPM (ALRM) Logs

No changes

3.17 SNMP (SNMP) Logs

No changes

3.18 RTA Collector (RTAC) Logs

No changes

3.19 File Transport (FTP) Logs

No changes

3.20 ORV (ORV) Logs

No changes

3.21 NMI SNMP (NMI) Logs

No changes

3.22 Audiocode Gateway (AC) Logs

No changes

3.23 System Manager (SMAL) Logs

No changes

3.24 NED (NED) Logs

No changes

3.25 OMI (OMIS) Logs

No changes

3.26 Transaction State Machine (XACT) Logs

No changes

3.27 NE Proxy (NEI) Logs

No changes

3.28 OM Query (OM) Logs

No changes

3.29 LOM (LOM) Logs

No changes

3.30 MAS Platform (MAS) Logs

No changes

3.31 Base Provisioning (PROV) Logs

No changes

3.32 IP Client Manager (ESM) Logs

No changes

3.33 MAS Provisioning Manager (MAS) Logs

No changes

3.34 Media Portal (RTP) Logs

The new MCS09 RTP Media Portal logs are described in the following sections.

3.34.1 RTP 808

Add/Modify/Delete

This log is being **added** for MCS09.

Explanation

The informational "Active Instance Log" is produced when a RTP Media Portal Service Instance becomes active.

Format

Table 36: RTP 808 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RTP/RTPIOCF
Event Type	Admin
Severity	INFO
Report Text	"RTP Media Portal instance $1 is active with the following IP addresses: service IP: $2 NET1 IP: $3 NET2 IP: $4

Table 37: RTP 808 Field descriptions

Field	Value	Description

$1	String	Instance Name
$2	Dotted IP Address	MPCP Service IP Address
$3	Dotted IP Address	Net1 Media IP Address
$4	Dotted IP Address	Net2 Media IP Address

Action

No action required.

Associated Operational Measurements or Performance Measurements

activeInstances (Integer): Meter showing number of active Service Instances in the Service Cluster.

3.35 Conference (CLS) Logs

No changes

3.36 RAS SIP Gateway (RAS) Logs

No changes

3.37 Voicemail (VM) Logs

No changes

3.38 Media Portal Service (MP) Logs

No changes

3.39 Emergency Service (EMRG) Logs

3.39.1 EMGR 802

Add

This log is being **added** for MCS09

Explanation

This log is generated when the E911 emergency operator attempts to callback the originating (enterprise) caller. This log is not generated for residential operator callback attempts.

Format

Table 38: EMGR 802 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMRG
Event Type	ADMINISTRATIVE
Severity	INFO
Report Text	Emergency operator callback to an enterprise ELIN $1 is being attempted.

Table 39: EMGR 802 Field Descriptions

Field	Value	Description
$1	The 10 digit ELIN/ANI	The ELIN is a PSTN routable address which routes to the originating emergency caller.

Action

No administrative action required.

Associated Operational Measurements or Performance Measurements

OM Group: Emergency

OM Row: SESM1

Register: operatorCallbackAttempt

3.39.2 EMGR 803

Add

This log is being **added** for MCS09

Explanation

This log is generated when the E911 emergency operator established voicepath with the originating (enterprise) caller. This log is not generated for residential operator callbacks.

Format

Table 40: EMGR 803 Attributes

Attribute Name	Attribute Value

Family Name (S/L)	EMRG
Event Type	ADMINISTRATIVE
Severity	INFO
Report Text	Emergency operator callback to an enterprise ELIN $1 has connected.

Table 41: EMGR 803 Field Descriptions

Field	Value	Description
$1	The 10 digit ELIN/ANI	The ELIN is a PSTN routable address which routes to the originating emergency caller.

Action

No administrative action required.

Associated Operational Measurements or Performance Measurements

OM Group: Emergency

OM Row: SESM1

Register: operatorCallbackConnected

3.39.3 EMGR 704

Add

This log is being **added** for MCS09

Explanation

This log is generated when any established emergency call is abnormally disconnected. In this context, abnormal disconnect refers to a failed call audit, possibly from device network isolation or client failure. The session manager will automatically free network (to PSAP) resources when this condition is detected.

Format

Table 42: EMGR 704 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMRG

Event Type	ADMINISTRATIVE
Severity	ABNORMAL
Report Text	Emergency call has abnormally disconnected. Call Audit failed for subscriber $1.

Table 43: EMGR 704 Field Descriptions

Field	Value	Description
$1	SIP Subscriber	The disconnected subscriber; previously engaged in emergency call.

Action

No administrative action required.

Associated Operational Measurements or Performance Measurements

Not Applicable

3.39.4 EMGR 705

Add

This log is being **added** for MCS09

Explanation

This log is generated when a PSAP connect failure is detected while attempting to establish an emergency call. Connection failure scenarios include: no answer timeout, busy trunks or gateway unavailable.

Format

Table 44: EMGR 705 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMRG
Event Type	ADMINISTRATIVE
Severity	ABNORMAL
Report Text	Could not establish emergency call. Failure connecting with E911 operator route $1.

Table 45: EMGR 705 Field Descriptions

Field	Value	Description
$1	PSAP destination	The attempted PSAP route destination that failed to connect during an emergency call. Format: user@domain.

Action

No administrative action required.

Associated Operational Measurements or Performance Measurements

OM Group: Emergency

OM Row: SESM1

Register: operatorConnectFailure

3.40 Message Validator Service (MSGV) Logs

No changes

3.41 Presence Service (PRS) Logs

No changes

3.42 NCL Service (NCL) Logs

No changes

3.43 Treatment Service (TRMT) Logs

No changes

3.44 Service Package (SVP) Logs

No changes

3.45 H323 Call Processing (H323) Logs

No changes

3.46 H323 Maintenance (H323) Logs

No changes

3.47 IP Device (IDEV) Logs

No changes

3.48 TCP Framework (TCP) Logs

No changes

3.49 NCAS Logs

3.49.1 NCAS 102

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates NCAS link state changes.

Format

Table 46: NCAS 102 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	NCAS/NCAS
Event Type	COMM
Severity	INFO
Report Text	NCAS Link State Report: Core Address: [X] Admin State: [Y] Oper State: [Z]

Table 47: NCAS 102 Field descriptions

Field	Value	Description
[X]	IP Address	The IP Address for the CS2K Core
[Y]	String	The administrative state of the link: ONLINE or OFFLINE
[Z]	String	The operational state of the link: CONNECTING, CONNECTED, or DISCONNECTED

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

Not applicable

3.50 Static Client Audit Logs

3.50.1 EPMTC 601

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the daily static client audit has begun on the Session Manager.

Format

Table 48: EPMTC 601 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMTC/EPMTC
Event Type	AUDIT
Severity	INFO
Report Text	Static SIP Line client audit started

Table 49: EPMTC 601 Field descriptions

Field	Value	Description
N/A	N/A	N/A

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

Not applicable

3.50.2 EPMTC 602

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the daily static client audit has completed on the Session Manager.

Format

Table 50: EPMTC 602 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMTC/EPMTC
Event Type	AUDIT
Severity	INFO
Report Text	Static SIP Line client audit completed. [X] existing static clients ([Y] % of these are unreachable).

Table 51: EPMTC 602 Field descriptions

Field	Value	Description
[X]	Integer	The total number of static clients homed on this Session Manager.
[Y]	Integer	The percentage of static clients homed on this Session Manager that are unreachable.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

Not applicable

3.50.3 EPMTC 603

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates when a SIP Line static client fails to respond to the OPTIONS ping. From our perspective, the SIP Line static client is registered with contacts but is not responding.

Format

Table 52: EPMTC 603 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMTC/EPMTC
Event Type	AUDIT
Severity	ALERT
Report Text	No audit response from static SIP Line client [X].

Table 53: EPMTC 603 Field descriptions

Field	Value	Description
[X]	String	The subscriber's registered contact, typically in the format of `userName@ipAddress:port` If the subscriber's registered contact is not available, the subscriber's internal resource id is included in the log.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

Not applicable

3.50.4 EPMTC 604

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates when an error has occurred when attempting to send an OPTIONS ping to a SIP Line static client. Errors may include:

(1) Not being able to locate the user in our in-memory table

(2) Not being able to send out OPTIONS via Radvision

(3) Not being able to acquire registered destinations.

Format

Table 54: EPMTC 604 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMTC/EPMTC
Event Type	AUDIT
Severity	ALERT
Report Text	Static SIP Line client [X]: [Y].

Table 55: EPMTC 604 Field descriptions

Field	Value	Description
[X]	String	The subscriber's SIP URI, typically in the format of `userName@domain` If the subscriber's SIP URI is not available, the subscriber's internal resource id is included in the log.
[Y]	String	The text describing why an error was encountered.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

Not applicable

3.50.5 EPMTC 605

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates when a SIP Line static client does not have any registered destinations.

Format

Table 56: EPMTC 605 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMTC/EPMTC
Event Type	AUDIT
Severity	ALERT
Report Text	No registered destinations for static SIP Line client [X].

Table 57: EPMTC 605 Field descriptions

Field	Value	Description
[X]	String	The subscriber's SIP URI, typically in the format of `userName@domain`

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

Not applicable

3.50.6 EPMTC 606

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates when the audit's start hour of day has been manually changed.

Format

Table 58: EPMTC 606 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	EMTC/EPMTC
Event Type	AUDIT
Severity	INFO
Report Text	Static SIP Line audit has been re-scheduled for [X], due to a configuration change.

Table 59: EPMTC 606 Field descriptions

Field	Value	Description
[X]	String	The new start time for the audit.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

Not applicable

3.50.7 EPMTC 607

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates when the audit's start hour of day has been manually changed and the current audit has been prematurely stopped.

Format

Table 60: EPMTC 607 Attributes

Attribute Name	Attribute Value

Family Name (S/L)	EMTC/EPMTC
Event Type	AUDIT
Severity	INFO
Report Text	Static SIP Line audit has been prematurely halted and re-scheduled for [X], due to a configuration change.

Table 61: EPMTC 607 Field descriptions

Field	Value	Description
[X]	String	The new start time for the audit.

Action

Not applicable.

Associated Operational Measurements or Performance Measurements

Not applicable

3.51 SIP Protocol (SIP) Logs

3.51.1 SIP 152

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the MCS SIP stack failed to send an outbound SIP request message. The reason why is provided in the log text but is typically because of a lack of resources in the stack.

Format

Table 62: SIP 152 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SIP/SIPPRTCL
Event Type	COMM
Severity	ALERT

Report Text	Stack Error Detected. Unable to send request: <request>. For the following reason: <reason>. Look for possible RVStack level SWER

Table 63: SIP 152 Field descriptions

Field	Value	Description
request	String	Textual representation of the request that the MCS was attempting to send.
reason	String	Description of the reason why the request could not be sent.

Action

Contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

3.51.2 SIP 153

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the MCS SIP stack failed to send an outbound SIP response message. The response being attempted is given in the log text.

Format

Table 64: SIP 153 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	SIP/SIPPRTCL
Event Type	COMM
Severity	ALERT
Report Text	Stack Error Detected. Unable to send response: <response>. Look for possible RVStack level SWER

Table 65: SIP 153 Field descriptions

Field	Value	Description
response	String	Textual representation of the response that the MCS was attempting to send.

Action

Contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

3.52 Tones Service (TONE) Logs

3.52.1 TONE 201

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the MCS Tones Service failed to register part of its state machine, indicative of a resource failure on system startup.

Format

Table 66: TONE 201 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	TONE/TONE
Event Type	RES
Severity	ALERT
Report Text	Failed to register state <state>.

Table 67: TONE 201 Field descriptions

Field	Value	Description
state	String	Textual representation of the state that failed to be registered to the service

Action

Contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

3.52.2 TONE 702

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the MCS Tones Service received a request to play a tone that it does not recognize.

Format

Table 68: TONE 702 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	TONE/TONE
Event Type	ABNORMAL
Severity	ALERT
Report Text	Unknown tone ID <tone-id>. No tone applied

Table 69: TONE 702 Field descriptions

Field	Value	Description
Tone-id	Integer	The integer representation of the tone that was requested that was not recognized by the service.

Action

Contact next level of support.

Associated Operational Measurements or Performance Measurements

Not applicable

3.53 Resource Management (RESM) Logs

3.53.1 RESM 200

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a partition name for a given resource is changed.

Table 709: RESM 200 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::changePartitionName successful.Resource Name:$1 | Old Partition Name:$2 | New Partition Name:$3

Table 50: RESM 200 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition name before the change.
$3	String	Indicates the partition name after the change.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.2 RESM 201

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a partition in a given resource is created.

Table 51: RESM 201 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::createPartition successful.Resource Name:$1 | Partition Name:$2 | Size:$3 | Usage:$4

Table 52: RESM 201 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition name that is created.
$3	String	Indicates the size of the new partition.
$4	String	Indicates the usage of the new partition.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.3 RESM 202

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the partition usage in a given resource is decremented.

Table 53: RESM 202 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::decrementPartitionUsage successful.Resource Name:$1 | Partition Name:$2 | Amount to decrease by:$3

Table 714: RESM 202 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition name of which usage is decremented.
$3	String	Indicates the amount that current usage is decreased by.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.4 RESM 203

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the partition size in a given resource is decremented.

Table 55: RESM 203 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES

Severity	INFO
Report Text	ResourceManager::decrementPartitionSize successful.Resource Name:$1 | Partition Name:$2 | Amount to decrease by:$3

Table 56: RESM 203 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition name of which size is decremented.
$3	String	Indicates the amount that current size is decreased by.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.5 RESM 204

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the partition in a given resource is deleted.

Table 57: RESM 204 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::deletePartition successful.Resource Name:$1 | Partition Name:$2

Table 58: RESM 204 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition that is deleted.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.6 RESM 205

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a partition's size in a given resource is incremented.

Table 59: RESM 205 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::incrementPartitionSize successful.Resource Name:$1 | Partition Name:$2 | Amount to increase by:$3

Table 60: RESM 205 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition of which size is incremented.
$3	String	Indicates the amount that the current size of the partition is

		increased by.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.7 RESM 206

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a partition's usage in a given resource is incremented.

Table 61: RESM 206 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::incrementPartitionUsage successful.Resource Name:$1 | Partition Name:$2 | Amount to increase by:$3

Table 62: RESM 206 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition of which usage is incremented.
$3	String	Indicates the amount that the current usage of the partition is increased by.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.8 RESM 207

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a partition's size in a given resource is set.

Table 63: RESM 207 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::setPartitionSize successful.Resource Name:$1 | Partition Name:$2 | New size:$3

Table 64: RESM 207 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition of which size is set.
$3	String	Indicates the amount that the size of the partition is set to.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.9 RESM 208

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a partition's usage in a given resource is set.

Table 65: RESM 208 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::setPartitionUsage successful.Resource Name:$1 | Partition Name:$2 | New usage:$3

Table 66: RESM 208 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that the partition belongs to.
$2	String	Indicates the partition of which usage is set.
$3	String	Indicates the amount that the usage of the partition is set to.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.10 RESM 209

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that the maximum capacity of a given resource is updated.

Table 67: RESM 209 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::updateResourceMax successful.Resource Name:$1 | New max:$2

Table 68: RESM 209 Field descriptions

Field	Value	Description
$1	String	Indicates the resource.
$2	String	Indicates the new maximum that the capacity of the resource is assigned to.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.11 RESM 210

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a new resource is managed.

Table 69: RESM 210 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES

Severity	INFO
Report Text	ResourceManager::manageResource successful.Resource Name:$1 | Max:$2

Table 70: RESM 210 Field descriptions

Field	Value	Description
$1	String	Indicates the resource that is managed.
$2	String	Indicates the maximum size that the capacity of the resource. Is assigned to.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.12 RESM 211

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that all occurrences of a given partition are deleted.

Table 71: RESM 211 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::deleteAllPartitions successful.Partition Name: $1 | Number of deleted:$2

Table 72: RESM 211 Field descriptions

Field	Value	Description

$1	String	Indicates the partition name that is deleted.
$2	String	Indicates number of deleted partitions.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.13 RESM 212

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a partition instance is deleted during deleteAllPartitions operation. For each instance deletion, this log is generated.

Table 73: RESM 212 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::deletePartition of deleteAllPartitions successful.Partition Name: $1 | Number $2 of $3

Table 74: RESM 212 Field descriptions

Field	Value	Description
$1	String	Indicates the partition name that is deleted.
$2	String	Indicates index of deleted partition.
$3	String	Indicates total expected deletions.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

3.53.14 RESM 213

Add/Modify/Delete

This log is being **added** for MCS09

Explanation

This log indicates that a resource is removed.

Table 75: RESM 213 Attributes

Attribute Name	Attribute Value
Family Name (S/L)	RESM/RESMGMT
Event Type	RES
Severity	INFO
Report Text	ResourceManager::removeResource successful.Resource Name:$1

Table 76: RESM 213 Field descriptions

Field	Value	Description
$1	String	Indicates the resource name that is removed.

Action

Not applicable

Associated Operational Measurements or Performance Measurements

Not applicable

Appendix J: MCS Operational Measurements

1 Operational Measurements Overview

1.1 Introduction

This document shall be considered an "amendment" to the previous release's (MCS 4.0) Operational Measurements Description document. In other words, the MCS 4.0 document will act as the "base" document with all adds/changes/deletes captured in this amendment.

The MCS 4.0 OMs Description document can be found in Livelink at http://livelink.us.nortel.com/livelink/livelink.exe?func=ll&objId=7698565&objAction=browse&sort=name

2 OM Groups Added

The OM Groups in this section have been added to this release.

2.1 OM Group Name: NCASLINK

2.1.1 Affected NE

This OM group is for the System Manager.

2.1.2 Explanation

The NCAS OM group provides data regarding the state and usage of the NCAS link. Applications use this link for non-call-associated signaling with the CS2K Core, such as QSIP queries.

2.1.3 Register Descriptions

Table 1: NCAS Register Descriptions

Register Name	Type	Description
linkUp	Counter	The number of times the logical link is transitioned into a

		connected state due to administrative action, network repair, etc.
linkDown	Counter	The number of times the logical link is transitioned into a disconnected state due to administrative action, network failure, etc.
msgSent	Counter	The number of messages successfully sent over the link.
msgRcvd	Counter	The number of messages successfully received over the link.
msgSendFail	Counter	The number of messages that failed to be sent.
msgRcvFail	Counter	The number of messages that failed to be received.

2.1.4 Thresholding and Alarms

Not Applicable.

2.2 OM Group Name: SIP_Delay_Report

2.2.1 Affected NE

This OM group is common to all network elements.

2.2.2 Explanation

The SIP_Delay_Report OM group provides information about processing time for SIP transactions on a network element. Unless otherwise noted in the SIP_Delay_Report Row Descriptions below, transaction processing time is the time that elapses between the receipt of a SIP request message and the sending of the response to that request message. The SIP_Delay_Report OM group is a set of rows and columns, where each row is a transaction type and the columns are registers that form a histogram of discrete time values.

2.2.3 Row Descriptions

Table 2: SIP_Delay_Report Row Descriptions

Row Name	Type	Description
ACK	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for ACKs in transactions. The delay values for ACKs are measured as the time taken between sending a 200 response back to the originator of a request message and the originator's responding with an ACK. If the final response to an INVITE is non-200, no delay statistics for the ACK are captured in the report (the ACK is effectively ignored for purposes of delay).

INFO	Set of Peg Registers	This row provides a set of delay peg registers for processing delay For INFO transactions.
INVITE	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for INVITE transactions. Delay values for INVITE transactions are measured as the time taken until a 18x or final response is sent back to the originator to the INVITE transaction (whichever comes first).
MESSAGE	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for MESSAGE transactions.
NOTIFY	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for NOTIFY transactions.
OPTIONS	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for OPTIONS transactions.
PUBLISH	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for PUBLISH transactions.
REFER	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for REFER transactions.
REGISTER	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for REGISTER transactions.
SUBSCRIBE	Set of Peg Registers	This row provides a set of delay peg-registers for processing delay for SUBSCRIBE transactions.
UPDATE	Set of Peg Registers	This row provides a set of delay peg-registerspeg-register for processing delay for UPDATE transactions.
[Totals]	Set of Peg Registers	This row is the totals of the columns of all of the above rows.

2.2.4 Register Descriptions

The registers in each of the rows in SIP_Delay_Report represent discrete time values. Each register is a count of the number of transactions whose processing time took at least that amount of time but less than the amount of time represented by the next register in ascending order.

Table 2: SIP_Delay_Report Register Descriptions

Register Name	Type	Description
_25ms	Peg Register	The number of transactions of the specified type which have completed in 25 milliseconds or less.
_50ms	Peg Register	The number of transactions of the specified type which have completed in more than 25 milliseconds but less than or equal to 50 milliseconds.

_100ms	Peg Register	The number of transactions of the specified type which have completed in more than 50 milliseconds but less than or equal to 100 milliseconds.
_125ms	Peg Register	The number of transactions of the specified type which have completed in more than 100 milliseconds but less than or equal to 125 milliseconds.
_150ms	Peg Register	The number of transactions of the specified type which have completed in more than 125 milliseconds but less than or equal to 150 milliseconds.
_175ms	Peg Register	The number of transactions of the specified type which have completed in more than 150 milliseconds but less than or equal to 175 milliseconds.
_200ms	Peg Register	The number of transactions of the specified type which have completed in more than 175 milliseconds but less than or equal to 200 milliseconds.
_250ms	Peg Register	The number of transactions of the specified type which have completed in more than 200 milliseconds but less than or equal to 250 milliseconds.
_300ms	Peg Register	The number of transactions of the specified type which have completed in more than 250 milliseconds but less than or equal to 300 milliseconds.
_350ms	Peg Register	The number of transactions of the specified type which have completed in more than 300 milliseconds but less than or equal to 350 milliseconds.
_400ms	Peg Register	The number of transactions of the specified type which have completed in more than 350 milliseconds but less than or equal to 400 milliseconds.
_450ms	Peg Register	The number of transactions of the specified type which have completed in more than 400 milliseconds but less than or equal to 450 milliseconds.
_500ms	Peg Register	The number of transactions of the specified type which have completed in more than 450 milliseconds but less than or equal to 500 milliseconds.
_550ms	Peg Register	The number of transactions of the specified type which have completed in more than 500 milliseconds but less than or equal to 550 milliseconds.
_600ms	Peg Register	The number of transactions of the specified type which have completed in more than 550 milliseconds but less than or equal to 600 milliseconds.
_650ms	Peg Register	The number of transactions of the specified type which have completed in more than 600 milliseconds but less than or equal to 650 milliseconds.
_700ms	Peg Register	The number of transactions of the specified type which have completed in more than 650 milliseconds but less than or equal to 700 milliseconds.
_750ms	Peg Register	The number of transactions of the specified type which have completed in more than 700 milliseconds

		but less than or equal to 750 milliseconds.
_800ms	Peg Register	The number of transactions of the specified type which have completed in more than 750 milliseconds but less than or equal to 800 milliseconds.
_850ms	Peg Register	The number of transactions of the specified type which have completed in more than 800 milliseconds but less than or equal to 850 milliseconds.
_900ms	Peg Register	The number of transactions of the specified type which have completed in more than 850 milliseconds but less than or equal to 900 milliseconds.
_950ms	Peg Register	The number of transactions of the specified type which have completed in more than 900 milliseconds but less than or equal to 950 milliseconds.
_1000ms	Peg Register	The number of transactions of the specified type which have completed in more than 950 milliseconds but less than or equal to 1000 milliseconds.
_1250ms	Peg Register	The number of transactions of the specified type which have completed in more than 1000 milliseconds but less than or equal to 1250 milliseconds.
_1500ms	Peg Register	The number of transactions of the specified type which have completed in more than 1250 milliseconds but less than or equal to 1500 milliseconds.
_1750ms	Peg Register	The number of transactions of the specified type which have completed in more than 1500 milliseconds but less than or equal to 1750 milliseconds.
_2000ms	Peg Register	The number of transactions of the specified type which have completed in more than 1750 milliseconds but less than or equal to 2000 milliseconds.
_3000ms	Peg Register	The number of transactions of the specified type which have completed in more than 2000 milliseconds but less than or equal to 3000 milliseconds.
_4000ms	Peg Register	The number of transactions of the specified type which have completed in more than 3000 milliseconds but less than or equal to 4000 milliseconds.
_8000ms	Peg Register	The number of transactions of the specified type which have completed in more than 4000 milliseconds but less than or equal to 8000 milliseconds.
_16000ms	Peg Register	The number of transactions of the specified type which have completed in more than 8000 milliseconds but less than or equal to 16000 milliseconds.

_32000ms	Peg Register	The number of transactions of the specified type which have completed in more than 16000.

2.2.5 Thresholding and Alarms

Not Applicable.

2.3 OM Group Name: SIP_Inbound_Response_Report

2.3.1 Affected NE

This OM group is common to all network elements.

2.3.2 Explanation

The purpose of the SIP_Inbound_Response_Report OM group is to provide counts of various responses messages received by a network element in response to outgoing SIP request messages. The SIP_Inbound_Response_Report OM group consists of a set of rows with each row containing and identical set of peg-registers. Each row corresponds to an outgoing SIP request message and each register (column) corresponds to a SIP response type of an incoming response. Additional SIP Response message details can be found in RFC-3261.

2.3.3 Row Descriptions

Table 3: SIP_Inbound_Response_Report Row Descriptions

Row Name	Type	Description
INFO	Set of Peg Registers	This row provides a set of peg-registers for the different response types for INFO transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing INFO transactions.
INVITE	Set of Peg Registers	This row provides a set of peg-registers for the different response types for INVITE transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing INVITE transactions.
MESSAGE	Set of Peg Registers	This row provides a set of peg-registers for the different response types for MESSAGE transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing MESSAGE transactions.
NOTIFY	Set of Peg Registers	This row provides a set of peg-registers for the different response types for NOTIFY transactions. Each peg-register counts the number of responses of the specified

		type that have been received in response to outgoing NOTIFY transactions.
OPTIONS	Set of Peg Registers	This row provides a set of peg-registers for the different response types for OPTIONS transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing OPTIONS transactions.
PUBLISH	Set of Peg Registers	This row provides a set of peg-registers for the different response types for PUBLISH transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing PUBLISH transactions.
REFER	Set of Peg Registers	This row provides a set of peg-registers for the different response types for REFER transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing REFER transactions.
REGISTER	Set of Peg Registers	This row provides a set of peg-registers for the different response types for REGISTER transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing REGISTER transactions.
SUBSCRIBE	Set of Peg Registers	This row provides a set of peg-registers for the different response types for SUBSCRIBE transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing SUBSCRIBE transactions.
UPDATE	Set of Peg Registers	This row provides a set of peg-registers for the different response types for UPDATE transactions. Each peg-register counts the number of responses of the specified type that have been received in response to outgoing UPDATE transactions.
[Totals]	Set of Peg Registers	This row is a set of totals of the other rows.

2.3.4 Register Descriptions

Each of the registers a in SIP_Inbound_Response_Report row counts the SIP response messages of the indicated type which have been received in response to outgoing SIP messages corresponding to the row type. For example, the _302 register in the INVITE row is a count of the number of 302 responses messages received in response to outgoing INVITE messages in the current Office Transfer Period.

Table 2: SIP_Inbound_Response_Report Register Descriptions

Register	Type	Description

Name		
_200	Peg Register	This register provides a count of the number of “200 OK” responses received in the current Office Transfer Period.
_202	Peg Register	This register provides a count of the number of “202 Accepted” responses received in the current Office Transfer Period.
_300	Peg Register	This register provides a count of the number of “300 Multiple Choices” responses received in the current Office Transfer Period.
_301	Peg Register	This register provides a count of the number of “301 Moved Permanently” responses received in the current Office Transfer Period.
_302	Peg Register	This register provides a count of the number of “302 Moved Temporarily” responses received in the current Office Transfer Period.
_303	Peg Register	This register provides a count of the number of “303 See Other” responses received in the current Office Transfer Period.
_304	Peg Register	This register provides a count of the number of “304 Warning” responses received in the current Office Transfer Period.
_305	Peg Register	This register provides a count of the number of “305 Use Proxy” responses received in the current Office Transfer Period.
_400	Peg Register	This register provides a count of the number of “400 Bad Request” responses received in the current Office Transfer Period.
_401	Peg Register	This register provides a count of the number of “401Unauthorized” responses received in the current Office Transfer Period.
_402	Peg Register	This register provides a count of the number of “402 Payment Required” responses received in the current Office Transfer Period.
_403	Peg Register	This register provides a count of the number of “403 Forbidden” responses received in the current Office Transfer Period.
_404	Peg Register	This register provides a count of the number of “404 Not Found” responses received in the current Office Transfer Period.
_405	Peg Register	This register provides a count of the number of “405 Method Not Allowed” responses received in the current Office Transfer Period.
_406	Peg Register	This register provides a count of the number of “406 Not Acceptable” responses received in the current Office Transfer Period.
_407	Peg Register	This register provides a count of the number of “407 Proxy

		Authentication Required" responses received in the current Office Transfer Period.
_408	Peg Register	This register provides a count of the number of "408 Request Timeout" responses received in the current Office Transfer Period.
_409	Peg Register	This register provides a count of the number of "409 Conflict" responses received in the current Office Transfer Period.
_410	Peg Register	This register provides a count of the number of "410 Gone" responses received in the current Office Transfer Period.
_411	Peg Register	This register provides a count of the number of "411 Length Required" responses received in the current Office Transfer Period.
_412	Peg Register	This register provides a count of the number of "412 Conditional Request Failed" responses received in the current Office Transfer Period.
_413	Peg Register	This register provides a count of the number of "413 Request Entity Too Large" responses received in the current Office Transfer Period.
_414	Peg Register	This register provides a count of the number of "414 Request-URI Too Long" responses received in the current Office Transfer Period.
_415	Peg Register	This register provides a count of the number of "415 Unsupported Media Type" responses received in the current Office Transfer Period.
_420	Peg Register	This register provides a count of the number of "420 Bad Extension" responses received in the current Office Transfer Period.
_423	Peg Register	This register provides a count of the number of "423 Interval Too Brief" responses received in the current Office Transfer Period.
_480	Peg Register	This register provides a count of the number of "480 Temporarily Unavailable" responses received in the current Office Transfer Period.
_481	Peg Register	This register provides a count of the number of "481 Call Or Transaction Does Not Exist" responses received in the current Office Transfer Period.
_482	Peg Register	This register provides a count of the number of "482 Loop Detected" responses received in the current Office Transfer Period.
_483	Peg Register	This register provides a count of the number of "483 Too Many Hops" responses received in the current Office Transfer Period.
_484	Peg Register	This register provides a count of the number of "484 Address Incomplete" responses received in the current Office Transfer Period.

_485	Peg Register	This register provides a count of the number of “485 Ambiguous” responses received in the current Office Transfer Period.
_486	Peg Register	This register provides a count of the number of “486 Busy Here” responses received in the current Office Transfer Period.
_487	Peg Register	This register provides a count of the number of “487 Request Terminated” responses received in the current Office Transfer Period.
_488	Peg Register	This register provides a count of the number of “488 Not Acceptable Here” responses received in the current Office Transfer Period.
_489	Peg Register	This register provides a count of the number of “489 Bad Event” responses received in the current Office Transfer Period.
_491	Peg Register	This register provides a count of the number of “491 Request Pending” responses received in the current Office Transfer Period.
_500	Peg Register	This register provides a count of the number of “500 Server Internal Error” responses received in the current Office Transfer Period. Note that this register is a call failure indication, and it has configurable thresholds for minor, major, and critical alarms.
_501	Peg Register	This register provides a count of the number of “501 Not Implemented” responses received in the current Office Transfer Period.
_502	Peg Register	This register provides a count of the number of “502 Bad Gateway” responses received in the current Office Transfer Period.
_503	Peg Register	This register provides a count of the number of “503 Service Unavailable” responses received in the current Office Transfer Period.
_504	Peg Register	This register provides a count of the number of “504 Server Timeout” responses received in the current Office Transfer Period.
_505	Peg Register	This register provides a count of the number of “505 Version Not Supported” responses received in the current Office Transfer Period.
_600	Peg Register	This register provides a count of the number of “600 Busy Everywhere” responses received in the current Office Transfer Period.
_603	Peg Register	This register provides a count of the number of “603 Decline” responses received in the current Office Transfer Period.
_604	Peg Register	This register provides a count of the number of “604 Does Not Exist Anywhere” responses received in the current Office Transfer Period.

_606	Peg Register	This register provides a count of the number of “606 Not Acceptable” responses received in the current Office Transfer Period.
Unknown 2xx	Peg Register	This register provides a count of the number of unrecognized 200-series responses received in the current Office Transfer Period.
Unknown 3xx	Peg Register	This register provides a count of the number of unrecognized 300-series responses received in the current Office Transfer Period.
Unknown 4xx	Peg Register	This register provides a count of the number of unrecognized 400-series responses received in the current Office Transfer Period.
Unknown 5xx	Peg Register	This register provides a count of the number of unrecognized 500-series responses received in the current Office Transfer Period.
Unknown 6xx	Peg Register	This register provides a count of the number of unrecognized 600-series responses received in the current Office Transfer Period.
Total	Peg Register	This register provides a count of the totals of all other registers in the row.

2.3.5 Thresholding and Alarms

There is a set of configurable thresholds for “500 Server Internal Error” responses. There are 3 configurable thresholds for each SIP transaction request type (row), representing minor, major, and critical alarms. The thresholds are configured via the Configuration Parameters entry for a network element in the management GUI. Each threshold indicates a percentage of total responses which are 500 responses. Threshold checking and alarm generation or clearing is performed at the end of each Office Transfer Period. If, when the threshold check is performed, the percentage of 500 responses reaches or exceeds one of the thresholds, an alarm of the corresponding type and severity will be raised. If an alarm was previously raised and the percentage of 500 responses falls below all configured thresholds when the threshold check is performed, the alarm will be retired automatically.

2.4 OM Group Name: SIP_Outbound_Response_Report

2.4.1 Affected NE

This OM group is common to all network elements.

2.4.2 Explanation

The SIP_Outbound_Response_Report OM group consists of a set of rows with each row containing and identical set of peg-registers. Each row corresponds to an incoming SIP request message and each register (column) corresponds to a SIP response type of an outgoing response. The registers count the number of SIP responses of the corresponding type that have been sent in response to incoming SIP request messages for the corresponding row type in the current Office Transfer Period. Additional SIP Response message details can be found in RFC-3261.

2.4.3 Row Descriptions

Table 4: SIP_Outbound_Response_Report Row Descriptions

Row Name	Type	Description
INFO	Set of Peg Registers	This row provides a set of peg-registers for the different response types for INFO transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming INFO transactions.
INVITE	Set of Peg Registers	This row provides a set of peg-registers for the different response types for INVITE transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming INVITE transactions.
MESSAGE	Set of Peg Registers	This row provides a set of peg-registers for the different response types for MESSAGE transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming MESSAGE transactions.
NOTIFY	Set of Peg Registers	This row provides a set of peg-registers for the different response types for NOTIFY transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming NOTIFY transactions.
OPTIONS	Set of Peg Registers	This row provides a set of peg-registers for the different response types for OPTIONS transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming OPTIONS transactions.
PUBLISH	Set of Peg Registers	This row provides a set of peg-registers for the different response types for PUBLISH transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming PUBLISH transactions.
REFER	Set of Peg Registers	This row provides a set of peg-registers for the different response types for REFER transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming

		REFER transactions.
REGISTER	Set of Peg Registers	This row provides a set of peg-registers for the different response types for REGISTER transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming REGISTER transactions.
SUBSCRIBE	Set of Peg Registers	This row provides a set of peg-registers for the different response types for SUBSCRIBE transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming SUBSCRIBE transactions.
UPDATE	Set of Peg Registers	This row provides a set of peg-registers for the different response types for UPDATE transactions. Each peg-register counts the number of responses of the specified type that have been sent in response to incoming UPDATE transactions.
[Totals]	Set of Peg Registers	This row is a set of totals of the other rows.

2.4.4 Register Descriptions

Each of the registers a in SIP_Outbound_Response_Report row counts the SIP response messages of the indicated type which have been sent in response to incoming SIP messages corresponding to the row type. For example, the _302 register in the INVITE row is a count of the number of 302 responses messages sent in response to incoming INVITE messages in the current Office Transfer Period.

Table 2: SIP_Outbound_Response_Report Register Descriptions

Register Name	Type	Description
_200	Peg Register	This register provides a count of the number of “200 OK” responses sent in the current Office Transfer Period.
_202	Peg Register	This register provides a count of the number of “202 Accepted” responses sent in the current Office Transfer Period.
_300	Peg Register	This register provides a count of the number of “300 Multiple Choices” responses sent in the current Office Transfer Period.
_301	Peg Register	This register provides a count of the number of “301 Moved Permanently” responses sent in the current Office Transfer Period.
_302	Peg Register	This register provides a count of the number of “302 Moved Temporarily” responses sent in the current Office Transfer Period.
_303	Peg Register	This register provides a count of the number of “303 See Other” responses sent in the current Office Transfer Period.

_304	Peg Register	This register provides a count of the number of “304 Warning” responses sent in the current Office Transfer Period.
_305	Peg Register	This register provides a count of the number of “305 Use Proxy” responses sent in the current Office Transfer Period.
_400	Peg Register	This register provides a count of the number of “400 Bad Request” responses sent in the current Office Transfer Period.
_401	Peg Register	This register provides a count of the number of “401Unauthorized” responses sent in the current Office Transfer Period.
_402	Peg Register	This register provides a count of the number of “402 Payment Required” responses sent in the current Office Transfer Period.
_403	Peg Register	This register provides a count of the number of “403 Forbidden” responses sent in the current Office Transfer Period.
_404	Peg Register	This register provides a count of the number of “404 Not Found” responses sent in the current Office Transfer Period.
_405	Peg Register	This register provides a count of the number of “405 Method Not Allowed” responses sent in the current Office Transfer Period.
_406	Peg Register	This register provides a count of the number of “406 Not Acceptable” responses sent in the current Office Transfer Period.
_407	Peg Register	This register provides a count of the number of “407 Proxy Authentication Required” responses sent in the current Office Transfer Period.
_408	Peg Register	This register provides a count of the number of “408 Request Timeout” responses sent in the current Office Transfer Period.
_409	Peg Register	This register provides a count of the number of “409 Conflict” responses sent in the current Office Transfer Period.
_410	Peg Register	This register provides a count of the number of “410 Gone” responses sent in the current Office Transfer Period.
_411	Peg Register	This register provides a count of the number of “411 Length Required” responses sent in the current Office Transfer Period.
_412	Peg Register	This register provides a count of the number of “412 Conditional Request Failed” responses sent in the current Office Transfer Period.
_413	Peg Register	This register provides a count of the number of “413 Request Entity Too Large” responses sent in the current Office Transfer Period.
_414	Peg Register	This register provides a count of the number of “414 Request-URI Too Long” responses sent in the current Office Transfer Period.
_415	Peg Register	This register provides a count of the number of “415 Unsupported Media Type” responses sent in the current Office Transfer Period.

_420	Peg Register	This register provides a count of the number of “420 Bad Extension” responses sent in the current Office Transfer Period.
_423	Peg Register	This register provides a count of the number of “423 Interval Too Brief” responses sent in the current Office Transfer Period.
_480	Peg Register	This register provides a count of the number of “480 Temporarily Unavailable” responses sent in the current Office Transfer Period.
_481	Peg Register	This register provides a count of the number of “481 Call Or Transaction Does Not Exist” responses sent in the current Office Transfer Period.
_482	Peg Register	This register provides a count of the number of “482 Loop Detected” responses sent in the current Office Transfer Period.
_483	Peg Register	This register provides a count of the number of “483 Too Many Hops” responses sent in the current Office Transfer Period.
_484	Peg Register	This register provides a count of the number of “484 Address Incomplete” responses sent in the current Office Transfer Period.
_485	Peg Register	This register provides a count of the number of “485 Ambiguous” responses sent in the current Office Transfer Period.
_486	Peg Register	This register provides a count of the number of “486 Busy Here” responses sent in the current Office Transfer Period.
_487	Peg Register	This register provides a count of the number of “487 Request Terminated” responses sent in the current Office Transfer Period.
_488	Peg Register	This register provides a count of the number of “488 Not Acceptable Here” responses sent in the current Office Transfer Period.
_489	Peg Register	This register provides a count of the number of “489 Bad Event” responses sent in the current Office Transfer Period.
_491	Peg Register	This register provides a count of the number of “491 Request Pending” responses sent in the current Office Transfer Period.
_500	Peg Register	This register provides a count of the number of “500 Server Internal Error” responses sent in the current Office Transfer Period. Note that this register is a call failure indication, and it has configurable thresholds for minor, major, and critical alarms.
_501	Peg Register	This register provides a count of the number of “501 Not Implemented” responses sent in the current Office Transfer Period.
_502	Peg Register	This register provides a count of the number of “502 Bad Gateway” responses sent in the current Office Transfer Period.
_503	Peg Register	This register provides a count of the number of “503 Service Unavailable” responses sent in the current Office Transfer Period.

_504	Peg Register	This register provides a count of the number of “504 Server Timeout” responses sent in the current Office Transfer Period.
_505	Peg Register	This register provides a count of the number of “505 Version Not Supported” responses sent in the current Office Transfer Period.
_600	Peg Register	This register provides a count of the number of “600 Busy Everywhere” responses sent in the current Office Transfer Period.
_603	Peg Register	This register provides a count of the number of “603 Decline” responses sent in the current Office Transfer Period.
_604	Peg Register	This register provides a count of the number of “604 Does Not Exist Anywhere” responses sent in the current Office Transfer Period.
_606	Peg Register	This register provides a count of the number of “606 Not Acceptable” responses sent in the current Office Transfer Period.
Unknown 2xx	Peg Register	This register provides a count of the number of unrecognized 200-series responses sent in the current Office Transfer Period.
Unknown 3xx	Peg Register	This register provides a count of the number of unrecognized 300-series responses sent in the current Office Transfer Period.
Unknown 4xx	Peg Register	This register provides a count of the number of unrecognized 400-series responses sent in the current Office Transfer Period.
Unknown 5xx	Peg Register	This register provides a count of the number of unrecognized 500-series responses sent in the current Office Transfer Period.
Unknown 6xx	Peg Register	This register provides a count of the number of unrecognized 600-series responses sent in the current Office Transfer Period.
Total	Peg Register	This register provides a count of the totals of all other registers in the row.

2.4.5 Thresholding and Alarms

Not Applicable.

2.5 OM Group Name: SIP_Transaction_Report

2.5.1 Affected NE

This OM group is common to all network elements.

2.5.2 Explanation

The SIP_Transaction_Report OM group consists of a set of rows with each row containing and identical set of peg-registers. Each row corresponds to an incoming or outgoing SIP transaction. There are two registers (columns) indicating the direction of transaction and a register indicating the current number of transactions which are currently active.

2.5.3 Row Descriptions

Table 5: SIP_Transaction_Report Row Descriptions

Row Name	Type	Description
ACK	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active ACK transactions.
BYE	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active BYE transactions.
CANCEL	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active CANCEL transactions.
INFO	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active INFO transactions.
INVITE	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active INVITE transactions.
MESSAGE	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active MESSAGE transactions.
NOTIFY	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active NOTIFY transactions.
OPTIONS	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active OPTIONS transactions.
PRACK	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active PRACK transactions.
PUBLISH	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active PUBLISH transactions.
REFER	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound,

		and currently active REFER transactions.
REGISTER	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active REGISTER transactions.
SUBSCRIBE	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active SUBSCRIBE transactions.
UPDATE	Two Peg Registers and one Usage Register	This row provides a set of registers indicating the number of inbound, outbound, and currently active UPDATE transactions.
[Totals]	Two Peg Registers and one Usage Register	This row is a set of totals of the other rows.

2.5.4 Register Descriptions

Each row in SIP_Transaction_Report contains two peg registers and one usage register. The registers are described in the SIP_Transaction_Report Register Descriptions table below.

Table 2: SIP_Transaction_Report Register Descriptions

Register Name	Type	Description
Inbound	Peg Register	This register provides a count of the number of SIP transactions of the corresponding row type which have been initiated by incoming message in the current Office Transfer Period.
Outbound	Peg Register	This register provides a count of the number of SIP transactions of the corresponding row type which have been initiated by incoming message in the current Office Transfer Period.
Active	Usage Register	This register provides a count of the currently active transactions of the corresponding row type. Each time a transaction is initiated by an incoming or outgoing message, this counter is incremented. Each time the transaction is concluded by the sending or receiving of a response message, this counter is decremented.

2.5.5 Thresholding and Alarms

Not Applicable.

2.6 OM Group Name: CPCheckpoint

2.6.1 Affected NE

Session Manager.

2.6.2 Explanation

This OM group is a usage counter on the inactive session Manager. It tracks the number of calls that the inactive session manager is checkpointing. In the event of a failover these calls will survive the failover. On the active node this counter is always 0. It is only tracking checkpointed calls on the hot standby instance.

2.6.3 Register Descriptions

Table 6: DB Register Descriptions

Register Name	Type	Description
CallP Checkpoint	Usage	Counts the current number of checkpointed calls.

2.6.4 Thresholding and Alarms

Not Applicable.

2.7 OM Group Name: Presence_Event_Report

2.7.1 Affected NE

This OM group is associated with the SESM only.

2.7.2 Explanation

The Presence Event Report OM group tracks the behavior of the various presence events that are processed by the SESM. Each of the rows in the report represents one of the eight presence event types as well as a total row.

Here is a brief description of the various presence events:

- Activity – A client has indicated that it has detected user activity (keyboard/mouse).
- End Call – A client has ended a call (excludes collaboration sessions).
- Inactive – A client has indicated that it has not detected user activity (keyboard/mouse) for an extended period of time.

- Login – A client has logged into the SESM.
- Logout – A client has logged out from the SESM.
- Manual – A client has indicated a presence state change through manual intervention (user interaction with the client interface).
- New Call – A client has entered into a stable call (excludes collaboration sessions).

2.7.3 Register Descriptions

Table 7: Presence Event Report Register Descriptions

Register Name	Type	Description
Created	Counter	The number of events of that type that have been created in the system. This gives the operator an idea of the relative frequency of occurrence for that presence event type.
Processed	Counter	The number of events of that type that have been processed by the presence event processor. Just because a presence event is created does not mean that it is guaranteed to ever be processed. It may be eliminated from consideration because of an opposing presence event (see optimized register).
Optimized	Counter	The number of events of that type that have been optimized by the presence vent processor. An event is optimized when an opposing presence vent is processed that nullifies the presence vent change that would have taken place. For instance, if a new call event is processed and the presence event processor sees that there is an opposing end call event in the queue or parked, then there is no further point in processing either event. The two events cancel each other out.
Queued	Usage	The number of events that are currently in the presence event processor queue waiting to be processed. This OM represents a snapshot view of the current presence event queue depth.
Parked	Usage	The number of events that have been initially processed, but must wait for the presence guard timer to expire before being processed. These events are “parked” waiting for the guard timer to expire. When the guard timer expires, they re-enter the presence event queue (which **does not** cause a second pegging of the processed counter for that event).

2.7.4 Thresholding and Alarms

Not Applicable.

2.8 OM Group Name: SyncSystem

2.8.1 Affected NE

This OM group is common to all network elements.

2.8.2 Explanation

The SyncSystem OM group tracks the processing of synchronization checkpoints between two synchronization peers. One peer is the checkpoint sender containing information to be checkpointed. The other is the checkpoint receiver requesting that information in order to be able to replicate the relevant state of the sender. Each peer group is collectively known as a "Sync System", Examples of a sync system include:

- The two network element instances in a fault tolerant pair. The checkpoint sender is the active instance and the checkpoint receiver is the synchronizing/hotStandby instance. The checkpoints contain call information.

- A network element instance and the fault processing manager (SM or FPM) to which the instance's alarms are sent[1]. The checkpoint sender is the network element instance, and the checkpoint receiver the fault processing manager. The checkpoints contain alarm information.

Each sync system has two rows, one corresponding to the sender and the other to the receiver, only one of which is used at a given point in time depending on the role of the network element (i.e. sender or receiver) in the sync system. The rows follow this naming convention:

- "<SyncSystemName>:send" for the sender row. For example "FaultTolerance:send".

- "<SyncSystemName>:recv" for the sender row. For example "FaultTolerance:recv".

2.8.3 Register Descriptions

Table 8: SyncSystem Register Descriptions

Register Name	Type	Description
checkpointGenerators	Usage	Number of entities capable of generating checkpoints.
checkpointsSent	Counter	Number of checkpoints sent.
receiverLag	Usage	Measure of how far behind the checkpoint

[1] Note that a fault processing manager reports its own alarms to itself via an internal mechanism, not via checkpoints.

		receiver is receiving checkpoints relative to how quickly the checkpoint sender is sending them.
processedLag	Usage	Measure of how far behind the checkpoint receiver is processing checkpoints relative to how quickly it's receiving them.

2.8.4 Thresholding and Alarms

Not Applicable.

2.9 OM Group Name: HALayer

2.9.1 Affected NE

This new OM group is only applicable to the new IBM BladeCenter-T based RTP Media Portal.

2.9.2 Explanation

The new BladeCenter-T RTP Media Portal supports all traditional RTP Media Portal functions – and introduces support for the clustering of RTP Media Portals into "N+1" fault tolerant service clusters (i.e. "N" active instances, and "1" standby). As a result, the new BladeCenter-T RTP Media Portal and the traditional CPX8216-T RTP Media Portal are identical from a functional perspective but very different conceptually:

- the CPX8216-T RTP Media Portal is comprised of software and hardware components having a static relationship.
- the BladeCenter-T "N+1" RTP Media Portal Service Cluster is comprised of a set of logical Service Instances ("N" active instances of RTP Media Portal that actively process calls) that "float" over a predefined set of underlying physical hardware (the Service Nodes). There is no fixed relationship between an active RTP Media Portal Service Instance and its hosting hardware. This allows very robust handling of failures as Service Instances can fail and be quickly re-instantiated on another available piece of hardware.

The software sub-component that provides the fault tolerance mechanisms (heartbeating, checkpointing, failure detection,…) supporting the "N+1" RTP Media Portal Service Cluster is the High Availability Layer (HAL). The new

HALayer OM Group gathers statistics on the performance of these underlying fault tolerance mechanisms.

2.9.3 Register Descriptions

Table 9: HALayer Register Descriptions

Register Name	Type	Description
statusCnt	Meter	Number of internal status change events generated by the Fault-tolerance mechanisms on this Service Node.
updateCnt	Meter	The number of Service Instances that have joined the Service Cluster (from the perspective of this service node).
chkPointsRcvd	Meter	Number of checkpoints received by this Service Node.
chkPointsSent	Meter	The number of checkpoints sent by this Service Node.
activeInstances	Meter	Number of active Service Instances in the Service Cluster associated with this Service Node.
standbyInstances	Meter	The number of standby Service Instances in the Service Cluster associated with this Service Node.

2.9.4 Thresholding and Alarms

Not Applicable.

3 OM Groups Modified

The OM Groups in this section have been modified for this release

3.1 OM Group Name: Emergency

3.1.1 Affected NE

This OM Group is applicable to SESM

3.1.2 Explanation

This OM Group was modified to add the “operatorCallbackAttempt”, “operatorCallbackConnected”, “operatorConnectFailure” counters.

3.1.3 Register Descriptions

Table 3: Emergency Register Descriptions

Register Name	Type	Description
operatorCallbackAttempt	Counter	This OM is pegged when the E911 emergency operator attempts to callback the originating (enterprise) caller. This OM is not pegged for residential operator callback attempts.
operatorCallbackConnected	Counter	This OM is pegged when the E911 emergency operator established voicepath with the originating (enterprise) caller. This OM is not generated for residential operator callbacks.
operatorConnectFailure	Counter	This OM is pegged when a PSAP connect failure is detected while attempting to establish an emergency call. Connection failure scenarios include: no answer timeout, busy trunks or gateway unavailable.

3.2 OM Group Name: PRESENCE

3.2.1 Affected NE

This OM Group is associated with the SESM only.

3.2.2 Explanation

This OM Group was modified to add two registers: throttleNotifySelfOnly and throttleNotifyAll. These registers track interactions between the presence service and overload controls on the SESM.

3.2.3 Register Descriptions

Table 10: Presence Register Descriptions

Register Name	Type	Description
throttleNotifySelfOnly	Counter	This OM is pegged every time the system does not send out notifications to non-self subscriptions because of a presence state change during minor overload. This is pegged once for the entire state change, and does not reflect the actual number of NOTIFY messages that were not sent out.
throttleNotifyAll	Counter	This OM is pegged every time the system does not send out any notifications, including self-subscriptions because of a presence state change during major or severe overload. This is pegged once for the entire state change, and does not reflect the actual number of NOTIFY messages that were not sent out.

4 OM Groups Deleted

The OM Groups in this section have been deleted in this release.

4.1 OM Group Name: <name>

4.1.1 Affected NE

This OM Group was applicable to <xxx>.

4.1.2 Explanation

This OM Group was deleted due to <xxx>.

(I)SN09 OSS Guide

Advance Feature Guide

Publication number: PLN-i09-OSS
Product release: (I)SN09
Document release: Standard 01.04
Date: January 2006
United States of America

NORTEL NETWORKS™

How the world shares ideas.