

# Disaster Recovery

## What's new in this release

The table [\(I\)SN09 features](#) highlights the features introduced in this release. Refer to the OSS Advanced Feature Guide for more information about new features in this release.

**Table 1 (I)SN09 features**

Feature descriptions
A00012210 -- SPFS09 - GEO: REMOTE CLONING FOR STANDBY NODE (UA-IP)  This Automatic Backup and Accelerated restore feature, 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).





# Disaster Recovery

---

## Overview

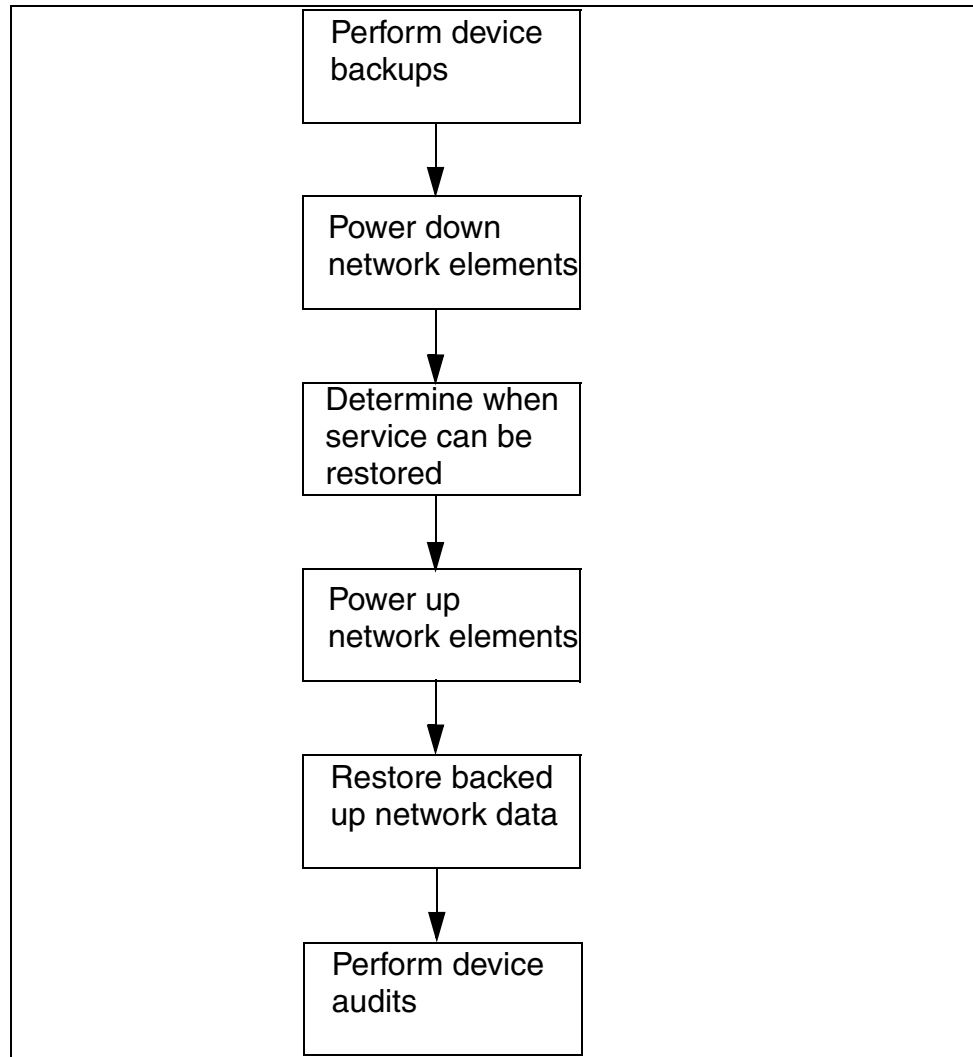
This document provides an overview of the Disaster Recovery process for Carrier Voice over IP solutions. A disaster is defined as one of the following events:

- fire
- flood
- lightning storm
- explosion
- tornado
- earthquake
- hurricane
- terrorism
- any other incident causing damage beyond normal repair to telecommunications facilities

This document should be used to restore communication capability within the affected central office or network.

## Disaster Recovery process

The following figure illustrates the general order for Disaster Recovery.

**Figure 1 Disaster Recovery flowchart**

### Power conservation

Several components in this document can be partially powered down to conserve power but keep the network in an operational state. These procedures typically involve powering down inactive or spare units or keeping only a certain set of hardware or cards active. The following

table lists the components covered in this document and what type(s) of power procedures are available.

**Table 1 Power procedures**

Component or network element	Full	Partial
XA-Core	X	X
Ethernet Routing Switch 8600	X	X
SDM (CS 2000 Core Manager)	X	
Netra t1400	X	
Netra N240	X	X
Border Control Point	X	
Services Application Module Frame (SAMF)	X	
Call Control Frame (CCF)	X	
USP	X	X
Media Gateway/Multiservice Switch 15000	X	X
Media Gateway/Multiservice Switch 7480	X	
MDM	X	
SPM	X	X
MCS	X	
Border Control Point Manager	X	
Media Server 2000 Series	X	
UAS	X	
MG 9000	X	X

When a partial power down is performed for a component, the corresponding partial power down recovery procedure should be followed. Do not use a partial power down recovery procedure to

recover from a full power down. Conversely, do not use a full power down recovery procedure to recover from a partial power down.

**Note:** Recovery from a partial power down of the MG 9000 is performed using the same procedure as recovery from a full power down.

## Backup and restore

Backup and restore operations for Succession solutions are performed at the component level. They are performed on the components at different intervals during periods of low service activity. No provisioning or configuration changes are to be made during the backup and restore window.

### ATTENTION

Back up all related devices in the solution during the same window of time. No changes are allowed to any related devices during this period until all backups are completed or those changes will not be captured as part of the coordinated backup and would be lost in case of the need to restore the system. For example, the CS 2000, CS 2000 GWC Manager, and MG 9000 Manager all share line service data and must be backed up in the same window.

Correspondingly all related devices need to be restored together to return the system to a known state. No changes are allowed to the system until the restoration is completed or data mismatches will result.

## Backup operations

There are two types of backup operations for components of Succession solutions: service data backup and fileset level backup.

Service data backup is typically performed once per day during a period of low activity. The following table lists components which are typically backed up using a service data backup.

### Service data backup components

Component	Procedure (s)	Page
NETWORK INTELLIGENCE		
CS 2000	<a href="#">How to backup an XA-Core office image from disk to tape</a>	<a href="#">99</a>
Call Agent	<a href="#">Call Agent backup</a> <a href="#">Backing up files to DVD-RW</a>	<a href="#">109</a> <a href="#">113</a>
SAM21	none (See <a href="#">Note 1</a> )	
GWC	none (See <a href="#">Note 1</a> )	

**Service data backup components**

Component	Procedure (s)	Page
Session Server	<a href="#">Session Server - Trunks backup</a> <a href="#">Starting or stopping the automated synchronous backup</a> <a href="#">restore manager service</a>	<a href="#">123</a> <a href="#">91</a>
Ethernet Routing Switch 8600	<a href="#">Saving the Ethernet Routing Switch 8600 boot configuration file</a>	<a href="#">129</a>
UAS	<a href="#">Backing up UAS configuration files</a>	<a href="#">131</a>
MS 2000 Series	Displaying the MS 2000 Series node configuration: <a href="#">Configuring automated INI file backups</a> <a href="#">Changing the SNMP community string password for a Media Server 2010 node</a> <a href="#">Changing the SNMP community string password for a Media Server 2020 node</a> <b>Backing up all MS 2000 Series node INI files:</b> <a href="#">Backing up INI files for all nodes</a> <b>Configuring the MS 2000 Series CLUI tool:</b> <a href="#">Displaying Media Server 2010 node current configuration</a> <a href="#">Displaying Media Server 2020 node current configuration</a>	<a href="#">135</a> <a href="#">137</a> <a href="#">141</a> <a href="#">145</a> <a href="#">147</a> <a href="#">151</a>
APS	<a href="#">Backing up the APS-specific Oracle database and application files</a>	<a href="#">155</a>
USP	<a href="#">USP OAM&amp;P Workstation Backup</a>	<a href="#">159</a>
Real-time Transport Protocol (RTP) Media Portal	RTP Media Portal Basics, NN10367-111	
CICM	CICM Security and Administration, NN10252-611	
CORE NETWORK		
Multiservice Switch or Media Gateway devices	<a href="#">Backing up a Multiservice Switch or Media Gateway device</a>	<a href="#">163</a>
GATEWAYS		
MG 9000	none (See <a href="#">Note 1</a> )	
MG 4000	none (See <a href="#">Note 2</a> )	



**Service data backup components**

<b>Component</b>	<b>Procedure (s)</b>	<b>Page</b>
IW SPM	none (See <a href="#">Note 2</a> )	
NETWORK MANAGEMENT		
CS 2000 Core Manager CBM	<a href="#">Starting or stopping the automated synchronous backup restore manager service</a>	91
Core Element Manager	<a href="#">Starting or stopping the automated synchronous backup restore manager service</a>	91
CS 2000 Management Tools	<a href="#">Performing a backup of oracle data on an SSPFS-based server</a>	173
	<a href="#">Performing a backup of file systems on an SSPFS-based server</a>	179
	<a href="#">Starting or stopping the automated synchronous backup restore manager service</a>	91
Integrated Element Management System	<a href="#">Performing a backup of oracle data on an SSPFS-based server</a>	173
	<a href="#">Performing a backup of file systems on an SSPFS-based server</a>	179
	<a href="#">Starting or stopping the automated synchronous backup restore manager service</a>	91
IEMS centralized security server	<a href="#">Backing up the central security server on page 183</a>	183
	<a href="#">Backing up an SSPFS-based security client on page 185</a>	185
MG 9000 Manager	<a href="#">Performing a backup of oracle data on an SSPFS-based server</a>	173
	<a href="#">Performing a backup of file systems on an SSPFS-based server</a>	179
	<a href="#">Starting or stopping the automated synchronous backup restore manager service</a>	91

## Service data backup components

Component	Procedure (s)	Page
MDM	none (See <a href="#">Note 3</a> )	
<p><b>Note 1:</b> Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures.</p> <p><b>Note 2:</b> Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up.</p> <p><b>Note 3:</b> MDM backups are performed by copying the files to tape or an off box storage system through UNIX commands or CRON jobs.</p> <p><b>Note 4:</b> A script purgeTempData.sh is provided in the /opt/nortel/iems/current/bin directory. This script will purge all event, alarm and performance data from the IEMS database. After purging the data it can't be retrieved. It deletes all events, alarms and performance data. To reduce the time taken to backup/restore, a user must stop the IEMS server and execute the purgeTempData.sh script to purge the events, alarms and performance data from the database.</p>		

Fileset level backups back up the software as well as configuration data. This type of backup is performed after hardware changes, software updates or patches, or major reconfigurations. Fileset backup also need to be performed before a major upgrade. The following table provides a list of components with fileset level backup procedures.

## Fileset level backup components

Component	Procedure (s)	Page
NETWORK INTELLIGENCE		
GWC	<a href="#">Create a backup of the GWC load file</a>	<a href="#">187</a>
USP	<a href="#">USP Backup</a>	<a href="#">189</a>
GATEWAYS		
Multiservice Switch or Media Gateway devices	<a href="#">Backing up a Multiservice Switch or Media Gateway device</a>	<a href="#">163</a>

## Fileset level backup components

Component	Procedure (s)	Page
NETWORK MANAGEMENT		
CS 2000 Core Manager or CBM	<a href="#">Creating system image backup tapes (S-tapes) manually</a>	<a href="#">191</a>
	<a href="#">Configuring SBA backup volumes on the core</a>	<a href="#">221</a>
USP Manager	<a href="#">Creating USP Disaster Recovery Floppy Disks</a>	<a href="#">307</a>

### Frequency of backup operations

The following table lists each component along with how often backup operations are recommended to be performed.

### Component backup frequency

Component	Backup Frequency
NETWORK INTELLIGENCE	
CS 2000	Weekly
Call Agent	Weekly
SAM21	See <a href="#">Note 1</a>
GWC	See <a href="#">Note 1</a>
CS 2000 CS LAN	Full backup - monthly, and prior to all migrations and patch operations and configuration changes
UAS	Daily
MS 2000 Series	Daily
APS	Daily
RTP Media Portal	Daily
CICM	Daily
USP	Full system backup - once a week Modified (differential) backup - once a day

**Component backup frequency**

<b>Component</b>	<b>Backup Frequency</b>
CORE NETWORK	
Multiservice switches	Full backup - monthly, and prior to all migrations and patch operations
GATEWAYS	
MG 9000	See <a href="#">Note 1</a>
MG 4000	See <a href="#">Note 2</a>
IW SPM	See <a href="#">Note 2</a>
NETWORK MANAGEMENT	
CS 2000 Management Tools	Daily
MG 9000 Manager	Daily
IEMS	Daily
MDM	Full backup - monthly, and prior to all migrations and patch operations Incremental backup - weekly
<p><b>Note 1:</b> Service data from the SAM21, GWC, and MG 9000 is not backed up locally. It is backed up at the manager. The manager is backed up to tape using CS 2000 Core Manager or CS 2000 Management Tools procedures.</p> <p><b>Note 2:</b> Service data from the IW SPM and MG 4000 is automatically backed up when the CS 2000 is backed up.</p>	

---

## Synchronized Backup Manager overview

---

### Synchronized Backup Manager description

Throughout this document, the backup restore functionality delivered under this feature is referred to in three distinct ways:

- Synchronous Backup Restore Manager (SBRM) refers specifically to the IEMS launched synchronized backup/restore software. The SRBM controls/synchronizes the backup related activities across other components/devices which contain related backup software.
- Device Backup Restore Manager (DBRM) refers specifically to the component-/device-level backup software which is controlled by the SBRM.
- Backup Restore Manager is a generic term encompassing both SBRM and DBRM functionalities and in general simply refers to the software which is common to both.

The feature provides a centralized mechanism that allows the user to initiate a synchronous backup for the core components of the CVoIP Call Server. Providing this capability reduces the possibility of error caused by manual backup procedures on the various component platforms spread across the Call Server solution.

From (I)SN08, the Backup Manager provides synchronous centralized control of the backup functionality resident within the following Call Server components

- CS 2000 Management Tools (CSMT) server
- MG9000 Manager (MG9K) server
- Supernode Data Manager (SDM) / Core Billing Manager (CBM) server. The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. no SDM/CBM data is backed up via the Backup Restore Manager software.
- Integrated Element Management System (IEMS) server

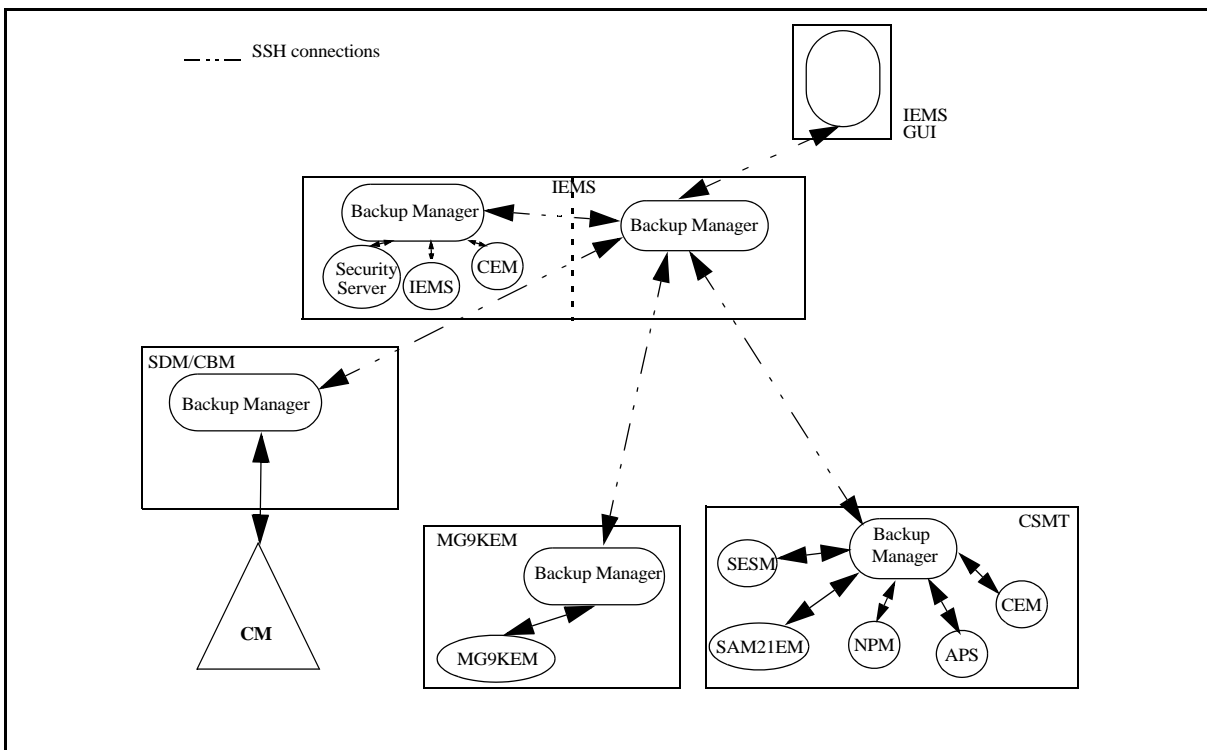
**Note:** The IEMS may reside with the CSMT (and other applications) on the CSMT server.

From the IEMS GUI, the user launches the SBRM command line interface and initiates a backup for the core components of the CVoIP Call Server. The SBRM receives the user request, and subsequently initiates a backup command sequence (using CLI commands over SSH) to execute a synchronous backup of the components. Once the

backup is complete, the backup files are stored locally on each component.

The following figure shows a high-level functional overview of the SBRM.

### High-level functional overview of the SBRM



### Sequence of events to run the Synchronized Backup Manager

The component onto which the SBRM is being installed determines the sequence of events.

#### Installing and configuring SBRM on the SDM

To install and configure the Synchronized Backup Manager (SBRM) on the SDM, the following steps are required:

1. To install the Backup Restore Manager on the SDM, refer to procedure, [Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager on page 21](#).
2. To configure the bkmgrusr user ID and password on the SDM, refer to procedure, [Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM on page 69](#).

3. To configure SSH between the backup manager restore servers, refer to procedure, [Configuring SSH between the backup restore manager servers on page 77](#).
4. To configure core access for the SBRM through the SDM, refer to procedure, [Configuring core access for SBRM through the CS 2000 Core Manager on page 71](#).
5. To create the backup user ID on the core for SBRM, refer to procedure, [Creating the backup user ID on the core for SBRM on page 73](#).
6. To configure automated execution of backups, refer to procedure, [Configuring the automated synchronous backup restore manager service on page 85](#).
7. Configure the specific Backup Restore Manager installations, setting the appropriate properties for the SBRM which resides in the IEMS and the individual component-level Backup Restore Managers which reside in the other platforms (for example, the CSMT and SDM).
8. Complete the common procedures for all components on page [16](#).

### **Installing and configuring SBRM on the CBM 850**

To install and configure the Synchronized Backup Manager (SBRM) on the CBM 850, the following steps are required:

1. To install the Backup Restore Manager on the CBM 850, refer to procedure, [Installing optional software on a CBM 850 on page 29](#).  
  
**Note:** No special configuration is required whilst performing this operation.
2. To configure SSH between the backup manager restore servers, refer to procedure, [Configuring SSH between the backup restore manager servers on page 77](#).
3. To configure core access for SBRM through the CBM 850, refer to procedure [Configuring core access for SBRM through the CBM 850 on page 75](#).
4. To create the backup user ID on the core for SBRM, refer to procedure, [Creating the backup user ID on the core for SBRM on page 73](#).
5. Complete the common procedure for all components in this section on page [16](#).

### Common procedures for all components

The following procedures are required in order to configure the SBRM on all components.

- To configure SSH between the backup manager restore servers (if not already completed), refer to procedure, [Configuring SSH between the backup restore manager servers on page 77](#).

The following sections provide additional information regarding the SBRM:

- To configure automated execution of backups, refer to procedure, [Configuring the automated synchronous backup restore manager service on page 85](#).
- To control the automated execution of backups, refer to procedure, [Starting or stopping the automated synchronous backup restore manager service on page 91](#).

To configure the IEMS to support the SRBM, refer to the following procedures:

- To add the SBRM to the IEMS using the Java Web Start Client, refer to procedure, “Adding a Synchronized Backup Restore Manager application (SBRM application)” in *IEMS Configuration Management*, NN10330-511.
- To add the SBRM to the IEMS using the web client, refer to procedure, “Adding an SBRM application” in *IEMS Configuration Management*, NN10330-511.
- To launch the CLI for the SBRM using the IEMS Java Web Start Client, refer to the procedure, “Launching CLI for SBRM application” in *IEMS Basics*, NN10329-111. The SBRM cannot be launch using the IEMS web client.

A network backup (that is, where several components are backed up at once) is invoked from the IEMS Backup Manager. In rare instances, it may be necessary to run various portions of the backup process on individual components/servers themselves. This capability is implemented as a CLUI interface, as in the following section.



## Execution of a backup at the component-level

### ATTENTION

Execution of a backup at the component-level should be used only in rare circumstances. Care should be taken to keep the SBRM and the DBRM in sync.

The CLUI interface to perform a backup at the component-level can be invoked by logging into the appropriate component via a Telnet session. Refer to procedure, [Invoking the synchronous backup restore manager through telnet on page 95](#).

## Hardware and software requirements

Backup Restore Manager functionality requires that the appropriate software is resident and configured in all platforms which require synchronized imaging. The Backup Restore Manager software itself is included in various platform software packages, including the SPFS and SDM. SPFS Backup Restore Manager functionality is used for integration of Call Server Management Tools (CSMT), the Media Gateway 9000 Element Manager (MG9KEM), the IEMS, and the CBM. The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.

## Requirements and restrictions

The following requirements and restrictions apply to Synchronized Backup Manager functionality from (I)SN08:

- All platforms requiring Backup Manager software functionality must be Java compatible and must provide a resident Java runtime system.
- Restore of generated synchronized backup images is not supported in the SBRM software. Existing manual restore procedures must be followed in order to utilize the backup images produced by the Backup Restore Manager.
- The Backup Restore Manager system does not perform automatic spooling of backup data/image files to secure/redundant servers. Customers are required to manage their own secure server archiving capabilities. The Backup Restore Manager system will

publish data/image files in pre-determined/configurable directories on various servers:

- SPSF Platform data/image file location: /data/bkresmgr/backup.
- XACore/3PC data/image file location: Configurable

- Backup of program store and associated patches is not covered as part of the functionality associated with Synchronous Backup Restore Manager. If a customer needs to completely 'restore' a server/component, they will need to reinstall their applications and reapply the associated patches.
- The backup "abort" command may require manual cleanup/removal of some backup files. The user will be notified at "abort" command completion time if this is the case.
- The backup process itself cannot be executed while certain constructive/destructive system audits are in progress (e.g. SESM's CS 2000 Data Integrity Audit). In general, if a backup is attempted while these audits are in progress, the backup attempt will be rejected. However, some constructive/destructive audits will be postponed when a backup request is received (e.g. MG9KEM Network Element Audit). The architecture of the system in question determines the appropriate behavior. In general, any system rejections of the backup request will result in an appropriate message being displayed to the Synchronous Backup Restore Manager client user.
- No system wide coordination between Synchronous Backup Restore Manager and other applications (e.g. UpgradeManager, CS 2000 Audits, CM dump scheduling, etc.) is delivered. All application activity interdependencies must be manually managed by the user. For example, scheduled activities such as audits should be stopped during system backup. Also, any automated CM image dumps should be cancelled since the Synchronous Backup Restore Manager will be used to drive the dump within a synchronized system wide backup window.
- APS and NPM queries will be disallowed during backup. This is due to the applications being shut down during backup. Active clients will be informed of the application shutdown.
- Backup of the MG 9000 EM in isolation is not recommended due the CSMT platform data dependency. The MG 9000 EM database is hosted on the CSMT server.
- Synchronous Backup Restore Manager user authorization only controls the launch of the CLI. CLI Command specific authorization is not provided, therefore only users authorized to actually launch the Synchronous Backup Restore Manager CLI will be allowed to

perform query commands at the Synchronous Backup Restore Manager CLI.

- The software on the SDM/CBM acts only to allow control of the XACore/3PC backup. No SDM/CBM data is backed up via the Backup Restore Manager software.

During the period when the backup is executing, user's of the various GUI and command line provisioning interfaces will be restricted from attempting actions which result in configuration and provisioning data changes. These restrictions include the following:

- Adding/deleting/updating GWCs at the Call Server Management Tools (CSMT) GUI or OSSGate interface.
- Adding/deleting/updating line service at the at the CSMT OSSGate interface.
- Manually invoking (or running via the scheduler) the various audits at the CSMT GUI.
- Adding/deleting/updating objects in the Integrated Element Management Server (IEMS) topology via the IEMS client.
- Adding/modifying collection jobs via the IEMS client.
- Using the Runtime Administration interface at the IEMS client to perform OSS configuration.
- Using the Security Administration interface at the Integrated client to add/delete Users/Groups/Operations.
- Using the Security Administration interface at the IEMS client to change a user password.
- Adding/deleting/updating Trunks/Carriers via the CSMT.
- Node provisioning/deprovisioning via the SAM21Manager.
- ATM connection set provisioning/deprovisioning via the SAM21 Manager.



## Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager

### Purpose

Use this procedure to install and configure the Backup Restore Manager application on the CS 2000 Core Manager

### Application

The Backup Restore Manager application functionality requires the appropriate software resident and configured on platforms that require synchronized imaging. Although no CS 2000 Core Manager data is backed up through the Backup Restore Manager, the Backup Restore Manager software must be installed on the CS 2000 Core Manager to allow control of the XA-core and 3PC (Compact) backup.

### Prerequisites

You must be a user authorized to perform config-admin actions.

Before executing this procedure, ensure that a user name and password used for logging into the core to initiate an image dump is created and enabled. For assistance refer to procedure, "Creating the backup user ID on the core for SBRM" in CS 2000 Core Manager Configuration Management, NN10104-511, or in ATM/IP Solution-level Security and Administration, NN10402-600.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Other activities related to using this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN10170-611
Displaying actions a user is authorized to perform	CS 2000 Core Manager Security and Administration, NN10170-611

## Procedures

### ATTENTION

Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

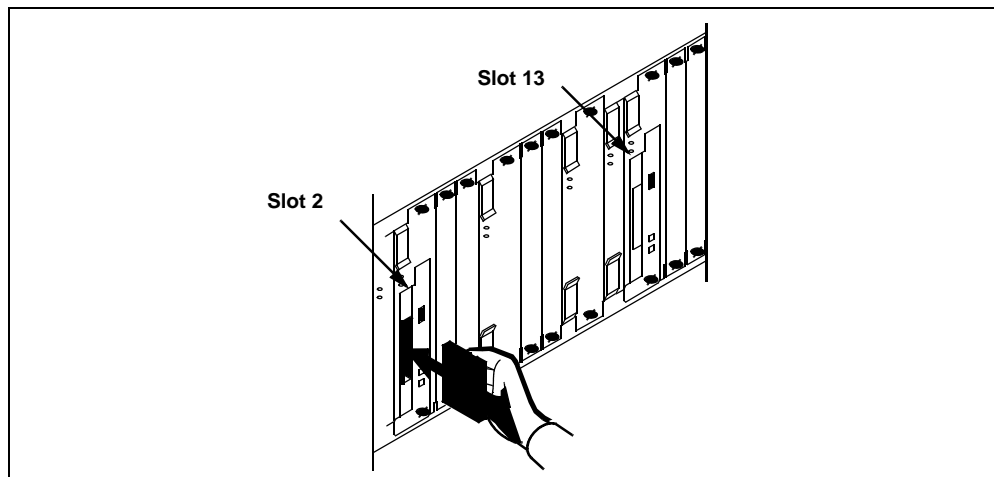
Use the following table to determine the correct procedure to use.

If	Do
you are installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager for the first time	procedure <a href="#">Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager</a>
you are only reconfiguring the user name and password for an existing Backup Restore Manager application on the Core Manager	procedure <a href="#">Reconfiguring the Backup Restore Manager application on the CS 2000 Core Manager on page 26</a>

### Installing and configuring the Backup Restore Manager application on the CS 2000 Core Manager

#### *At the CS 2000 Core Manager*

- 1 Insert the tape for the software load into one of the tape drives (slot 2 or slot 13) of the main chassis, as shown in the following figure. Wait until the tape drive stabilizes (yellow LED is off) before you proceed.



### ***At the maintenance interface***

- 2 Determine the installation method.

If you choose to install OM Data Delivery by	Do
logging onto a local VT100 terminal connected to the CS 2000 Core Manager	log on to the CS 2000 Core Manager as a user authorized to perform config-admin actions at the VT-100 terminal, and go to step <a href="#">6</a>
using telnet from a remote UNIX workstation to the CS 2000 Core Manager	step <a href="#">3</a>

- 3 Open a VT-100 compatible terminal window at the remote UNIX workstation.
- 4 Log onto the CS 2000 Core Manager from the terminal window prompt:
 

```
telnet <ip_address>
```

 where
 

```
<ip_address>
```

 is the IP address of the CS 2000 Core Manager you want to install the Backup Restore Manager application on.
- 5 When prompted, enter the login ID and password for a user authorized to perform config-admin actions.

- 6 Access the maintenance interface level:  
**sdmmtc**
- 7 Access the software inventory manager (SWIM) level:  
**swim**  
The CS 2000 Core Manager lists the software applications currently installed.
- 8 List the contents of the tape you previously inserted:  
**apply <n>**  
where  
**<n>**  
is either 0 (slot 2) or 1 (slot 13).
- 9 Locate the Java Runtime Environment (JRE) 1.3 packages.  
**Note:** If necessary, use the up (enter 12, u, or up) and down (enter 13, d, or down) commands to locate the JRE 1.3 packages.
- 10 Select and install the Java Runtime Environment Executables 1.3.0.0 package:  
**apply <n>**  
where  
**<n>**  
is the number next to the Java Runtime Environment Executables 1.3.0.0 package.
- 11 Confirm the apply command:  
**y**
- 12 Select and install the Java Runtime Environment Libraries 1.3.0.0 package:  
**apply <n>**  
where  
**<n>**  
is the number next to the Java Runtime Environment Libraries 1.3.0.0 package.
- 13 Confirm the apply command:  
**y**
- 14 Select and install the Java Runtime Environment Executables 1.3.0.15 package:  
**apply <n>**



where

**<n>**

is the number next to the Java Runtime Environment Executables 1.3.0.15 package.

**15** Confirm the apply command:

**y**

**16** Select and install the Java Runtime Environment Libraries 1.3.0.15 package:

**apply <n>**

where

**<n>**

is the number next to the Java Runtime Environment Libraries 1.3.0.15 package.

**17** Confirm the apply command:

**y**

**18** Select and install Succession Provisioning Data Sync Manager (or Backup Restore Manager fileset, SDM\_BKM.bkm).

**apply <n>**

where

**<n>**

is the number next to the Backup Restore Manager fileset, SDM\_BKM.bkm (or Succession Prov Data Sync Manager)

**19** Confirm the apply command:

**y**

The application installation script runs.

**20** As part of the Backup Restore Manager application installation, a script runs that enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). As the

script runs, you are prompted for the user name. The script restricts the name to a maximum of 16 characters.

#### **ATTENTION**

The user name must be one that exists and is used to log in to the core to initiate an image dump. The user name you enter must also be enabled on the core. For assistance, refer to procedure, "Creating the backup user ID on the core for SBRM" in CS 2000 Core Manager Configuration Management, NN10104-511, or in ATM/IP Solution-level Security and Administration, NN10402-600.

- 21** You are prompted for the password of the user you entered in the previous step. The script restricts the password to a maximum of 16 characters.

#### **ATTENTION**

This password is set up when the user name in the previous step is created. For assistance refer to procedure, "Creating the backup user ID on the core for SBRM" in CS 2000 Core Manager Configuration Management, NN10104-511, or in ATM/IP Solution-level Security and Administration, NN10402-600.

- 22** You are prompted for the logical volume where the backup is stored. This is the device on which the core image dump is stored. Ensure that this device has enough space to store the backup.
- 23** You are prompted for the core type: either XA-core or Compact.  
**Note:** This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 24** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## **Reconfiguring the Backup Restore Manager application on the CS 2000 Core Manager**

At any time after the configuring the Backup Restore Manager is complete, you wish to reconfigure user access to the core for the SBRM

### ***At the maintenance interface***

- 1** Access the config level of the SDM maintenance interface:  
**sdmmtc config**

- 2 From the list of filesets that display, locate the application number of the Succession Provisioning Data Sync Manager fileset or Backup Restore Manager fileset, SDM\_BKM.bkm, then type:

**config <n>**

where

**<n>**

is the application number for the Succession Provisioning Data Sync Manager fileset or Backup Restore Manager fileset, SDM\_BKM.bkm

- 3 If applicable, confirm the config command:

**y**

The Backup Restore Manager application script runs that enables you to reconfigure access to the core for the Synchronous Backup Restore Manager (SBRM).

- 4 You are prompted for the user name. The script restricts the name to a maximum of 16 characters.

#### **ATTENTION**

The user name must be one that exists and is used to log in to the core to initiate an image dump. The user name you enter must also be enabled on the core. For assistance, refer to procedure, "Creating the backup user ID on the core for SBRM" in CS 2000 Core Manager Configuration Management, NN10104-511, or in ATM/IP Solution-level Security and Administration, NN10402-600.

- 5 You are prompted for the password of the user you entered in the previous step. The script restricts the password to a maximum of 16 characters.

#### **ATTENTION**

This password is set up when the user name in the previous step is created. For assistance refer to procedure, "Creating the backup user ID on the core for SBRM" in CS 2000 Core Manager Configuration Management, NN10104-511, or in ATM/IP Solution-level Security and Administration, NN10402-600.

- 6 You are prompted for the logical volume where the backup is stored. This is the device on which the core image dump is

stored. Use the same logical volume used previously, unless otherwise specified.

- 7 You are prompted for the core type: either XA-core or Compact. Enter the same core type previously used, unless otherwise specified.

**Note:** This information is needed in order for the software to know whether the core will also have a Message Switch load.

- 8 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Installing optional software on a CBM 850

### Purpose

This is a generic procedure that is used for installing optional software packages on the CBM 850. Consult [Filesets available for the CBM 850 on page 29](#) to determine the optional software packages (filesets) that you can install through this procedure.

This procedure must be performed on a pre-cloned system. If the procedure is not performed on a pre-cloned system, clone the image of the active node to the inactive node of the cluster after the software package has been installed and configured, and after the active node has been made patch-current.

### Filesets available for the CBM 850

The following table lists filesets (applications) included in the CBM0090 load. The table also shows which filesets are included with the CBM 850 at the time of installation (Base) and which filesets are optional and that you can install later.

#### Filesets available for the CBM 850 (Sheet 1 of 2)

Fileset	Description	Type
SDM_BASE.version_20.81.0.0	Load Lineup Information	Base
CBM_SETUP	CBM installation and upgrade tool; available only on CD	Base
NT_SIM.tools	Patching Tools	Base
SDM_ACE	SDM ACE distribution	optional
SDM_AFT.DMS500	SBA Automatic File Transfer	optional
SDM_BASE.base	Platform Base	Base
SDM_BASE.comm	Platform Maintenance Common	Base
SDM_BASE.gdd	Generic Data Delivery	Base
SDM_BASE.logs.client	Log Delivery Service Client	optional
SDM_BASE.logs	Log Delivery Service	Base
<b>Note:</b> Base = included with the CBM 850		

**Filesets available for the CBM 850 (Sheet 2 of 2)**

<b>Fileset</b>	<b>Description</b>	<b>Type</b>
SDM_BASE.mtce	Platform Maintenance	Base
SDM_BASE.omsl	OM Access Service	Base
SDM_BASE.tasl	Table Access Service	Base
SDM_BMI.bmi	Base Maintenance Interface	optional
SDM_DDMS_ossaps	OSS and Application Svcs	optional
SDM_DDMS_osscomms	OSS Comms Svcs	optional
SDM_BASE.util	Platform Utilities	Base
SDM_DEBUG.tools	SDM/CBM Debug Helper Tools	Base
SDM_DMA.dma	DMS Maintenance Application	optional
SDM_FTP.proxy	FTP Proxy	optional
SDM_GR740PT.gr740pt	GR740 Pass Through	optional
SDM_LOGS.mdm	Passport Log Streamer	optional
SDM_OMDD.omdd	OM Delivery	optional
SDM_REACHTHRU.rttl1	Reach Through SPM	optional
SDM_SBA.DMS500	SDM Billing Application	optional
SDM_SCFT.scft	Core File Transfer	optional
SDM_SWLD.swld	Bootpd and tftpd	optional
NTbkupmgr	Succession Provisioning Data Synch Manager	optional
NTdtsv	CEM DMS Data Server	optional
NTprxy	CEM Telnet Ftp Handler	optional
NTsaf	CEM Store and Forward	optional
<b>Note:</b> Base = included with the CBM 850		

## Procedure for installing optional software on a CBM 850

Use the following procedure to install optional software on a Core and Billing Manager (CBM) 850.

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Installing optional software on a CBM 850

#### *At your workstation*

- 1 Open a connection to the active node of the CBM 850 using SSH and log in as the root user:

```
ssh -l root <ip_address>
```

where

**<ip\_address>**

is the IP address of the active node of the CBM 850 cluster

- 2 Enter the password for the root user.
- 3 Use the following table to determine your next step.

If	Action
you are installing the DDMS application	Perform steps <a href="#">1</a> and <a href="#">5</a> only, of <a href="#">Procedure for installing DDMS on page 34</a> , then go to step <a href="#">5</a> of this procedure.
you are installing the OMDD application	Perform step <a href="#">1</a> only, of <a href="#">Procedure for installing the OM Data Delivery software package on page 41</a> , then go to step <a href="#">5</a> of this procedure.

If	Action
you are installing the log delivery service application	Perform <a href="#">Procedure for installing the Passport Log Streamer application on page 51</a> ,  then go to step <a href="#">9</a> of this procedure.
you are installing the SBA or AFT applications	Perform <a href="#">Procedure to install the SBA and AFT software packages on page 53</a> ,  then go to step <a href="#">9</a> of this procedure.
you are installing GR740PT application server	Perform <a href="#">Procedure for installing GR740PT application server on page 53</a> ,  then go to step <a href="#">9</a> of this procedure.
you are installing the FTP Proxy application	Create logical volume: /cbmdata/00/esa, with size 25 Mbyte, using the logical volume creation procedure found in CBM 850 Security and Administration, NN10358-611,  then go to step <a href="#">4</a> of this procedure.
you are installing the Backup Restore Manager software	Perform procedure <a href="#">Installing the Backup Restore Manager software on page 65</a> ,  then go to step <a href="#">9</a> of this procedure.
you are installing any other optional software application	Go to step <a href="#">4</a>

- 4 Apply the software application package by performing the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 56](#).



- 5 Use the following table to determine your next step.

If	Action
you are installing any other applications that require you to create logical volumes	Return to step <a href="#">3</a> in this procedure and follow the required action for the next application you are installing.
you are not installing any other applications that require you to create logical volumes	Go to step <a href="#">6</a>

- 6 Ensure that you have created any required logical volumes for all of the applications you are installing before continuing.
- 7 If you created any logical volumes in step [3](#), reboot the CBM 850:  
**init 6**
- 8 After the node reboot is complete, use the following table to determine your next step.

If	Action
you are installing the DDMS application	Perform the remaining steps of <a href="#">Procedure for installing DDMS on page 34</a> , starting with step <a href="#">14</a> ,  then go to step <a href="#">9</a> of this procedure.
you are installing the OMDD application	Perform the remaining steps of <a href="#">Procedure for installing the OM Data Delivery software package on page 41</a> , starting with step <a href="#">2</a> ,  then go to step <a href="#">9</a> of this procedure.
you are installing the FTP Proxy application	Go to step <a href="#">9</a> .
you are installing any other optional software application	Go to step <a href="#">9</a>

- 9 Ensure that your CBMs are patch-current. For patching procedures, refer to ATM/IP Solution-level Security and Administration, NN10402-600.
- 10 Clone the image of the active node to the inactive node by performing the procedure, [Cloning the image of the active node to the inactive node of a CBM 850 cluster on page 62](#).
- 11 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

### Procedure for installing DDMS

This procedure enables you to install the DDMS application.

#### Prerequisites

The following prerequisites apply to using this procedure.

- For a successful installation of DDMS, verify that the Log Delivery Service application is in service.
- When Enhanced Password Control is in effect on the CM or core, the DDMS software has the ability to manage automatic password changing on the CBM and the CM, before passwords expire. It is not necessary to manually change any of the passwords for the SDM01-SDM04 userids on the CBM or CM. When the DDMS software is returned to service, it reads the tables, ofcopt and ofceng, on the CM to determine whether Enhanced Password Control is in effect. If Enhanced Password Control is in effect, the DDMS software reads the password lifetime value and automatically changes the passwords one day before they expire.

If you make manual changes to the password lifetime value, or if you turn the Enhanced Password Control off or on, these changes must be synchronized with DDMS software by performing a bsy or rts of the DDMS application. If you change any of the SDM01-SDM04 passwords manually, you must apply the same password changes in the DDMS configuration file.

## Action

### ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Installing DDMS on a CBM 850

### *At your workstation*

- 1 Set Enhanced Password Control for the SDM01 userid.

```
permit sdm01 <sdm01_pswd> 4 10000 english all
```

where

**<sdm0n\_pswd>**

is the CM password for user SDM01

**Note:** If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

- 2 Set Enhanced Password Control for the SDM02 userid.

```
permit sdm02 <sdm02_pswd> 4 10000 english all
```

where

**<sdm0n\_pswd>**

is the CM password for user SDM02

- 3 Set Enhanced Password Control for the SDM03 userid.

```
permit sdm03 <sdm03_pswd> 4 10000 english all
```

where

**<sdm0n\_pswd>**

is the CM password for user SDM03

- 4 Set Enhanced Password Control for the SDM04 userid.

```
permit sdm04 <sdm04_pswd> 4 10000 english all
```

where

**<sdm0n\_pswd>**

is the CM password for user SDM04

- 5 Create the first required logical volume for the DDMS application.

```
make1v /cbmdata/00/osscomms 16
```

- 6 Set the access privileges of the first logical volume for the DDMS application.  
**chmod 755 /cbmdata/00/osscomms**
- 7 Set the ownership privileges of the first logical volume for the DDMS application.  
**chown maint:maint /cbmdata/00/osscomms**
- 8 Create the second required logical volume for the DDMS application.  
**makelv /cbmdata/00/ossaps 112**
- 9 Set the access privileges of the second logical volume for the DDMS application.  
**chmod 755 /cbmdata/00/ossaps**
- 10 Set the ownership privileges of the second logical volume for the DDMS application.  
**chown maint:maint /cbmdata/00/ossaps**
- 11 Create the third required logical volume for the DDMS application.  
**makelv /cbmdata/00/ossapslog 112**
- 12 Set the access privileges of the third logical volume for the DDMS application.  
**chmod 755 /cbmdata/00/ossapslog**
- 13 Set the ownership privileges of the third logical volume for the DDMS application.  
**chown maint:maint /cbmdata/00/ossapslog**
- 14 Apply the two software application packages, OSS and Application Svcs and OSS Comms Svcs by performing the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 56](#). Specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.

- 15** You are prompted automatically to configure the OSS Comms Svcs package. Use the following table to determine your next step.

**Note:** The OSS and Application Svcs package does not require configuration.

If	Do
you are prompted automatically to configure the OSS Comms Svcs package	step <a href="#">19</a>
you are not prompted automatically to configure the OSS Comms Svcs package	step <a href="#">16</a>

- 16** Access the config level of the maintenance interface:  
**cbmmtc config**
- 17** In the list of applications, locate the OSS Comms Svcs application and record its application number (located next to the names of the applications). Select the application:  
**select <application number>**  
 where  
**<application number>**  
 is the number associated with the OSS Comms Svcs application, that you noted.  
*In response to the command, the OSS Comms Svcs application is highlighted on the cbmmtc config screen.*
- 18** Invoke the configuration of the OSS Comms Svcs application.  
**config**
- 19** When prompted to enter the logroute tool, as shown in the following figure, press Enter.

#### DDMS logroute tool banner

```
#####
##
# Adding DDMS logroute configuration
#####
##
Please add DDMS log routing:
```

### DDMS logroute tool banner

```
#####  
##  
Device type      = file  
File             = /cbmdata/00/logs/ossaps/ossapslog  
Routing         = addrep  
log_type        = DDMS  
Press <RETURN> when ready
```

*The Logroute Main Menu appears, as shown in the following figure.*

### Logroute tool main menu

```
Logroute Main Menu  
  
1 - Device List  
2 - Global Parameters  
3 - CM Configuration File  
4 - GDD Configuration  
5 - Help  
6 - Quit Logroute  
  
Enter Option ==>
```

- 20** Set up a path and file to store DDMS customer logs. Select the Device List menu

**1**

The Device List Menu screen is displayed.

- 21** Select 1 to display the Device List screen.

If the list	Do
includes device /cbmdata/00/logs/ossaps/ossapslog	step <a href="#">22</a>
does not include device /cbmdata/00/logs/ossaps/ossapslog	step <a href="#">23</a>

- 22** Press the Enter key.
- 23** Begin to add a new device:  
**2**
- 24** Select a file device:  
**3**  
*Response:*  
 Enter file name ==> /data/logs/
- 25** Complete the path name by typing  
**ossaps/ossapslog**  
 You have now set up the log routing for the DDMS.
- 26** When prompted, enter STD log format (from the range displayed).
- 27** When prompted, set the ECOPE option to ON.
- 28** Select addrep:  
**a**
- 29** Enter the log identifier by typing, in uppercase  
**DDMS**
- 30** When prompted to enter more log routing details, enter  
**N**
- 31** Save the new device:  
**y**  
*Response:*  
 Save completed -- press return to continue
- 32** Press the Enter key to return to the Add Device screen.

**33** Return to the Device List Menu screen:

5

**34** Return to the main menu screen:

6

**35** Exit logroute:

6

*The CM User Setup screen is displayed as shown in the following figure, and the required CM users, SDM01-SDM04, for DDMS are added to the DDMS configuration file. The passwords for these users are the same as those entered in step 1*

**Note:** *The userIDs and passwords are not case sensitive. You can change them after this installation is complete.*

### Example of DDMS CM user setup screen

```
CM User Setup

0. QUIT
1. Add user
2. Delete user (by ID)
3. Update passwd (by ID)
4. Display users (ID)

Enter choice:
```

**36** Add a new user for each of the required userIDs:

1

**37** When prompted, enter the user name (for example, sdm01).

**38** When prompted enter the user password.

**Note:** The first entry of a user name and password generates the following message: Error: file not valid. You can ignore this message.

**39** If applicable, continue to add other user names and passwords at the prompt, otherwise continue with the next step.

**40** Exit the CM User Setup screen:

0

*The DDMS Clients Configuration screen is displayed as shown in the following example.*



### Example of DDMS Clients Configuration screen

```
DDMS Clients Configuration

0. Quit
1. Add new clients
2. Remove existing clients
3. List existing clients
Enter choice:
```

**41** Add a new DDMS client.

**1**

**Note:** The DDMS clients are the CS 2000 Management Tools servers with the SESM load.

**42** When prompted, enter the IP address for each of the CS 2000 Management Tools servers, pressing the Enter key after each entry. If the CS 2000 Management Tools server is a cluster configuration, add the IP address of both the active and inactive units.

**43** After you have entered all the IP addresses, type

**done**

**44** Exit the DDMS clients configuration screen:

**0**

**45** You have completed this procedure. Return to step [9](#) of the higher level task flow or procedure [Installing optional software on a CBM 850](#).

### Procedure for installing the OM Data Delivery software package

This procedure contains the steps for installing and configuring the OM Data Delivery application on the CBM 850 cluster.

#### Functional overview

The Operational Measurement Delivery (OMD) application collects customer-defined operational measurement (OM) data from the DMS switch, and stores the data in OM report files on the core manager in comma-separated value (CSV) format. The OMD application is configured using the OM user interface (OMUI).

An OM report file is a collection of OM groups that are monitored at selected reporting intervals. Secure File Transfer (SFT) or File Transfer Protocol (FTP) sends OM report files from the core manager to an

operations support system (OSS). A data browser such as a spreadsheet program provides access to the contents of the files.

**Report elements** Report elements define the content of OM report files, and combine content of related OM groups for monitoring and analysis. A report element contains a user-defined report element name, a reporting interval for a report element (five minutes, or the office transfer period of 15 or 30 minutes), and names of the OM groups and registers.

**Subtraction profiles** The subtraction profile determines the change in the value of an OM group register between five-minute OM reports, as defined in a report element. The subtraction profile applies only when the reporting interval is set to five minutes. The following table lists the types of subtraction profiles.

#### Subtraction profiles

Type	Description
Single	A single register represents a running total
Double	Two registers (base and extension) represent a running total
Non-subtraction	Subtraction is not performed on selected registers

**Data collection schedules** A data collection schedule defines start and stop times for OM report collection. The collecting interval determines how often in the time period an OM report collection occurs. The data is collected to the same report file for schedules with collecting intervals after midnight. The following table lists the data collection schedule types.

#### Data collection schedule repetition types (Sheet 1 of 2)

Repetition	Schedule information
Daily	Daily start and stop time. Format: hhmm, <i>where</i> hh = hour (00 to 24), and mm = minute (00 or 30). Specifies only a single time period; for multiple time periods in the same day, you must define multiple schedules.

**Data collection schedule repetition types (Sheet 2 of 2)**

Repetition	Schedule information
Weekly	Weekly start and stop time. Values: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday. Format: hhmm; multiple days can be specified in same schedule.
Monthly	Monthly start and stop time. Values:1 to 31. Format: hhmm; multiple days can be specified in the same schedule.

**File rotation schedules** File rotation schedules specify when to rotate report files. File rotation closes an open report file and moves it to the */omdata/closedNotSent* directory on the core manager. Each file rotation schedule contains

- a user-defined file rotation schedule name
- a repetition rate for the rotation schedule based on either the number of report records collected or the number of hours to collect records
- a schedule that defines the time to rotate the report file

The data collection and file rotation schedules operate independently of each other. If a file rotation schedule event occurs during a scheduled data collection period, the file rotation schedule closes and rotates the OM report file, and a new OM report file with the same name is opened. The new file starts collecting immediately and continues until the end of the collection period. The open OM report file remains in the */omdata/open* directory until the file rotation schedule closes it and rotates it to the */omdata/closedNotSent* directory.

**File transfer destinations** File transfer destinations define remote downstream destinations of OM report files. Each destination entry contains

- a user-defined file transfer destination name
- the valid IP address of a remote destination host (xxx.xxx.xxx.xxx)
- the FTP port address of the remote host (default: 21)
- the remote host login ID and password

**Note:** The core manager does not authenticate the IP and port addresses or the login ID and password.

An invalid destination causes the file transfer to fail. When a file fails to transfer, log entries are written to the customer log file at */var/adm/custlog*. The file is not re-sent, and the report file must be

transferred manually using either the OMFTP command, SFT or standard FTP.

**File transfer schedules** File transfer schedules specify when to transfer OM report files downstream. Each file transfer schedule contains a

- user-defined file transfer schedule name
- repetition rate for the transfer schedule
- schedule defining when to transfer the report file (if using a repetition rate)
- remote file transfer destination host system (<16 destinations/schedule)
- destination storage directory for each defined transfer destination

The files are transferred downstream using FTP, and move from the */omdata/closedNotSent* directory to the */omdata/closedSent* directory. If a scheduled file transfer fails, a log is raised and the report file that could not be transferred moves to the */omdata/closedSent* directory. The OMDD keeps track of the destination to which the report file could not be transferred. Then, at the next scheduled file transfer, the OMDD attempts to send the report file to the destination again. The OMDD will repeat this activity until one of the following situations occurs:

- the file is transferred successfully
- the file exceeds the retention period for the *closedNotSent* directory
- the file gets deleted during an audit because the *omdata* filesystem usage has exceeded the allowable limit
- the file is deleted by the *omdelete* utility

**Report registrations** A report registration links information from the report element and schedules for data collection, file rotation and file transfer to collect OM data. The user can create up to 32 report registrations. Once a report registration has been created, it can be deleted but not modified. Each report registration contains user-defined names for the report registration, report elements and each schedule type. The schedules become active immediately after the creation of the report registration.

An OM report file opened by the data collection schedule in the */omdata/open* directory uses the name of the report registration as part of the OM report file name. Linking a file transfer schedule into a report registration provides regular and automatic transfers of OM report files to remote downstream destinations. Unless you link a file transfer

schedule to a report registration, you must manually transfer your OM report files downstream.

**Report registration limit** The report registration limit is the maximum number of report registrations that can be configured on a core manager without affecting processing performance. The number of report registrations range from 1 to 32 (default value: 32). To set the limit, use the Set Report Registration Limit option from the OMUI main menu.

**File retention periods** A cleanup of OM report files that have been sent downstream automatically occurs every night at midnight (00:00 or 24:00). Files in the */omdata/closedSent* directory are deleted at an interval based on the file retention period defined in the OMUI (range: 1 to 14 days). The default interval is set to 7 days at OMD installation. Unsent OM report files older than 32 days in the */omdata/closedNotSent* directory are deleted. This 32-day default value is read from a configuration file set up when the core manager is commissioned.

**OMD data collection capacity** Collection of more than 10,000 tuples reduces core manager performance and the retention period for OM report files. To determine the number of tuples in an OM group, either monitor the OM group and count the tuples in the report file or use the OMSHOW command from the MAP (maintenance and administration position) on the DMS switch. Use the formulas in the following table to calculate the limit for OMD data collection.

#### Formulas for calculating the limit for OMD data collection

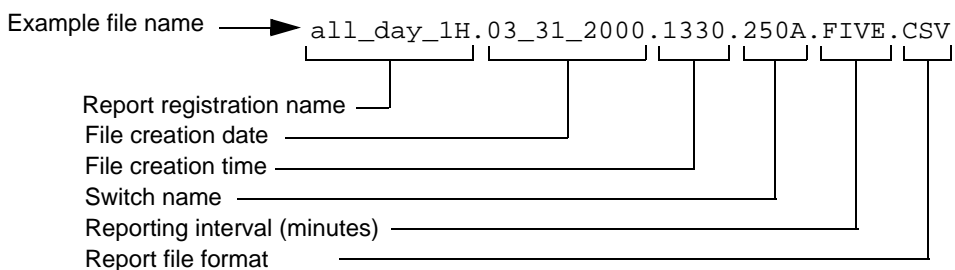
OMD data capacity transfer type	Formula
5- and 15-minute	$x + y/3 = n \leq 10,000$ tuples (without loss of data)
5- and 30-minute	$x + z/6 = n \leq 10,000$ tuples (without loss of data)
where: <b>x</b> = the number of OM tuples collected every 5 minutes <b>y</b> = the number of OM tuples collected every 15 minutes <b>z</b> = the number of OM tuples collected every 30 minutes <b>n</b> < 10,000 tuples	

The following table lists the current OMD data collection capacity.

**OMD maximum data collection capacity**

Transfer type	Capacity (number of tuples)
5-minute	6000
15-minute	12,000
30-minute	24,000

**OM report file naming** Report files are named according to the report registration name, file creation date and time, name of the switch generating the OMs, and reporting interval. Refer to the following example file name and explanation.



**OM report file contents** Tuple information for an OM group can be viewed in CSV format from the OM report file on the core manager, and by entering the OMSHOW command on the MAP. The following table shows an OM report file.

**Contents of an OM report file**

Date	Time	Switch Names	Group Name	Key/Info Field	Reg1 Name	Reg1 Value	Reg2 Name	Reg2 Value	Reg31 Name	Reg31 Value
2/23/00	3:35:00	250U	TRK	ISU_GWC.2W.0.0	AOF	0	ANF	0		
2/23/00	3:35:00	250U	TRK	ESADGTR.OG.0.0	AOF	0	ANF	0		

## Contents of an OM report file

Date	Time	Switch Names	Group Name	Key/Info Field	Reg1 Name	Reg1 Value	Reg2 Name	Reg2 Value	Reg31 Name	Reg31 Value
2/23/00	3:35:00	250U	TRK	HSET.OG.3.0	AOF	0	ANF	0		
2/23/00	3:35:00	250U	TRK	JACK.OG.2.0	AOF	0	ANF	0		
2/23/00	3:35:00	250U	TRK	LTU.OG.2.0	AOF	0	ANF	0		
2/23/00	3:35:00	250U	TRK	MONTALK.OG.0.0	AOF	0	ANF	0		
2/23/00	3:35:00	250U	TRK	OCKT.OG.0.0	AOF	0	ANF	0		

**Audits** The OM report files are stored in the omdata filesystem. This filesystem is audited every 30 minutes for the amount of usage. To ensure that the omdata filesystem usage does not reach 100% at any time, the system performs the following actions:

- When the filesystem usage reaches 60%, Major trouble log SDM338 is raised indicating that OM report files will be deleted at the time of the next audit, if usage exceeds 90%. Then, if usage exceeds 90% at the time of the next audit log SDM639 is raised indicating all report files in the closedSent directory will be deleted, and the report files are deleted.
- If omdata filesystem usage does not fall below 80% after deletion of all report files in the closedSent directory, report files from the closedNotSent directory will be deleted, starting from the oldest file, until the usage is at 80% or less. As each report file is deleted from the closedNotSent directory, log SDM631, which describes the action, is raised.

### Prerequisites

Ensure that the OM Access Service and Table Access Service application filesets are installed and in service on your core manager before executing this procedure.

For the wireless market, the Nortel support group must increase the buffer size within the OM Access Service to 2.5 MB to accommodate the amount of data transferred by the front end for a transfer period of every 30 minutes.

### Action

#### ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Installing and configuring the OM Data Delivery application on a Core and Billing Manager 850

#### At your workstation

- 1 Create the following logical volume (directory for a file system) required for the OMDD software package you are installing:  

```
makelv /cbmdata/00/omdata 1008
```
- 2 Using the procedure, [Applying software packages on a CBM 850 using the CBMMTC interface on page 56](#) apply the SDM\_OMDD.omdd software package located in the /cdrom/cdrom/applications/cbm/packages directory. Since CD-ROM is being used to install the application, specify /cdrom/cdrom/applications/cbm/packages as the directory path of the source directory when you perform that procedure.
- 3 Access the Config level of the CBM maintenance interface:  

```
cbmmtc config
```
- 4 Configure OM Data Delivery:  

```
config <n>
```

where  

```
<n>
```

is the number next to OM Data Delivery under fileset description



- 5 The system indicates that the Tuple Number option is inactive and prompts you to determine whether you want to activate it.

**Note:** The Tuple Number option allows you to activate or disable a tuple number so that it can be included in a CSV file with other OM information.

If you	Do
want to activate the Tuple Number option	Type <b>y</b>
do not want to activate the Tuple Number option	Type <b>n</b>

- 6 The system prompts you to confirm whether the Multiservice Data Manager (MDM) and core manager are integrated. To indicate that the MDM is connected to the core manager for collecting Passport 15000 performance measurement data, type **y**
- 7 Configure the core manager to communicate with the MDM as follows. When prompted, enter the IP address of the first MDM you want to connect to.
- 8 When prompted, enter the hostname of the first MDM.
- 9 When prompted, enter the IP address of the second (alternate) MDM you want to connect to.
- 10 When prompted, enter the hostname of the second MDM.
- 11 When prompted, enter the port for 5-minute performance PM (performance measurement) data. The default port is 1646.
- 12 When prompted, enter the port for 30-minute PM data. The default port is 1647.
- 13 You are prompted as to whether you want to use custom connection retry settings. In case of connection failure, OMDD will try connecting to the MDMs, alternatively. When prompted,

indicate whether you want to use custom connection retry settings.

If you	Do
want to use custom retry settings	Type <b>y</b>  then go to step <a href="#">14</a>
do not want to use custom retry settings but want, instead, to use default settings	Type <b>n</b>  then go to step <a href="#">19</a>

- 14** Configure the custom retry settings. Enter a numeric value (in seconds) for the first connection retry interval.  
  
*Note:* Values higher than 300 seconds are not recommended as they can adversely affect recovery time.
- 15** Enter the number of retry attempts for the first retry interval.
- 16** Enter a numeric value (in seconds) for the second connection retry interval.
- 17** Enter the number of retry attempts for the second connection retry interval.
- 18** Enter a numeric value (in seconds) for the third connection retry interval.
- 19** When prompted, confirm the configuration data you have entered by typing **y**, otherwise type **n** to re-enter all of the configuration data.
- 20** The system indicates that the configuration is complete.  
Press the Enter key.
- 21** The system indicates that the changes will take place after the OM Data Delivery application is restarted.  
Press the Enter key to restart the OM Data Delivery application.
- 22** Exit the maintenance interface by typing  
**quit all**
- 23** You have completed this procedure. Return to step [9](#) of the higher level task flow or procedure [Installing optional software on a CBM 850](#).

## Procedure for installing the Passport Log Streamer application

The following procedure contains the steps for installing and configuring the Passport Log Streamer application on the CBM 850 cluster.

For full operation, the log delivery application requires installation of the following application filesets:

- log delivery service (base software)
- log delivery service client (optional software)
- Generic Data Delivery (base software)
- Passport Log Streamer, if the core manager needs to communicate with the Multiservice Data Manager (MDM) for fault data. (optional software)

### Prerequisites

Before performing this procedure, ensure that there are no disk faults on the core manager.

In order to ensure that the Passport Log Streamer is able to communicate with the configured MDMs and to collect logs, any restrictions for the configured MDM ports must be removed from all of the firewalls that exist between the MDM and the CBM 850.

### Action

#### ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Installing and configuring the Passport Log Streamer application on the Core and Billing Manager 850

### *At your workstation*

- 1 Perform the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 56](#) to apply the SDM\_LOGS.mdm\_21.39.9.0.pkg software package located in the /cdrom/cdrom/applications/cbm/packages directory. Since CD-ROM is being used to install the application, specify /cdrom/cdrom/applications/cbm/packages as the directory path of the source directory when you perform that procedure.

- 2 Configure the Passport Log Streamer application. When prompted, enter the IP address for the first MDM node.
- 3 When prompted, enter the IP address for the second MDM node.
- 4 When prompted, enter the port number configured for the pserver application on the first MDM node.
- 5 When prompted, enter the port number configured for the pserver application on the second MDM node.
- 6 When prompted, indicate that you do not want to receive MDM logs by entering n.
- 7 When prompted, indicate that you do not want to specify Passport 15000 log filters by entering n.
- 8 When prompted, indicate that you do not want to specify Passport 8600 log filters by entering n.
- 9 When prompted, confirm the configuration data you entered by entering y.
- 10 Place the log delivery service application and the Passport Log Streamer application into service by accessing the Application (Appl) level of the CBM maintenance interface:  
**appl**
- 11 Busy the application filesets:  
**bsy <fileset\_number> <fileset\_number>**  
**where**  
fileset\_number is the number next to each of the following application filesets:
  - Log delivery service
  - Passport Log Streamer
- 12 Return the application filesets to service:  
**rts <fileset\_number> <fileset\_number>**  
**where**  
fileset\_number is the number next to each of the application filesets you busied in the previous step  
  
Once the application filesets are in service, the system retrieves any current log records. To view or store the log records, refer to procedure "Displaying or storing log records using log receiver" in Core and Billing Manager Fault Management, NN10351-911.
- 13 Exit the CBM maintenance interface:  
**quit all**

- 14 You have completed this procedure. Return to step 9 of the higher level task flow or procedure [Installing optional software on a CBM 850](#).

### **Procedure to install the SBA and AFT software packages**

This procedure enables you to install the SuperNode Billing Application (SBA) and Automatic File Transfer (AFT) software packages on the CBM 850 cluster.

#### **Prerequisites**

There are no prerequisites for this procedure.

#### **Action**

### **Installing the SBA and AFT software packages on a CBM 850**

#### ***At your workstation***

- 1 Using the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 56](#), apply the SBA and AFT software packages located in the /cdrom/cdrom/applications/cbm/packages directory.
- 2 Create the necessary logical volumes (directories for file systems) required for the SBA using procedure “Adding a logical volume through the command line” in Core and Billing Manager 850 Accounting, NN10363-811.
- 3 To configure the SBA for operation, refer to Core and Billing Manager 850 Accounting, NN10363-811, for the procedures to use.
- 4 To configure AFT for operation, refer to Core and Billing Manager 850 Accounting, NN10363-811, for the procedures to use.
- 5 You have completed this procedure. Return to step 9 of the higher level task flow or procedure [Installing optional software on a CBM 850](#).

### **Procedure for installing GR740PT application server**

This procedure enables you to install the GR740PT application server.

#### **Prerequisites**

To ensure a successful GR740PT application server operation, the following must first be configured:

- the settings for office parameters eadas\_dc\_interface and eadas\_nm\_interface in table OFCVAR, and the settings for the

EADAS SOCs (OAM00005 and OAM00006) are correct for your configuration.

- OAM00004 for EADAS/DC is ON and that office parameters eadas\_mpc\_and\_link and netminder\_mpc\_and\_link are appropriately datafilled in table OFCVAR when BX25 connectivity is required.

The following table lists the supported configurations for EADAS GR740PT application server.

### CM EADAS TCP/IP configurations

Supported configurations	Setting for eadas_dc_interface	Setting for eadas_nm_interface	SOC OAM00005	SOC OAM00006
DC and NM over BX25	X25	N/A	ON	IDLE
DC and NM over TCP/IP	TCP_IP	N/A	ON	IDLE
DC and Netminder over BX25	X25	X25	IDLE	ON
DC over BX25 and Netminder over TCP/IP	X25	TCP_IP	IDLE	ON
DC over TCP/IP and Netminder over BX25	TCP_IP	X25	IDLE	ON
DC and Netminder over TCP/IP	TCP_IP	TCP_IP	IDLE	ON

The following table lists the channel assignments for EADAS. Note that DC EADAS channels 1, 2 and 3 support TR-740/746 compliant header and message. NM EADAS channels 1, 2 and 3 support SR3942 and TR746 to Netminder.

### EADAS channel assignments

Description	Service name	TCP port	MTS offset
DC EADAS lc 1	DC_EADAS_LOG_CHAN1	9550	234
DC EADAS lc 2	DC_EADAS_LOG_CHAN2	9551	235
DC EADAS lc 3	DC_EADAS_LOG_CHAN3	9552	236
NM EADAS lc 1	NM_EADAS_LOG_CHAN1	9553	237

**EADAS channel assignments**

Description	Service name	TCP port	MTS offset
NM EADAS lc 2	NM_EADAS_LOG_CHAN2	9554	238
NM EADAS lc 3	NM_EADAS_LOG_CHAN3	9555	239

**Action****Installing GR740PT application server*****At your workstation***

- 1 Using procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 56](#), apply the GR740PT software package located in the /cdrom/cdrom/applications/cbm/packages directory.
- 2 When prompted to: Enter mode of security, use the following table to determine your response.

If	Do
you are not configuring GR740PT in non-secure mode	select 1. Non-secure
you are configuring GR740PT in local secure mode	select 2. Local (SSH) security

- 3 You have completed this procedure. Return to step [9](#) of the higher level task flow or procedure [Installing optional software on a CBM 850](#)

**Procedure for Applying software packages on a CBM 850 using the CBMMTC interface**

This procedure enables you to install optional software packages on the nodes of a CBM 850 cluster.

**Prerequisites**

There are no prerequisites for this procedure.

**Action****ATTENTION**

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

**Applying software packages on a CBM 850 using the CBMMTC interface****At your workstation**

- 1 From the command line prompt, access the apply level of the cbm maintenance interface:

```
cbmmtc apply
```

The system displays the apply level screen of the cbm maintenance interface, which shows a list of the packages, if any exist, in the default source directory.

**Note:** Up to 12 software packages can be displayed at a time. Use the Down command (command 13 as shown in the following example) to view other packages.

**Example of cbm maintenance interface apply level**

```

xterm
  CBM      MATE  NET  APPL  SYS  HW  CLI: SN100
  *        -    *   *    *   *  Host: SN100_CBM
                                Active

Apply
0 Quit
2
3
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 16:12 >

Source: the directory /data/swd/sdm.
Filter: sdm Interactive Mode: OFF
# Package Description          Version      Status
-----
No packages available in the directory /data/swd/sdm.
Use the Source command to list another directory.

```



**2** Use the following table to determine your next step.

If	Do
CD-ROM is being used to deliver the CBM software	step <a href="#">3</a> , and specify:  /cdrom/cdrom/applications/cbm/packages  as the <source_directory_name>
you want to exit from the cbm maintenance interface	step <a href="#">13</a>

**3** Insert the CD-ROM into the CD drive if it is not already present in the drive.

**4** At the command line located at the bottom of the cbmmtc user interface screen, type:

**source <source\_directory\_name>**

*where*

**<source\_directory\_name>**

*is the full pathname of the directory containing the package that you want to apply. Since CD-ROM is being used for the installation, specify  
/cdrom/cdrom/applications/cbm/packages as the  
source\_directory\_name*

*As shown in the following example, the system displays the apply level screen of the cbm maintenance interface, which shows a list of all packages in the source directory that you specified.*

## Example of apply level showing the CD-ROM source directory

```

xterm
  CBM      MATE     NET      APPL     SYS      HW      CLI: SN100
  *        -       *       *       *       *       Host: SN100_CBM
                                     Active

Apply
0 Quit
2 Source
3 Reload
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh

Source: the directory /cdrom/cdrom/applications/cbm/packages.
Filter: sdm Interactive Mode: OFF
# Package Description          Version      Status
-----
1 Platform Utilities          20.82.8.0   APPLIED
2 Table Access Service        20.82.8.0   APPLIED
3 Bootpd and tftpd           20.82.8.0   NOT APPLIED
4 SSH Core File Transfer      20.82.8.0   NOT APPLIED
5 SDM Billing Application      20.82.8.0   NOT APPLIED
6 Reach Through SPM          20.82.8.0   NOT APPLIED
7 Passport Log Streamer      20.82.8.0   NOT APPLIED
8 OSS Comms Svcs             20.82.8.0   NOT APPLIED
9 OSS and Application Svcs    20.82.8.0   NOT APPLIED
10 OM Access Service          20.82.8.0   APPLIED
11 OM Delivery                 20.82.8.0   NOT APPLIED

Packages on the source: 1 to 11 of 26

root
Time 15:50 >

```

- 5 In the list of packages, locate the packages to be applied and take note of their numbers (located next to the names of the packages). Select the packages that you have decided to apply:

```
select <package number> ... <package number>
```

where

**<package number>**

is the number associated with a package, that you noted. Each package number is separated by preceding and succeeding spaces.

### Example

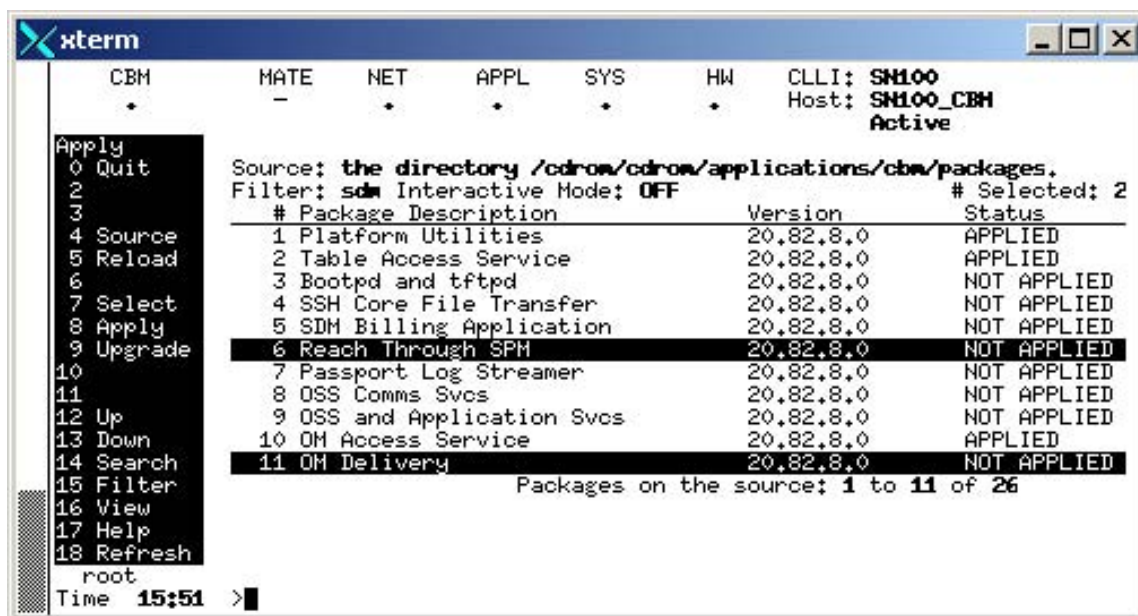
To select the Reach Through SPM application, which is number 6, and OM Delivery, which is number 11 in the sample screen display shown in the previous figure, enter

```
select 6 11
```

To de-select any packages that you selected, re-enter the select command for the packages you want to de-select. The highlighting on the packages that you de-select will be removed.

*The packages you selected are highlighted on the cbmmtc apply screen, as shown in the following figure.*

## Example of selecting packages to apply



```
xterm
  CBM      MATE     NET      APPL     SYS      HW      CLI: SN100
  *        -        *        *        *        *      Host: SN100_CBM
                                     Active

Apply
0 Quit
2 Source
3 Reload
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh

Source: the directory /cdrom/cdrom/applications/cbm/packages.
Filter: sdm Interactive Mode: OFF # Selected: 2
# Package Description Version Status
1 Platform Utilities 20.82.8.0 APPLIED
2 Table Access Service 20.82.8.0 APPLIED
3 Bootpd and tftpd 20.82.8.0 NOT APPLIED
4 SSH Core File Transfer 20.82.8.0 NOT APPLIED
5 SDM Billing Application 20.82.8.0 NOT APPLIED
6 Reach Through SPM 20.82.8.0 NOT APPLIED
7 Passport Log Streamer 20.82.8.0 NOT APPLIED
8 OSS Comms Svcs 20.82.8.0 NOT APPLIED
9 OSS and Application Svcs 20.82.8.0 NOT APPLIED
10 OM Access Service 20.82.8.0 APPLIED
11 OM Delivery 20.82.8.0 NOT APPLIED

Packages on the source: 1 to 11 of 26

root
Time 15:51 >
```

- 6 Apply the selected packages:  
**apply**
- 7 If a prerequisite package for the package(s) you have selected to apply is not already been applied on the system, the system SWIM tool will automatically select and apply the pre-requisite package unless the package is currently selected to be applied.

## Example of results screen after applying packages

```

xterm
  CBM      MATE     NET      APPL     SYS      HW      CLI: SN100
  *        -        *        *        *        *      Host: SN100_CBM
                                     Active

Apply
0 Quit
1
2
3
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 15:52 >

The following new packages have been selected for install.

NTttt1120 'Reach Through SPH' 20.82.8.0
NTowd20 'OH Delivery' 20.82.8.0

Do you wish to proceed?
Please confirm ("YES", "Y", "NO", or "N")

```

*The system prompts if you want to continue with applying the selected packages.*

- 8** Use the following table to determine your next step

If	Do
you want to continue the package application	step <a href="#">9</a>
you do not want to continue the package application	step <a href="#">12</a>

- 9** Type yes in response to the prompt.

*The status of each package application displays on the cbmmtc apply screen, as shown in the following figure.*

## Example apply level showing the status of applied packages

```

xterm
  CBM      MATE  NET  APPL  SYS  HW  CLI: SN100
  ISTb    -    .  ISTb  .    .  Host: SN100_CBM
                               Active
Apply
0 Quit
2
3
4 Source
5 Reload
6
7 Select
8 Apply
9 Upgrade
10
11
12 Up
13 Down
14 Search
15 Filter
16 View
17 Help
18 Refresh
root
Time 15:55 >
Source: the directory /cdrom/cdrom/applications/cbm/packages.
Filter: sdm Interactive Mode: OFF
# Package Description          Version      Status
-----
1 Platform Utilities          20.82.8.0   APPLIED
2 Table Access Service        20.82.8.0   APPLIED
3 Bootpd and tftpd            20.82.8.0   NOT APPLIED
4 SSH Core File Transfer      20.82.8.0   NOT APPLIED
5 SDM Billing Application      20.82.8.0   NOT APPLIED
6 Reach Through SPM          20.82.8.0   APPLIED
7 Passport Log Streamer      20.82.8.0   NOT APPLIED
8 OSS Comms Svcs              20.82.8.0   NOT APPLIED
9 OSS and Application Svcs    20.82.8.0   NOT APPLIED
10 OM Access Service          20.82.8.0   APPLIED
11 OM Delivery                 20.82.8.0   APPLIED
Packages on the source: 1 to 11 of 26

```

- 10 When the application is completed, the installed packages will appear in the list that displays when you enter the `cbmmtc` packages level. Verify that the status of the new packages indicates Applied under the Status column.

### ATTENTION

It is important that packages installed on the system not be left with a Partial status. If any package installed application fails or otherwise shows a Partial status, contact your next level of support for assistance.

- 11 If applicable, review details about the CBM package application by performing procedure [Viewing software transaction history and logs on the CBM 850 on page 67](#), otherwise continue with step 13.
- 12 Type `no` in response to the prompt.
- 13 Exit from the `cbm` maintenance interface:  
**quit all**
- 14 You have completed this procedure. Return to step 9 of the higher level task flow or procedure [Installing optional software on a CBM 850](#).

## Procedure for cloning the image of the active node to the inactive node

This procedure enables you to clone the image of the active node onto the inactive node of a CBM 850 cluster.

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Cloning the image of the active node to the inactive node of a CBM 850 cluster

### *At your workstation*

- 1 Start the cloning process by typing  
**startb**  
and press the Enter key.
- 2 Use the following table to determine your next step.

If the system	Do
prompts you for the Ethernet address	step <a href="#">3</a>
indicates it is using Ethernet address <EthernetAddress>	record the IP address, then go to step <a href="#">8</a>

### *At the console connected to the inactive node*

- 3 Log in to the inactive node through the console using the root user ID and password.
- 4 If the system is not already at the OK prompt, bring the system to the OK prompt:  
**init 0**

- 5 At the OK prompt, display the Ethernet address of the inactive node:

**OK banner**

*Example response:*

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.
```

- 6 Record the Ethernet address that is displayed.

***At your workstation (session connected to Active node)***

- 7 Enter the Ethernet address of the inactive node you recorded in step [6](#).
- 8 Use the following table to determine your next step.

If the system	Do
prompts you to enter the command: boot net - image	step <a href="#">9</a>
does not prompt you to enter the command: boot net - image	step <a href="#">10</a>

***At the console connected to the inactive node***

- 9 When prompted, boot the inactive node from the image of the active node by typing

**OK boot net - image**

and press the Enter key.

**Note:** There must be a space after the dash.

*Example response:*

```
SC Alert: Host System has Reset
```

```
Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.
```

```
Rebooting with command: boot net - image
```

```
.
.
.
```

```
SC Alert: Host System has Reset
```

### ***At your workstation (session connected to the Active node)***

- 10** Monitor the progress of the cloning from the active node. Cloning the inactive node takes approximately one hour to complete.

#### *Example response:*

```
Waiting for network response from
unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Deleted snapshot 0.
Deleted snapshot 1.
Deleted snapshot 2.
Deleted snapshot 3.
d99: Soft Partition is cleared
```

- 11** You have completed this procedure. Return to step [11](#) of the higher level task flow or procedure [Installing optional software on a CBM 850](#).

### **Procedure for installing the Backup Restore Manager software**

This procedure enables you to install the Backup Restore Manager software. The Backup Restore Manager application functionality requires the appropriate software resident and configured on platforms that require synchronized imaging. Although no Core and Billing



Manager 850 data is backed up through the Backup Restore Manager, the Backup Restore Manager software must be installed on the CBM 850 to allow control of the XA-core and 3PC (Compact) backup.

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ATTENTION

Instructions for entering commands in this procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Installing the Backup Restore Manager software

### At the *Cl* prompt on the core

- 1 Enter the following command:

```
permit <backupuser> <backupuser_pswd> 4 10000  
english all
```

where

**<backupuser>**

is the user name for the core, that is up to 16 characters in length, that will be used by SBRM for login

**<backupuser\_pswd>**

is the password for the <backupuser> user you are creating, which can be up to 16 characters in length

**4**

is the priority

**10000**

is the stack size

**english**

the language setting

**all**

is the privilege setting

**Note 1:** If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

**Note 2:** If Enhanced Password Control is in effect on the CM and after the user is permitted on the switch, log in to the core manually with this user first. The core will prompt you to

change the password at the first login after the login is permitted. Change the password and then perform step [1](#) again.

The SBRM does not have the ability to manage passwords. Therefore, you must re-run the configuration script in step [4](#).

### ***At your workstation***

- 2 Apply the software application package, NTbkupmgr by performing the procedure [Applying software packages on a CBM 850 using the CBMMTC interface on page 56](#). Specify /cdrom/cdrom/applications/cbm/packages as the source directory when you perform that procedure.
- 3 When the installation is complete, exit from the cbmmtc.
- 4 At the command line prompt, change directory to the directory containing configuration script:  

```
cd /opt/nortel/bkresmgr/cbm/scripts
```
- 5 Run the configuration script:  

```
./bkmgr_config.sh
```
- 6 You are first prompted for the user name. The user name is that used to log in to the core to initiate an image dump. The script restricts the user name to a maximum of 16 characters. The user name entered must first be enabled on the core in step [1](#)
- 7 You are prompted for the user name you entered in step [6](#)).
- 8 You are first prompted for the password. The configuration script restricts the password to a maximum of 16 characters. Use the password set up in step [1](#)
- 9 You are prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored.  

**Note:** Verify that this device has enough space to store the backup.
- 10 You are prompted for the core type, either XA-core or Compact.  

**Note:** This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 11 You have completed this procedure. Return to step [9](#) of procedure [Installing optional software on a CBM 850](#).

## Viewing software transaction history and logs on the CBM 850

### Purpose

This procedure enables you to view additional details about the package transactions, either package configuration or package removal, that you have performed on a CBM 850.

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ATTENTION

Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Viewing software transaction history and logs on the CBM 850

#### *At your workstation*

- 1 This procedure enables you to view logs that are local to each of the nodes in the CBM 850 cluster. Therefore, you must first choose the node in the cluster for which you want to view logs and then create a connection to that node.

If	Do
you are already connected to the CBM 850 for which you want to view logs	step <a href="#">4</a>
you are not already connected to a CBM 850 for which you want to view logs	step <a href="#">2</a>

- 2 Using SSH, open a connection to the node in the CBM 850 cluster for which you want to view logs and log in as the root user:

```
ssh -l root <ip_address>
```

where

**<ip\_address>**

is the IP address of the CBM 850 node for which you want to view logs

- 3 Enter the password for the root user.
- 4 Determine the next step to perform.

If	Do
you have already accessed the cbmmtc user interface	step <a href="#">6</a>
you have not accessed the cbmmtc user interface	step <a href="#">5</a>

- 5 Type the following on the command line:
 

```
cbmmtc
```
- 6 Type the following on the command line located at the bottom of the cbmmtc user interface screen:
 

```
history
```

*The system displays the information about the package transactions you have performed, including a log file and the results of the individual operations. Included also in this information is an indication as to the node on which the operations were performed. If the operations were performed on the active node, no special identifier, is provided. However, if the operations were performed on the inactive node, the inactive node identifier appears in the information displayed.*
- 7 If applicable, you can view more details about a specific log displayed in the history command output by typing:
 

```
ViewLog <#>
```

where

```
<#>
```

is the number of the log in the log file.
- 8 Exit from the cbmmtc user interface:
 

```
quit all
```
- 9 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Configuring the bkmgrusr user ID and password to enable communication between the DBRM and SBRM

### Purpose

This procedure enables you to configure the bkmgrusr user ID and password in order for the Synchronous Backup Restore Manager (SBRM) to communicate with the Device Backup Restore Manager (DBRM) on the CS 2000 Core Manager.

**Note:** This procedure applies only to the CS 2000 Core Manager running on an AIX platform. The procedure does not apply to the Core and Billing Manager (CBM) running on an SSPFS-based server.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN10170-611
Displaying actions a user is authorized to perform	CS 2000 Core Manager Security and Administration, NN10170-611

### Procedure

#### Configuring the bkmgrusr user ID and password for communication with SBRM

##### *At your workstation*

- 1 Log into the CS 2000 Core Manager on which the DBRM is installed as a user authorized to perform config-admin actions.

- 2 Create the user, "bkmgrusr":  
**mkuser bkmgrusr**
- 3 Create the groups, "emsmtc", "emsadm", and "emsrw":  
**mkgroup emsmtc**  
**mkgroup emsadm**  
**mkgroup emsrw**
- 4 Add the bkmgrusr user to the primary group, "maint", and to secondary groups, "emsmtc", "emsadm", "emsrw":  
**chuser pgrp=maint groups=emsmtc,emsadm,emsrw**  
**home=/export/home/bkmgrusr admin=true**  
**shell=/bin/ksh bkmgrusr**  

*Note:* Although it may be unclear from the command syntax shown above, this command is entered on a single line. Therefore, when you enter this command, ensure that there is a space between emsrw and home, and that there is a space between ksh and bkmgrusr
- 5 Confirm that the bkmgrusr user has been added to the required groups in step 4:  
**groups bkmgrusr**  

The system will display the groups that are associated with the bkmgrusr user.
- 6 Set the password for the bkmgrusr user:  
**passwd bkmgrusr**  

*Note:* The bkmgrusr user is disabled until this step is performed.
- 7 Log out of the CS 2000 Core Manager and then log back in as "bkmgrusr".  

When the system prompts you, change the password for the bkmgrusr user.
- 8 Change to the home directory and create the ".ssh" directory:  
**cd /export/home/bkmgrusr**  
**mkdir .ssh**  
**chmod 700 .ssh**
- 9 You have completed this procedure.

## Configuring core access for SBRM through the CS 2000 Core Manager

### Purpose

This procedure enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). This procedure must be performed before the SBRM can automatically backup a core image.

**Note 1:** Perform the procedure, [Creating the backup user ID on the core for SBRM on page 73](#) before you perform this procedure for the first time.

**Note 2:** This procedure should be performed to whenever the password for the core user password expires or is changed. This ensures that the password you set in this procedure matches that set for the user on the core.

### Prerequisites

You must be a user authorized to perform config-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Procedures related to this procedure

Procedure	Document
Logging in to the CS 2000 Core Manager	Security and Administration
Displaying actions a user is authorized to perform	Security and Administration

### Procedures

#### Configuring core access for SBRM through the CS 2000 Core Manager

##### *At the CS 2000 Core Manager*

- 1 Log into the core manager with the login ID and password for a user authorized to perform config-admin actions.

- 2 Use the following table to determine your next step.

If	Do
you wish to perform this procedure on the command line	step <a href="#">3</a>
you wish to perform this procedure through SDMMTC (SDM maintenance interface)	step <a href="#">5</a>

- 3 At the command line prompt, change directory to the directory containing appropriate configuration script:
- ```
cd /opt/nortel/bkresmgr/cbm/scripts
```
- 4 Run the configuration script:
- ```
./bkmgr_config.sh
```
- Go to step [7](#).
- 5 Access the config level of the SDM maintenance interface:
- ```
# sdmmtc config
```
- 6 From the list of filesets that displays, select the Succession Provisioning Data Sync Manager fileset (Backup Restore Manager fileset, SDM\_BKM.bkm) and then type config.
- 7 As the configuration script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, [Creating the backup user ID on the core for SBRM on page 73](#)
- 8 As the script continues to run, you are then prompted for the user you entered (in step [7](#)). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, [Creating the backup user ID on the core for SBRM on page 73](#)
- 9 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.
- 10 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 11 You have completed this procedure.



---

## Creating the backup user ID on the core for SBRM

---

### Purpose

This procedure enables you to create the user ID on the core to enable the operation of the Synchronous Backup Restore Manager (SBRM). The types of operations that can be performed by this user are:

- set dump\_restore\_in\_progress field in ofcstd table
- start image dump
- ability to run itocci command set
- ability to perform diskut commands

**Note 1:** This procedure should be performed before you first perform the procedure, “Configuring core access for SBRM”.

**Note 2:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedure

#### Creating the backup user ID on the core for SBRM

##### *At the CLI prompt on the core*

- 1 Enter the following command:

```
permit <backupuser> <backupuser_pswd> 4 10000  
english all
```

where

**<backupuser>**

is the user name for the core, that is up to 16 characters in length, that will be used by SBRM for login

**<backupuser\_pswd>**

is the password for the <backupuser> user you are creating, which can be up to 16 characters in length

**4**

is the priority

**10000**

is the stack size

**english**

the language setting

**all**

is the privilege setting

**Note 1:** If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

**Note 2:** If Enhanced Password Control is in effect on the CM and after the user is permitted on the switch, log into the core manually with this user first. The core will prompt you to change the password at the first login after the login is permitted. Change the password and then perform the procedure, “Configuring core access for SBRM” using the <backupuser> user you have created and the changed password.

The SBRM does not have the ability to manage passwords. Therefore, you must re-run the configuration script in “Configuring core access for SBRM” to ensure that the password for the <backupuser> user

- 2 You have completed this procedure.

## Configuring core access for SBRM through the CBM 850

### Purpose

This procedure enables you to configure access to the core for the Synchronous Backup Restore Manager (SBRM). This procedure must be performed before the SBRM can automatically backup a core image.

**Note 1:** Perform the procedure, [Creating the backup user ID on the core for SBRM on page 73](#) before you perform this procedure for the first time.

**Note 2:** This procedure should be performed whenever the password for the core user password expires or is changed. This ensures that the password you set in this procedure matches that set for the user on the core.

### Prerequisites

In order to perform this procedure, you must have the following authorization and access.

- You must be a user in a role group authorized to perform config-admin actions.
- You must obtain non-restricted shell access.

For more information on how to log in to the CBM as an authorized user, how to request a non-restricted shell access, or how to display actions a role group is authorized to perform, review the procedures in the following table.

| Procedure                                                | Document                                                              |
|----------------------------------------------------------|-----------------------------------------------------------------------|
| Logging in to the CBM                                    | Core and Billing Manager 850 Security and Administration, NN10358-611 |
| Requesting non-restricted shell access                   | Core and Billing Manager 850 Security and Administration, NN10358-611 |
| Displaying actions a role group is authorized to perform | Core and Billing Manager 850 Security and Administration, NN10358-611 |

## Procedure

### Configuring core access for SBRM

#### *At your workstation*

- 1 Log into the Core and Billing Manager 850 (CBM 850).
- 2 Log into the core manager as a user authorized to perform config-admin actions.
- 3 Change to the root user:  

```
su - root
```
- 4 When prompted, enter the root password.
- 5 Change directory to the directory containing appropriate configuration script:  

```
cd /opt/nortel/bkresmgr/cbm/scripts
```
- 6 Run the configuration script:  

```
./bkmgr_config.sh
```
- 7 As the script runs, you are first prompted for the user name. The user name is that which will be used to login to the core in order to initiate an image dump. The script restricts the name to a maximum of 16 characters. The user name you enter must first have been enabled on the core through the procedure, [Creating the backup user ID on the core for SBRM on page 73](#)
- 8 As the script continues to run, you are then prompted for the user you entered (in step 7). The script restricts the password to a maximum of 16 characters. This password is the one that was set up through the procedure, [Creating the backup user ID on the core for SBRM on page 73](#)
- 9 As the script continues to run, you are then prompted for the logical volume where the backup is to be stored. This is the device on which the core image dump will be stored. You should ensure that this device has enough space to store the backup.
- 10 As the script continues to run, you are then prompted for the core type, either xa-core or Compact. This information is needed in order for the software to know whether the core will also have a Message Switch load.
- 11 You have completed this procedure.

---

## Configuring SSH between the backup restore manager servers

---

### Application

Use this procedure to configure the secure shell (SSH) between the Integrated Element Management system (IEMS) server where the synchronous backup restore manager (SBRM) software is installed, and the SPFS-based servers where the device backup restore manager (DBRM) software is installed.

**Note:** Throughout the remainder of this procedure, the IEMS server will be referred to as the SBRM server and the SPFS-based servers will be referred to as the DBRM servers.

SSH provides authentication and secure communications over insecure channels.

This procedure contains the steps to generate the SSH key pair on the SBRM server and transfer the key pair to each DBRM server and the SDM platform in the network. It also contains the steps to transfer an existing SSH key pair from the SBRM server to new or existing DBRM servers and the SDM platform in the network.

### Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password for the SBRM server
- you need the password for the bkmgrusr on the DBRM server to transfer the SSH key pair

**Note:** The bkmgrusr is created on the DBRM server when SPFS is installed.

- you need the root password for the DBRM server when the DBRM server is a two-server configuration, to synchronize the SSH data between the two servers

### Action

Perform the following steps to complete this procedure.

#### **At your workstation**

- 1 Log in to the SBRM server by typing  
> **telnet <server>**  
and pressing the Enter key.  
where

**server**

is the IP address or host name of the IEMS server where the SBRM software is installed

**Note:** In a two-server configuration, log in to the Active server using its physical IP address.

- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  
**\$ su -**  
and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager configuration script is located by typing  
**# cd /opt/bkresmgr/admin/bin**  
and pressing the Enter key.
- 6 Run the backup restore manager configuration script by typing  
**# ./configure**  
and pressing the Enter key.

Example response:

```
Backup Restore Manager Configuration
```

```
1 - Backup Restore Manager SSH Setup
2 - Automated Synchronous Backup Restore
   Manager Service
```

```
X - exit
```

```
select - [X, 1-2]
```

- 7 Enter the number next to the “Backup Restore Manager SSH setup” option in the menu.

Example response:

SSH Setup for Synchronous Backup Restore Manager

- 1 - Generate SSH key and transfer to Device Backup Restore Manager servers
- 2 - Transfer existing SSH key to Device Backup Restore Manager servers

X - exit

select - [X, 1-2]

- 8** Use the following table to determine your next step.

| If you are                                                       | Do                      |
|------------------------------------------------------------------|-------------------------|
| configuring SSH for the first time, or changing the SSH key pair | step <a href="#">9</a>  |
| transferring the SSH key pair to a new or existing DBRM server   | step <a href="#">22</a> |

- 9** Enter the number next to the “Generate SSH key and transfer to Device Backup Restore Manager servers” option in the menu.

Example response:

Generate SSH key for Synchronous Backup Restore Manager and transfer to Device Backup Restore Manager servers.

WARNING: Running this script will generate a new SSH key for the bkmgrusr.

This new SSH key must be transferred to all existing and new Device Backup Restore Manager servers.

Do you want to continue? [y/n]:

- 10** When prompted, confirm you want to continue by typing **y** and pressing the Enter key.

Example response:

```
Generating SSH key for bkmgrusr.  
Sun Microsystems Inc. SunOS 5.9          Generic  
May 2002  
Generating public/private rsa key pair.  
Enter file in which to save the key  
(/export/home/bkmgrusr/.ssh/id_rsa):
```

- 11** When prompted, press the Enter key to accept the default location and filename “/export/home/bkmgrusr/.ssh/id\_rsa” for the key.

**Note 1:** If the default location and filename is not provided, enter “/export/home/bkmgrusr/.ssh/id\_rsa”.

**Note 2:** If the location and filename “/export/home/bkmgrusr/.ssh/id\_rsa” already exists and you wish to overwrite, enter y. Otherwise, enter n.

Example response:

```
Your identification has been saved in  
/export/home/bkmgrusr/.ssh/id_rsa.
```

```
Your public key has been saved in  
/export/home/bkmgrusr/.ssh/id_rsa.pub.
```

The key fingerprint is:

```
33:99:17:f0:ac:2a:3a:86:a9:d9:76:65:e6:70:4b:6  
:8 bkmgrusr@comp5iems
```

Synchronizing files IF clustered node

Transfer existing SSH key to Device Backup  
Restore Manager servers

WARNING: You must have the password for the  
bkmgrusr on the Device Backup Restore Manager  
server to transfer the SSH key.

Do you want to transfer the SSH key? [y/n]:

- 12** When prompted, confirm you want to transfer the SSH key pair by typing

**y**

and pressing the Enter key.



Example response:

```
Setting up to transfer SSH key to DBRM server.
```

```
Enter hostname or IP address of DBRM server to
transfer the SSH key to:
```

- 13** When prompted, enter the hostname or IP address of a DBRM server in your network.

Example response:

```
Platform type of DBRM server to transfer SSH key
to:
```

- 1 - SSPFS
- 2 - SDM

```
Enter platform type of DBRM server to transfer
SSH key to [1-2]:
```

- 14** When prompted, enter the number next to the platform type of the DBRM server.

**Note:** The SPFS platform type is for servers hosting the CS 2000 Management Tools, MG 9000 Manager and Core and Billing Manager (CBM). The SDM platform type is an AIX platform containing core management software.

Example response:

```
Sun Microsystems Inc. SunOS 5.9          Generic
May 2002
```

```
The authenticity of host 'comp5iems
(45.123.456.98)' can't be established.
```

```
RSA key fingerprint is
ff:eb:a8:87:14:d0:82:28:5c:43:70:5a:ab:af:e6:f
d
```

```
Are you sure you want to continue connecting
(yes/no)?:
```

- 15** When prompted, confirm you want to continue connecting by typing

**yes**

and pressing the Enter key.

```
Warning: Permanently added 'comp5iems
(45.123.456.98)' (RSA) to the list of known
hosts.
```

Password:

- 16** When prompted, enter the password for the bkmgrusr on the DBRM server.

Example response:

```
Transfer of SSH key to <server> complete.
```

```
Is DBRM <server> a High Availability (HA)
server? [y/n]:
```

- 17** When prompted, enter y if the DBRM server is a two-server configuration (HA), otherwise, enter n.

| If you entered | Do                      |
|----------------|-------------------------|
| y (yes)        | step <a href="#">18</a> |
| n (no)         | step <a href="#">21</a> |

**18**

#### ATTENTION

You need the password for the root user on the DBRM server to complete the steps that follow.

Example response:

```
WARNING: On HA DBRM servers, SSH setup is not
complete unless one of the following steps is
performed.
```

- a) The HA DBRM server <servername> is cloned.
- b) The SSH data on HA DBRM <servername> is manually synched.

```
WARNING: Choosing this option requires the
root password for <servername>
```

```
Do you want to manually synchronize the SSH data
on DBRM <servername> now [y/n]
```

- 19 When prompted, enter y if you want to manually synchronize the SSH data, otherwise, enter n.

| If you entered | Do                      |
|----------------|-------------------------|
| y (yes)        | step <a href="#">20</a> |
| n (no)         | step <a href="#">21</a> |

- 20 When prompted, enter the root password for the DBRM server  
Example response:  
Synchronization of SSH data on DBRM <servername>  
complete.
- 21 When prompted, indicate that you want to transfer the SSH key pair to the DBRM installation on the SBRM server in your network.  
**Note:** The SBRM always makes a SSH connection to the DBRM residing on the local server so that the local IEMS application is notified of the synchronized backup by way of SBRM to DBRM messaging.
- 22 Enter the number next to the “Transfer existing SSH key to Device Backup Restore Manager servers” option in the menu.  
Example response:  
Transfer existing SSH key to Device Backup  
Restore Manager servers  
  
WARNING: You must have the password for the bkmgrusr on the Device Backup Restore Manager server to transfer the SSH key.  
  
Do you want to transfer the SSH key? [y/n]:
- 23 Exit the “Backup Restore Manager SSH setup” level by typing  
**select - x**  
and pressing the Enter key.
- 24 Exit the “Backup Restore Manager Configuration” level by typing  
**select - x**  
and pressing the Enter key.  
You have completed this procedure.



---

## Configuring the automated synchronous backup restore manager service

---

### Application

Use this procedure to configure the synchronous backup restore manager (SBRM) service on the SPFS-based server where the SBRM software is installed, for automated execution of backups. You can configure the SBRM service to execute backups on a weekly or daily basis

### Prerequisites

You need the root user ID and password for the SPFS-based server where the SBRM software is installed.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the SBRM server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the IEMS server where the SBRM software is installed

**Note:** In a two-server configuration, log in to the Active side using its physical IP address.

- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager configuration script is located by typing

```
# cd /opt/bkresmgr/admin/bin
```

and pressing the Enter key.

- 6 Run the backup restore manager configuration script by typing
- ```
# ./configure
```

and pressing the Enter key.

Example response:

```
Backup Restore Manager Configuration
```

```
1 - Backup Restore Manager SSH Setup
2 - Automated Synchronous Backup Restore
  Manager Service
```

```
X - exit
```

```
select - [X, 1-2]
```

- 7** Enter the number next to the “Automated Synchronous Backup Restore Manager Service” option in the menu.

Example response:

```
Automated Synchronous Backup Restore Manager
Service
```

```
1 - Configure Automated Synchronous Backup
  Restore Manager Service
2 - Start the Automated Synchronous Backup
  Restore Manager Service
3 - Stop the Automated Synchronous Backup
  Restore Manager Service
4 - View the Automated Synchronous Backup
  Restore Manager Service Configuration
```

```
X - exit
```

```
select - [X, 1-4]
```

- 8** View the configuration settings as follows:

- a** Enter the number next to the “View the Automated Synchronous Backup Restore Manager Service Configuration” option in the menu.

Example response:

```
The Automated Synchronous Backup Restore
Manager Service is not running
```

```
Automated Synchronous Backup Restore Manager
Service Configuration Settings
```

```
Backup Enabled           : N
Backup Day               : SUNDAY
Backup Hour              : 24
```

- b** Use the following table to determine your next step.

If you	Do
want to change the configuration settings of the SBRM service	step <a href="#">9</a>
do not want to change the configuration settings of the SBRM service	step <a href="#">11</a>

- 9** Change the configuration settings as follows:

- a** Enter the number next to the “Configure Automated Synchronous Backup Restore Manager Service” option in the menu.

Example response:

```
Automated Synchronous Backup Restore Manager
Service Configuration
```

```
Configuring the Automated Synchronous Backup
Restore Manager Service does not START the
service. Return to the previos menu and
select 'Start the Automated Synchronous
Backup Restore Manager Service' to start the
service.
```

```
Do you want the backup to run 1.daily or
2.weekly [1/2] :
```

- b** When prompted, enter the number next to daily or weekly.

Example response if daily is selected:

```
Hour to run the Synchronous Backup Restore
Manager based on 24 hour clock:
```

```
Example 1 is 1 AM, 12 is noon, and 24 is
midnight.
```

```
This is the hour on the <DAY> the Synchronous
Backup Restore Manager will execute a full
backup.
```

```
Enter hour to run the Synchronous Backup
Restore Manager (default: 24)
```

**Example response if weekly is selected:**

Day of the week to run the Synchronous Backup Restore Manager:

This is day of the week the Synchronous Backup Restore Manager will execute a full backup.

- 1 - MONDAY
- 2 - TUESDAY
- 3 - WEDNESDAY
- 4 - THURSDAY
- 5 - FRIDAY
- 6 - SATURDAY
- 7 - SUNDAY

Enter day of week to run the Synchronous Backup Restore Manager (default: SUNDAY):

If you selected	Do
weekly	step <a href="#">c</a>
daily	step <a href="#">d</a>

- c** When prompted, enter the number next to the day of the week on which you want the backup to execute, or press the Enter key to accept the default value if one is specified.

**Example response:**

Hour to run the Synchronous Backup Restore Manager based on 24 hour clock:

Example 1 is 1 AM, 12 is noon, and 24 is midnight.

This is the hour on the <DAY> the Synchronous Backup Restore Manager will execute a full backup.

Enter hour to run the Synchronous Backup Restore Manager (default: 24)

- d** When prompted, enter the time of day at which you want the backup to execute, or press the Enter key to accept the default value if one is specified.



**Example response:**

Automated Synchronous Backup Restore Manager Service Configuration complete.

Configuring the Automated Synchronous Backup Restore Manager Service does not START the service. Return to the previous menu and select 'Start the Automated Synchronous Backup Restore Manager Service' to start the service.

- 10** Use the following table to determine your next step.

<b>If you</b>	<b>Do</b>
want to start the automated SBRM service now	perform procedure <a href="#">Starting or stopping the automated synchronous backup restore manager service on page 91</a>
do not want to start the automated SBRM service now	step <a href="#">11</a>

- 11** Exit the “Automated Synchronous Backup Restore Manager Service” level by typing  
**select - x**  
and pressing the Enter key.
- 12** Exit the “Backup Restore Manager Configuration” level by typing  
**select - x**  
and pressing the Enter key.  
You have completed this procedure.



---

## Starting or stopping the automated synchronous backup restore manager service

---

### Application

Use this procedure to start or stop the synchronous backup restore manager (SBRM) service on the SPFS-based server where the SBRM software is installed.

### Prerequisites

You need the root user ID and password for the SPFS-based server where the SBRM software is installed.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the SBRM server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the IEMS server where the SBRM software is installed  
**Note:** In a two-server configuration, log in to the Active side using its physical IP address.
- 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 Change directory to where the backup restore manager configuration script is located by typing  

```
# cd /opt/bkresmgr/admin/bin
```

and pressing the Enter key.
- 6 Run the backup restore manager configuration script by typing  

```
# ./configure
```

and pressing the Enter key.

**Example response:**

Backup Restore Manager Configuration

- 1 - Backup Restore Manager SSH Setup
- 2 - Automated Synchronous Backup Restore Manager Service

X - exit

select - [X, 1-2]

- 7** Enter the number next to the “Automated Synchronous Backup Restore Manager Service” option in the menu.

**Example response:**

Automated Synchronous Backup Restore Manager Service

- 1 - Configure Automated Synchronous Backup Restore Manager Service
- 2 - Start the Automated Synchronous Backup Restore Manager Service
- 3 - Stop the Automated Synchronous Backup Restore Manager Service
- 4 - View the Automated Synchronous Backup Restore Manager Service Configuration

X - exit

select - [X, 1-4]

- 8** Use the following table to determine your next step.

If you want to	Do
start the automated SBRM service	step <a href="#">9</a>
stop the automated SBRM service	step <a href="#">10</a>

- 9** Start the SBRM service as follows:
- a** Enter the number next to the “Start the Automated Synchronous Backup Restore Manager Service” option in the menu.

**Example response:**

```
Start the Automated Synchronous Backup
Restore Manager Service
```

```
WARNING: Running this script will start the
Automated Synchronous Backup Restore Manager
Service
```

```
Starting the service does not initiate a
backup until the day and time configured.
```

```
Do you want to continue? - [y/n]:
```

- b** When prompted, confirm you want to start the SBRM service by typing

**y**

and pressing the Enter key.

**Example response:**

```
Registering with SERVMAN.
```

```
Starting the Automated Synchronous Backup
Restore Manager Service.
```

```
Starting AUTO_BACKUP_MANAGER through
servstart AUTO_BACKUP_MANAGER Started
```

- c** Proceed to step [11](#).

**10** Stop the SBRM service as follows:

- a** Enter the number next to the “Stop the Automated Synchronous Backup Restore Manager Service” option in the menu.

**Example response:**

```
Stop the Automated Synchronous Backup Restore
Manager Service
```

```
WARNING: Running this script will stop the
Automated Synchronous Backup Restore Manager
Service
```

```
Stopping the service does not abort a backup
in progress.
```

```
Do you want to continue? - [y/n]:
```

- b** When prompted, confirm you want to stop the SBRM service by typing

**y**

and pressing the Enter key.

Example response:

```
Stopping the Automated Synchronous Backup  
Restore Manager Service.
```

```
Stopping group using servstop  
AUTO_BACKUP_MANAGER Stopped
```

```
Deregistering with SERVMAN
```

- 11** Exit the “Automated Synchronous Backup Restore Manager Service” level by typing

**select - x**

and pressing the Enter key.

- 12** Exit the “Backup Restore Manager Configuration” level by typing

**select - x**

and pressing the Enter key.

You have completed this procedure.

---

## Invoking the synchronous backup restore manager through telnet

---

### Application

Use this procedure to run various portions of the synchronous backup restore manager (SBRM) process from the backup manager CLUI on an SPFS-based server where the Device Backup Restore Manager (DBRM) software resides, rather than from the CLUI on the Integrated Element Management System (IEMS) server where the Synchronous Backup Restore Manager (SBRM) software resides.

**Note:** All backups will be stored in a common file location. For example, “/data/bkresmgr/backup”.

### Prerequisites

You need the root user ID and password for the SPFS-based server on which you are running the various portions of the SBRM process.

### Action

Perform the following steps to complete this procedure.

#### *At your workstation*

- 1 Log in to the SPFS-based server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SPFS-based server on which you are running the various portions of the SBRM process  
**Note:** In a two-server configuration, log in to the Active side using its physical IP address.
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Change directory to where the backup restore manager script is located by typing  

```
# cd /opt/nortel/bkresmgr/nbm
```

and pressing the Enter key.

- 6 Start the backup restore manager by typing

```
# ./bkmgr
```

and pressing the Enter key.

- 7 Invoke the desired step of the backup process by typing

```
bkmgr> <command>
```

where

**command**

is any one of the following commands:

- precheck
- stopprov
- dumpdata
- verify
- startprov
- activatenew

Refer to [Additional information on page 96](#) for further information on commands.

You have completed this procedure.

## Additional information

The following commands are available through telnet:

- **commands**: Lists all the commands that are available in the SBRM CLUI.
- **help [command]**: Displays information on the command, or all commands if no command is specified.
- **exit** or **quit**: Exits the SBRM CLUI.
- **query status**: Displays the status of the backup at a high level. For example, "Backup in progress" or "Backup failed".
- **query history**: Displays information about most recent backup. For example, "Last backup executed <date> <time> successful".
- **query inventory**: Displays the components available for backup.
- **precheck**: Performs a basic sanity check to ensure the system is in a state to perform a backup. For example, disk space check and subtending application health if applicable.
- **stopprov**: Stops the provisioning process.



- `dumpdata`: Backs up the critical data.
- `startprov`: Starts the provisioning process (if stopped)
- `verify`: Checks the validity of the backed up data. For example, validates the database data.
- `activatenew`: Marks the new backup data as the current backup.

The following commands are not available through telnet:

- `backup full`: Performs a complete backup. If a failure is encountered, the process stops, and manual intervention is required to recover from the failure.
- `backup auto`: Performs a complete backup. If a failure is encountered, the backup process will restore provisioning if it was stopped by the backup process.
- `backup abort`: Aborts the backup after completion of the current step, and restarts provisioning if it was stopped by the backup process.



---

## How to backup an XA-Core office image from disk to tape

---

### Application

Use this procedure to copy the office image files of an eXtended Architecture Core (XA-Core). Use this procedure to copy the office image files from a disk to a digital audio tape (DAT) cartridge in an XA-Core shelf.

### Interval

Perform this procedure each week or as indicated in the routine maintenance schedule for your office.

### Common procedures

There are no common procedures.

### Action

This procedure contains a summary flowchart and a list of steps. Use the flowchart to review the procedure. Follow the steps to perform this procedure.

#### How to backup an XA-Core office image from disk to tape

##### *At the MAP*

- 1 To access the MAP CI level display, type:  
**>QUIT ALL**  
and press the Enter key.  
Example of a MAP response  
CI:
- 2 To access the image table of contents (ITOC) user interface, type:  
**>ITOCCI**  
and press the Enter key.  
Example of a MAP response  
ITOC User Interface is now active.  
ITOCCI:
- 3 To list the boot file for the XA-Core in ITOC, type:  
**>LISTBOOTFILE XA**  
and press the Enter key.

### Example of a MAP response

Image table Of Contents for XA :

```

A Registered          Generic Device File
L Date              Time                Name
R MM/DD/YYYY HH:MM:SS
-----
0 * 05/17/1999 19:26:29 F02LIMAGE
IMG0517CY_CM

```

**Note:** The example of a MAP response identifies the autoload registered (ALR) image file by an asterisk (\*) in the ALR column. Each image file has an index number at the beginning of the tuple line. The ALR image in the example of a MAP response has an index number of 0. The XA-Core selects the ALR image file first to boot the switch. If the ALR image file does not boot the switch then the XA-Core selects the next image file. The next image file is by sequence of the index number from the top of the table.

- 4 To list the boot file for the message switch (MS) in ITOC, type

>**LISTBOOTFILE MS**

and press the Enter key.

### Example of a MAP response

Image Table of Contents for MS :

```

A Registered          Generic Device File
L Date              Time                Name
R MM/DD/YYYY HH:MM:SS
-----
0 * 05/17/1999 19:26:29 F02LIMAGE
IMG0517CY_MS

```

- 5 Determine if the XA-Core and MS have image files that are autoload registered (ALR). The examples of a MAP response in steps <3> and <4> identify the ALR image files by an asterisk (\*) in the ALR column.

**If the image files are**

**Do**

ALR

step [6](#)

not ALR

step [24](#)

- 6 Record the names of the office image files for XA-Core and MS that are ALR. Also record the volume name that has these office image files. The ALR image file is the file that you copy to the XA-Core tape.

**Note 1:** In the example of a MAP response in step 3, the name of the office image file for XA-Core is IMG0517CY\_CM. Image file IMG0517CY\_CM is ALR. Image file IMG0517CY\_CM is in volume F02LIMAGE.

**Note 2:** In the example of a MAP response in step 4, the name of the office image file for the MS is IMG0517CY\_MS. Image file IMG0517CY\_MS is ALR. Image file IMG0517CY\_MS is in volume F02LIMAGE.

- 7 To quit the ITOCCI user interface, type:

>QUIT

and press the Enter key.

Example of MAP response

CI :

### ***At the shelf***

- 8



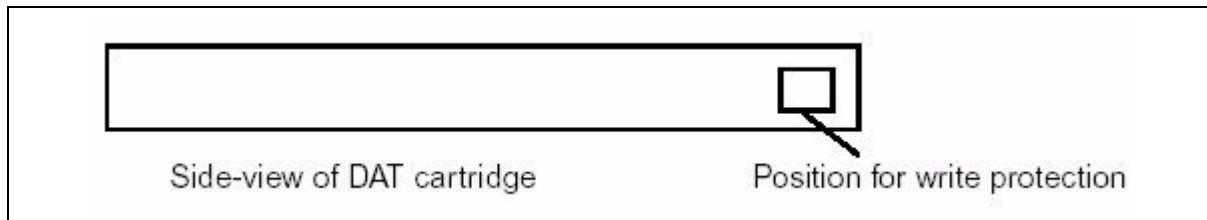
#### **WARNING**

**Static electricity damage**

Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape and packlet. The use of the wrist strap protects the packlets against damage caused by electrostatic discharge (ESD).

- Determine from office records or office personnel if the DAT tape drive is clean. Refer to the XA-Core procedure "How to clean the XA-Core tape drive" in the XA-Core Maintenance Manual, 297-8991-510.
- 9 Get a tape cartridge that has the approval of Nortel Networks. Determine the tape planned for a backup of an office image. Determine the tape to use from the office records or from office personnel.
  - 10 Make sure the tape write protection is at the position that permits recording (closed). The tape write protection is an entrance on one side of the tape that has a sliding door. The sliding door is open for write protection and closed to allow a write to the tape.


## Write protection of DAT cartridge



- 11 Insert the DAT tape cartridge into the XA-Core tape drive and close the drive door. The XA-Core tape drive is in the input/output processor (IOP) card of the XA-Core shelf.

### At the MAP

12



**CAUTION**  
File of tape lost when formatted  
If the tape had files, the formatting of the tape loses the files. Make sure the tape has no files that your office needs.

To access the MAP disk utility, type:

```
>DISKUT
```

and press the enter key.

Example of a MAP response:

```
Disk utility is now active.
```

```
DISKUT:
```

- 13 To insert the tape in the MAP disk utility, type  

```
>INSERTTAPE snnpTAPE WRITELABEL label_name
```

and press the enter key.  
where  
  - s**  
is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device
  - nn**  
is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**  
is the upper (U) or lower (L) packlet position of the IOP that has the tape device

**label\_name**  
is the alphanumeric name of the tape label that records the data. The name can be up to 32 characters long. If blank spaces are in the label name then enclose the label name with quotation marks.

Example of MAP input:

```
>INSERTTAPE F02UTAPE WRITELABEL IMAGE_1
```

Example of a MAP response

```
*****          WARNING          *****
```

```
Writing the label IMAGE_1 to tape volume  
F02UTAPE on node CM will destroy all files  
stored on this tape volume.
```

```
Do you want to continue?
```

```
Please confirm ("YES", "Y", "NO", or "N")
```

**14** To confirm the command, type:

```
>YES
```

and press the enter key.

Example of a MAP response:

```
The INSERT operation may take up to 5 minutes to  
tension the tape.
```

```
A tape is now available to user on unit 0, node  
CM.
```

```
Name IMAGE_1 has been written to the tape label.
```

**15** To list the files in the volume that contains the office image, type:

```
>LISTFL vol_name
```

and press the enter key.

where

**vol\_name**  
is the name of the disk volume that contains the office image files

Example of MAP input

```
>LISTFL F02LIMAGE
```

**Example of a MAP response**

File information for volume F02LIMAGE:

{NOTE: 1 BLOCK = 512 BYTES }

```

-----
FILE NAME                O R I O O V FILE    MAX
NUM OF   FILE    LAST
                                R E T P L L CODE  REC
RECORDS  SIZE  MODIFY
                                G C O E D D LEN
IN        IN DATE
                                C N                FILE
BLOCKS
-----
IMG0517CY_MS            I F Y                0 1020
7542 15360 990517
IMG0517CY_CM            I F Y                0 1020
165180 329728 990517

```

**Note:** A volume can have more files listed by command LISTVOLS than by command LISTFL in the MAP disk utility. The difference in the number of files between the commands is because of directory files not displayed by command LISTFL.

- 16** Begin the disk to tape backup process. To create a backup copy of the XA-Core image file, type:

**>BACKUP FILE file\_name snpTAPE**

and press the Enter key.

where

**s**  
is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn**  
is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**  
is the upper (U) or lower (L) packlet position of the IOP that has the tape device



Example of MAP input:

```
>BACKUP FILE IMG0517CY_CM F02UTAPE
```

Example of a MAP response

FTFS file IMG0517CY\_CM on disk volume F02LIMAGE on node CM backed up as file IMG0517CY\_CM on tape device F02UTAPE on node CM.

If the command was	Do
successful	step <a href="#">17</a>
not successful	step <a href="#">24</a>

- 17 To create a backup copy of the MS image file, type:

```
>BACKUP FILE file_name snnp TAPE
```

and press the enter key.

where

**file\_name**

is the name of the MS image file that requires backup to tape

**s**

is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn**

is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**

is the upper (U) or lower (L) packlet position of the IOP that has the tape device

Example of MAP input

```
>BACKUP FILE IMG0517CY_MS F02UTAPE
```

Example of a MAP response

FTFS file IMG0517CY\_MS on disk volume F02LIMAGE on node CM backup up as file IMG0517CY\_MS on tape device F02UTAPE on node CM.

If the command was	Do
successful	step <a href="#">18</a>
not successful	step <a href="#">24</a>

- 18** To check the backup copies of the image files on the tape, type  
**>LISTFL snnpTAPE**  
and press the enter key.

where

**s**

is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn**

is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**

is the upper (U) or lower (L) packlet position of the IOP that has the tape device

Example of MAP input

**>LISTFL F02UTAPE**

Example of a MAP response

File information for tape volume F02UTAPE, node CM:

{Note: 1 BLOCK = 512 BYTES}

-----  
CREATE ORG FILE V FILE NUM OF REC FILE NAME

DATE TYPE CODE L SIZE IN RECORDS LEN

D BLOCKS IN FILE  
-----

990520 IMAG 0 329070 165180 1020 IMG0517CY\_CM

990520 IMAG 0 15026 7542 1020 IMG0517CY\_MS

- 19** To eject the tape from the MAP disk utility after the backup procedure completes, type

**>EJECTTAPE snnpTAPE**

and press the enter key.

where

**s**

is the front (F) or rear (R) shelf position of the input output processor (IOP) that has the tape device

**nn**

is the number of the slot position on the XA-Core shelf for the IOP that has the tape device

**p**

is the upper (U) or lower (L) packet position of the IOP that has the tape device

Example of MAP input

```
>EJECTTAPE F02TAPE
```

Example of a MAP response

The EJECT operation may take up to 5 minutes to position the tape to the beginning.

Rewind of tape F02UTAPE, unit 0, on node CM is completed.

This tape device is not available to the user now.

**20** To exit the MAP disk utility and return to the MAP CI level, type

```
>QUIT
```

and press the Enter key.

Example of a MAP response

CI:

### ***At the shelf***

**21**



#### **WARNING**

**Static electricity damage**

Wear a wrist strap connected to the wrist-strap grounding point of the frame supervisory panel (FSP) when you handle the tape and packet. The use of the wrist strap protects the packets against damage caused by electrostatic discharge (ESD).

Remove the tape cartridge from the tape drive. Set the tape write protection to the position that does not permit recording (open). The tape write protection is an entrance on one side of the tape that has a sliding door. The sliding door is open for write protection and closed to allow a write to the tape.

## Write protection of DAT cartridge



- 22** Store the tape cartridge per office procedure.
- 23** Go to step [25](#).
- 24** For additional help, contact the next level of support.
- 25** You have completed this procedure.

## Call Agent backup

The Call Agent uses two software loads. The first software load includes the platform software such as the operating system and system utilities. The second software load provides the call processing application.

This procedure describes how to make a backup of the call processing application. Images to be backed up are created either manually with the DUMP command, or automatically scheduled with entries in table IMAGEDEV and IMGSCHEM.

### At the MAP

- 1 List the available images to determine which image to backup. The image with the asterisk in the ALR column identifies the image that is set to Auto Load Record and is the image to backup.

```
CI:
>ITOCCI
ITOC User Interface is now active.
ITOCCI:
>LBF CM
Image Table Of Contents:
  A Registered          Generic Device      File
  L Date              Time
  R MM/DD/YYYY HH:MM:SS
-----
  0  01/22/2003  10:29:53  SD00IMAGE1      SN04_JAN07_CM
  1  01/22/2003  12:07:26  SD00IMAGE0      SN04_JAN22_CM
  2  01/22/2003  13:00:50  SD00IMAGE0      BOTHELL_010903
  3 * 01/30/2003  14:31:47  SD00IMAGE0      IMG_TO_BACKUP
```

### At the Call Agent Manager

- 2 Log in to the inactive Call Agent and change directory to the location of the image.

The location of the image is identified by the value in the Generic Device column as follows:

**/3PC**  
is prefixed in all cases

**sd0x/**  
is taken from the first four characters in the Generic Device name

**imagex/**

is taken from the remaining characters in the Generic Device name

```
[mtc@hostname mtc]$ cd /3PC/sd00/image0
[mtc@hostname image0]$ ls -l IMG_TO_BACKUP
-rw-r--r-- 1 root root 225820860 Feb 27 11:37 IMG_TO_
[mtc@hostname image0]$
```

**3****ATTENTION**

Do not modify files at this level. Any modification to files must be completed through the MAP.

Open a file transfer protocol (FTP) session to the CS 2000 Core Manager and transfer the file.

```
[mtc@hostname image0]$ ftp <core_manager_ip>
Connected to <core_manager_ip>
220 <core_manager_ip> SFTPD Server (Version 19.0.0.0 Nov 14
Name (<core_manager_ip>:mtc): root
Password: <root_passwd>
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd /swd/3pc
250 CWD command successful.
ftp> put IMG_TO_BACKUP
local: IMG_TO_BACKUP remote: IMG_TO_BACKUP
227 Entering Passive Mode (10,40,44,6,195,224)
150 Opening data connection for IMG_TO_BACKUP (binary mode)
226 Transfer complete.
225820860 bytes sent in 332 secs (6.7e+02 Kbytes/sec)
ftp> bye
221 Goodbye.
```

**At the SDM**

- 4** Insert a DAT cassette.

**At the CS 2000 Core Manager**

- 5 Verify that the size of the transferred file is the same as in [step 2](#) and copy the file to tape.

```
# cd /swd/3pc
# ls -l
total 19816
-rw-r--r-- 1 swld      swld      1527 Feb 27 12:40 000167C42C
-rw-r--r-- 1 swld      swld      1527 Feb 26 17:58 000F07C430
-rw-rw-rw- 1 ftpuser  maint    225820860 Feb 21 09:56 IMG_TO_B
# tar cvf /dev/rmt0 IMG_TO_BACKUP
```

**Note:** Use the `rvf` argument to append to the tape. After the backup completes, optionally verify the integrity of the backup by using `tar tvf /dev/rmt0` to view the contents of the tape.

- 6 Use the `rm` command to erase the oldest image so the volume does not fill up.
- 7 This procedure is complete.





---

## Backing up files to DVD-RW

---

### Application

Use this procedure to copy office images or all the files from a disk volume to a digital video disk read write optical disk (DVD-RW).

**Note:** Rewritable DVDs (DVD+RW) will not work. Use a blank DVD-RW (write once).

**CAUTION****Maximum one volume per DVD-RW**

Copy no more than one volume onto a DVD-RW. To copy multiple volumes, use a separate DVD-RW for each volume.

### Interval

Perform this procedure when required by your office.

### Common procedures

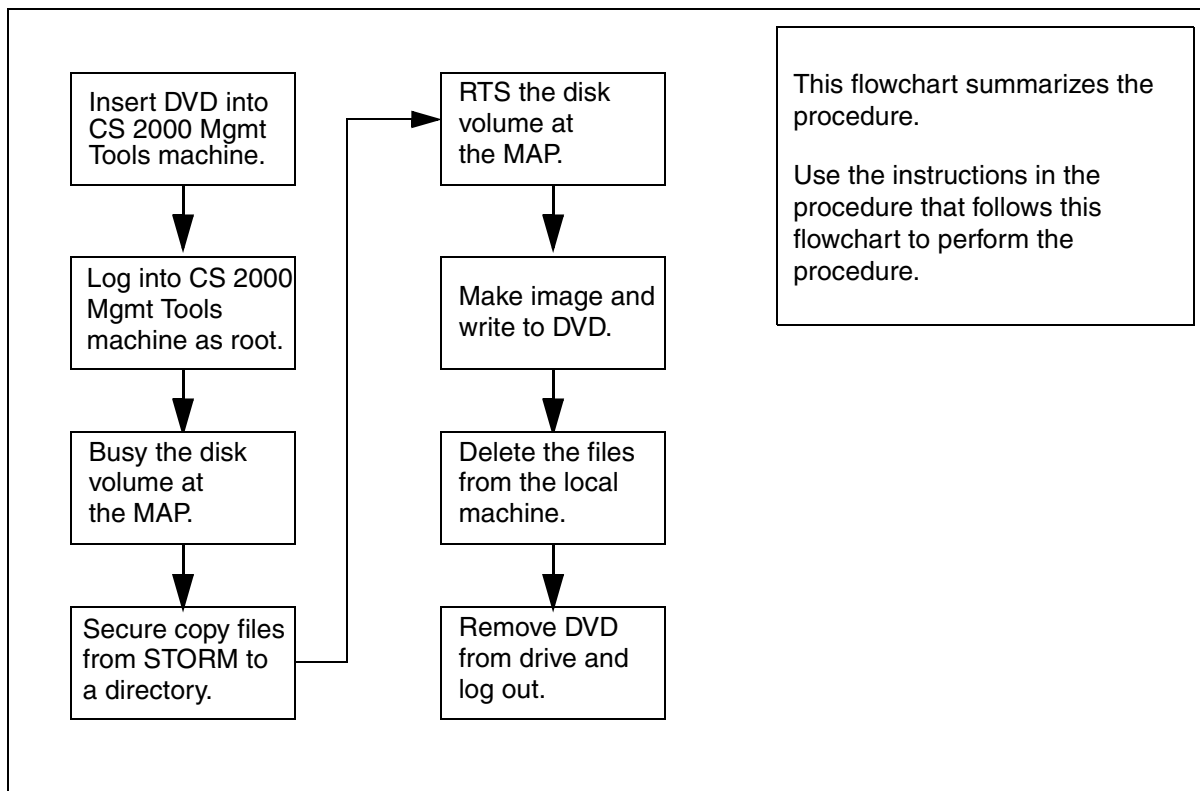
The UNIX commands `mkisofs` and `cdrw` are used. For information about these commands, type **man mkisofs** or **man cdrw** at a terminal prompt.

The IP addresses of the STORM units are determined in [step 1](#). The root password for STORM is needed. The root password for the CS 2000 Management Tools server is needed.

### Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

## Summary of backing up files to DVD-RW



### At the Call Agent Manager

- Quit the maintenance application and then use the mount command to determine the IP addresses of the STORM units.

```
> quit all
[mtc@ip_address mtc]$ mount
```

Determine which STORM unit provides sd00 and which provides sd01. This information is needed in [step 12](#).

```
[mtc@10.40.44.67 mtc]$ mount
/dev/ram0 on / type ext2 (rw)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,mode=0622)
10.40.44.238:/nfsserv/3pc/mtc/tape0 on /TAPE type nfs (rw,rsize=4096...
10.40.44.239:/nfsserv/3pc/mtc/tape1 on /TAPE1 type nfs (rw,rsize=409...
10.40.44.238:/nfsserv/3pc/cs/sd00 on /3PC/sd00 type nfs (rw,rsize=409...
10.40.44.239:/nfsserv/3pc/cs/sd01 on /3PC/sd01 type nfs (rw,rsize=409...
10.40.44.238:/nfsserv/3pc/mtc/log0 on /var/log_mate type nfs (rw,rsi...
10.40.44.239:/nfsserv/3pc/mtc/log1 on /var/log type nfs (rw,rsize=409...
```

**At the CS 2000 Management Tools server**

2

**CAUTION**

Maximum one volume

Copy only *one* volume onto a DVD-RW. To copy multiple volumes, use a separate DVD-RW for each volume.

Determine the volume to backup. Determine the volume from office records or from office personnel. Record the volume name.

- 3 Get a DVD-RW that has the approval of Nortel.
- 4 Insert the DVD-RW (write once DVD) into the DVD tray. If the CS 2000 Management Tools server is a pair of Sun Microsystems Netra 240 machines, put the DVD-RW into the machine with a lit USER LED on the faceplate.

**At a CS 2000 Management Tools server terminal**

- 5 Log in as a maintenance level user such as the maint user. Root permissions are used later in this procedure to write the DVD.
- 6 Change directory to `/data` and create a temporary directory to store the files:

```
$ cd /data
```

```
$ mkdir tmp
```

**Note:** Do not change directory into `tmp` now. The `tmp` directory will hold the data to backup.

- 7 Determine the environment shell:

```
$ env | grep SHELL
```

```
SHELL=/bin/ksh
```

- 8 Set a filesize creation limit for this instance of the shell. Choose the **one** that is applicable to your shell. `/bin/ksh` is the default shell:

```
for /bin/ksh:
```

```
$ ulimit -f 2929688
```

```
for /bin/bash:
```

```
$ ulimit -f 1464844
```

```
for /bin/csh:
```

```
$ limit filesize 1500 megabytes
```

### At the MAP

9 Determine the approximate size of the image or volume:

Data to backup	How to determine size																																																	
image	<p>Listfile the volume that the image is in:</p> <pre>&gt; DISKUT; LF &lt;vol_name&gt;</pre> <pre>&gt; LF SD00ADUMPO</pre> <p>File information for volume SD00ADUMPO: {NOTE: 1 BLOCK = 512 BYTES }</p> <pre>-----</pre> <table border="1"> <thead> <tr> <th>FILE NAME</th> <th>O R I O O V</th> <th>FILE</th> <th>MAX</th> <th>NUM OF</th> <th>FILE</th> <th>LAST</th> </tr> <tr> <th></th> <th>R E T P L L</th> <th>CODE</th> <th>REC</th> <th>RECORDS</th> <th>SIZE</th> <th>MODIFY</th> </tr> <tr> <th></th> <th>G C O E D D</th> <th></th> <th>LEN</th> <th>IN</th> <th>IN</th> <th>DATE</th> </tr> <tr> <th></th> <th>C N</th> <th></th> <th></th> <th>FILE</th> <th>BLOCKS</th> <th></th> </tr> </thead> <tbody> <tr> <td>S040210135002HIS</td> <td>O V</td> <td></td> <td>0 255</td> <td>276</td> <td>27</td> <td>040210</td> </tr> <tr> <td>S040210135002_CM</td> <td>I F Y</td> <td></td> <td>0 1020</td> <td>220288</td> <td>438855</td> <td>040210</td> </tr> <tr> <td>S040210135002_MS</td> <td>I F Y</td> <td></td> <td>0 1020</td> <td>7803</td> <td>15546</td> <td>040210</td> </tr> </tbody> </table> <pre>-----</pre> <p>The approximate size of the image in megabytes is NUM OF RECORDS IN FILE / 1000: <b>220288 / 1000 = 220 MB</b></p>	FILE NAME	O R I O O V	FILE	MAX	NUM OF	FILE	LAST		R E T P L L	CODE	REC	RECORDS	SIZE	MODIFY		G C O E D D		LEN	IN	IN	DATE		C N			FILE	BLOCKS		S040210135002HIS	O V		0 255	276	27	040210	S040210135002_CM	I F Y		0 1020	220288	438855	040210	S040210135002_MS	I F Y		0 1020	7803	15546	040210
FILE NAME	O R I O O V	FILE	MAX	NUM OF	FILE	LAST																																												
	R E T P L L	CODE	REC	RECORDS	SIZE	MODIFY																																												
	G C O E D D		LEN	IN	IN	DATE																																												
	C N			FILE	BLOCKS																																													
S040210135002HIS	O V		0 255	276	27	040210																																												
S040210135002_CM	I F Y		0 1020	220288	438855	040210																																												
S040210135002_MS	I F Y		0 1020	7803	15546	040210																																												
volume	<p>Listvols the volume with the megabyte option:</p> <pre>&gt; DISKUT; LV SD00TEMP MB</pre> <p>Subtract FREE MBYTES from TOTAL MBYTES to determine the approximate size of the volume: <b>400 - 340 = 60 MB</b></p>																																																	

10 If backing up an entire volume, enter the DISKADM level and busy the volume:

```
> QUIT ALL
> DISKADM <sd0x>; BSY <volname>
> QUIT
sd0x
is SD00 or SD01
```

**volname**

is the name of the volume such as TEMP or ADUMP0

*The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. Consider [step 13](#) to RTS the volume as soon as possible or convenient after copying the files.*

*If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.*

**At a CS 2000 Management Tools server terminal**

- 11 Ensure that enough disk space is available for the data to record. Twice the space determined in [step 9](#) is needed:

```
$ df -k /data
```

*The free space on the device that /data is mounted is printed. The value for “avail” is the number of free kilobytes. Divide that number by 1000 to determine the number of free megabytes. Ensure that there is free space for two times the size of the data to record.*

```
$ df -k /data
```

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/md/dsk/d20	3082223	144125	2876454	5%	/data

```
2876454 / 1000 = 2876 MB free
```

- 12 Secure copy the files from the STORM unit to the /data/tmp directory created in [step 6](#). Enter the root password for the STORM unit when prompted:

```
$ scp -r "root@<stormip>:</path_to_files>" /data/tmp
```

**Note:** There is a space before the /data/tmp argument.

**stormip**

is the IP Address of the STORM unit such as 10.40.44.238. Use the value determined in [step 1](#).

**/path\_to\_file**

is the absolute path to the files on the STORM unit to copy such as /nfsserv/3pc/cs/sd00/temp/\*

**Example**

Copy an office image named S040210135002\_CM from SD00ADUMP0:

```
$ scp -r
"root@<stormip>:/nfsserv/3pc/cs/sd00/adump0/S04021
0135002_CM" /data/tmp
```

**Note:** The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "yes." The root password for the STORM unit is needed.

*The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.*

**At the MAP**

- 13 If the volume was busied in [step 10](#), enter the DISKADM level and RTS the copied volumes:

```
> DISKADM <sd0x>; RTS <volname>
> QUIT
```

**At a CS 2000 Management Tools server terminal**

- 14 If only image files are transferred, and the files do not end in \_CM or \_MS, rename the files to include the file attributes IMG and 1020:

```
$ mv <image_filename> <image_filename>.IMG1020
```

**Example**

```
$ mv raleigh_04wk06 raleigh_04wk06.IMG1020
```

**Note:** If the name of the image already ends in \_CM or \_MS, skip this step.

- 15 Change directory out of /data/tmp and make an ISO9660 image named dvdimage.iso with Rock Ridge extensions from the files in tmp:

```
$ cd /data
$ mkisofs -R -o /data/dvdimage.iso -r /data/tmp
```

*Status is printed to the terminal:*

## Create dvdimage.iso with mkisofs command

```
$ mkisofs -R -o /data/dvdimage.iso -r /data/tmp
4.56% done, estimate finish Tue Feb 10 14:52:00 2004
9.11% done, estimate finish Tue Feb 10 14:52:00 2004
13.67% done, estimate finish Tue Feb 10 14:52:00 2004
...
95.67% done, estimate finish Tue Feb 10 14:52:05 2004
Total extents actually written = 109764
Total translation table size: 0
Total rockridge attributes bytes: 421
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 8000
109764 extents written (214 Mb)
$
```

- 16** Become the root user:

```
$ su - root
```

Provide the root password at the prompt.

- 17** Optionally verify the ISO9660 image:

```
# lofiadm -a /data/dvdimage.iso /dev/lofi/1
# mount -F hsfs /dev/lofi/1 /mnt
# ls -asl /mnt
```

*The contents of the ISO 9660 image are displayed. These files will be written to the DVD-RW. Ensure the display looks similar to the following image.*

**Note 1:** *If the lofiadm command reports the error “lofiadm: could not map file /data/dvdimage.iso to /dev/lofi/1: Device busy,” then the first loopback file driver is already in use. Reenter the command and substitute /dev/lofi/2 for /dev/lofi/1. Continue incrementing the number until the command succeeds and then use the successful value in the mount command.*

**Note 2:** *If the mount command reports the error “mount: /dev/lofi/1 is already mounted, /mnt is busy, or allowable number of mount points exceeded,” unmount the /mnt directory with the **umount /mnt** command and reenter the mount command.*

## List contents of the ISO 9660 image

```
# lofiadm -a /data/dvdimage.iso /dev/lofi/1
# mount -F hsfs /dev/lofi/1 /mnt
# ls -asl /mnt
total 431996
  4 dr-xr-xr-x  2 root  sys      2048 Apr 20 09:48 .
  2 drwxr-xr-x 33 root  root    1024 Apr 20 11:16 ..
431990 -rw-r--r--  1 maint maint 221178840 Apr 20 09:47 IMG_TO_BACKUP.img1
```

- 18 Determine the name of the DVD-RW device:

```
# cdrw -l
```

*All optical disk devices are printed.*

## Determine the DVD-RW device name

```
# cdrw -l
Looking for CD devices...
  Node                Connected Device                Device type
-----+-----+-----
  cdrom0              | TOSHIBA DVD-ROM SD-R6012 1033 | CD Reader/Writer
```

**Note:** *If the command responds with “No CD writers found or no media in the drive,” and the CS 2000 Management Tools server is a cluster then verify that the DVD-RW is placed in the active unit. The active unit is identified by a lit USER LED on the face of the unit.*

- 19 Optionally simulate (-S flag) recording the image to verify that the ISO 9660 image can be recorded on the DVD-RW. This step requires approximately 10 minutes:

```
# cdrw -d <dvd_dev> -S -i /data/dvdimage.iso
```

### Example

```
# cdrw -d cdrom0 -S -i /data/dvdimage.iso
```

*The CDROM tray ejects after this simulation. **Close the CDROM tray and continue this procedure to write the DVD-RW.***

- 20 Record the image. This step requires approximately 10 minutes:

```
# cdrw -d <dvd_dev> -i /data/dvdimage.iso
```

### Example

```
# cdrw -d cdrom0 -i /data/dvdimage.iso
```



*If the error response "Media in the device is not writable" is returned, verify that the CDROM tray is closed.*

*Approximately two minutes pass before progress is printed to the screen. After the first 1% is written, each additional percent requires about two seconds.*

## CDRW command progress

```
# cdrw -d cdrom0 -i /data/dvdimage.iso
Initializing device...done.
Preparing to write DVD
Writing track 1 ... 99 %
```

*Approximately nine minutes pass before the command completes.*

```
done.
done.
Finalizing (Can take up to 4 minutes)...done.
$
```

*The CDROM tray on the CS 2000 Management Tools server ejects. **Close the CDROM tray and continue this procedure to verify the contents of the DVD-RW.***

- 21** Check that ISO9660 image recorded correctly:

```
# ls -asl /cdrom/cdrom
```

*The contents of the DVD-ROM are printed.*

- 22** Unmount the DVD-RW, eject it, and exit from root privilege:

```
# eject cdrom
```

If the ISO 9660 image was verified with the lofiadm command, remove the loopback file driver device:

```
# umount /mnt
```

```
# lofiadm -d /dev/lofi/1
```

**Note:** If /dev/lofi/2 was used above, substitute /dev/lofi/2 in this command.

Exit from root privilege:

```
# exit
```

```
$
```

*The dollar sign command prompt returns.*

- 23** Remove the local copies of the files:

```
$ rm /data/tmp/*  
$ rm /data/dvdimage.iso
```

***At the CS 2000 Management Tools server***

- 24** Remove the DVD-RW from the tray and close the tray. Label the DVD-RW.
- 25** Store the DVD-RW per office procedure.
- 26** This procedure is complete.

## Session Server - Trunks backup

By default, the unit performs a backup of the database and critical files every day at 1:00 AM. Refer to [Rescheduling backup time on page 126](#) to alter the schedule.

The contents of the backup are stored locally on each unit in the `/data/bkresmgr/backup` directory in tape archive (tar) format.

Security related files are not automatically backed up. Refer to [Manual backup of security related files on page 127](#).

### Purpose of this procedure

Use this procedure to make a manual backup or change the backup time.

### Limitations and Restrictions

#### ATTENTION

SIP Gateway application provisioning activities must be suspended during the time of the database backup in order to ensure that an accurate and complete copy of the active unit database is created. However, call processing is not affected and there is no enforcement in the database to prevent provisioning.

Security related files must be backed up manually.

### Prerequisites

#### ATTENTION

The SIP Gateway application database must be in sync with the CS 2000 to ensure an accurate copy of the active unit database is created. Verify this condition using procedure [Verify synchronization status on page 543](#).

### Making a backup

Follow this procedure to make an immediate backup.

#### *At the NCGL CLI or IEMS client*

- 1 Log on to the **ACTIVE** unit and change to the root user.

- 2 Execute the command to make the backup by typing `/opt/apps/db_install/sd/bkup_ngss.sh` and pressing the Enter key.

*The following output is printed to the screen and the backup is recorded to /data/bckresmgr/backup.*

**bkup\_ngss.sh response**

```
-----  
- Move files  
-----  
-----  
- Backup Solid database -  
-----  
-----  
- Copy certificate files to backup directory -  
-----  
-----  
- Copy commish files to backup directory -  
-----  
-----  
- Copy web files to backup directory -  
-----  
-----  
- Creating Meta-Data File Listing -  
-----  
-----  
- Waiting for Solid DB to complete backup -  
-----  
-----  
- Waiting for Solid DB to complete backup -  
-----  
-----
```

← The backup pauses at this point while the database is backed up.

**bkup\_ngss.sh response**

```
data/bkresmgr/temp/  
data/bkresmgr/temp/gen_cert.txt  
data/bkresmgr/temp/server.crt  
data/bkresmgr/temp/trusted.crt  
data/bkresmgr/temp/hosts  
data/bkresmgr/temp/ntp.conf  
data/bkresmgr/temp/ifcfg-eth0  
data/bkresmgr/temp/netnodes  
data/bkresmgr/temp/group  
data/bkresmgr/temp/passwd  
data/bkresmgr/temp/shadow  
data/bkresmgr/temp/ssh_host_dsa_key.pub  
data/bkresmgr/temp/ssh_host_key.pub  
data/bkresmgr/temp/ssh_host_rsa_key.pub  
data/bkresmgr/temp/server.xml  
data/bkresmgr/temp/redirect.jsp  
data/bkresmgr/temp/redirect_SSPFS.jsp  
data/bkresmgr/temp/redirect_no-SSPFS.jsp  
data/bkresmgr/temp/redirect_apps.php  
data/bkresmgr/temp/META-DATA.txt  
data/bkresmgr/temp/hostname.txt  
data/bkresmgr/temp/solid.db
```

*The backup filename is located in /data/bkresmgr/backup and is identified by hostname, date, and time as indicated in the following example:*

**Example**

*unit0.backupfile.2005-04-12\_17-10.tgz*

- 3** For security purposes, ensure that a copy of the backup file is transferred to a secure location.  
  
Use the **scp** command to make a secure copy of the backup file to a secure, remote server on your network. This server should be continuously available for cases where a restoration of the unit become necessary, such as during an upgrade rollback.
- 4** If security related files should be backed up, refer to [Manual backup of security related files on page 127](#).
- 5** You have completed this procedure. Repeat this procedure on the second unit.

## Rescheduling backup time

Each unit performs an automatic backup at 1:00 AM daily. Use the following procedure to change the schedule.

### *At the NCGL CLI or IEMS client*

- 1 Log onto the unit and change to the root user.
- 2 Remove the existing backup schedule from the crontab by typing  
**/opt/apps/db\_install/sd/uninstallBkres.sh**
- 3 Edit the backup schedule file by typing  
**vi /opt/apps/db\_install/sd/backup.cron**  
*The file is opened for editing.*

```
# Cron data file for NGSS Backup timings  
0 1 * * * /opt/apps/db_install/sd/bkup_ngss.sh
```

- 4 Modify the first five fields (indicated by “0 1 \* \* \*” in the example). The fields are identified in order from left to right:
  - minute — the minute of the hour that the command will run, values are 0 to 59
  - hour — the hour of the day the command will run, values are 0 to 23 with 0 being midnight
  - day — the day of the month the command will run, values are 1 to 31, an asterisk indicates to run the command all days
  - month — the month of the year the command will run, values are 0 to 12, an asterisk indicates to run the command all months
  - weekday — the day of the week that the command will run, values are 0 to 6, with 0 being Sunday, an asterisk indicates to run the command all weekdaysDo not modify the sixth field (/opt/.../bkup\_ngss.sh).  
When done, write and quit the file.
- 5 Install the newly created schedule in the crontab by typing  
**/opt/apps/db\_install/sd/installBkres.sh**
- 6 After the scheduled time, verify that a backup file is created in the /data/bkresmgr/backup directory and that it is created at the new time, not the previously scheduled time.

- 7 This procedure is complete. Repeat this procedure on the second unit.

## Manual backup of security related files

The automatic backup does not backup the certificate.keystore or key files. This guards against loss or theft of the backup which would compromise the key without the operating company personnel knowing about the breach.

Copy the following files to a safe location:

- /opt/base/share/ssl/certificate.keystore
- /opt/base/share/ssl/gen\_cert.txt
- /opt/base/share/ssl/server.crt
- /opt/base/share/ssl/server.key
- /opt/base/share/ssl/trusted.crt
- /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\_host\_rsa\_key

The following procedure provides a suggestion of how to backup these security related files.

### ***At the NCGL CLI or IEMS client***

- 1 Log in to either unit (usually the unit where the latest version of security certificates are stored), and change to root user.
- 2 Change directories to the /opt/base/share/ssl directory:  
**cd /opt/base/share/ssl**
- 3 Create a new directory to store backup copies of the certificate files:

```
mkdir <SNxx_ddmmyyyy>
```

where

#### **SNxx\_ddmmyyyy**

is the name of the new directory based on the currently installed release of the system software (for example SN08) and the current date in the format ddmmyyyy

- 4 Copy the certificates to the newly created backup directory:

```
cp * <SNxx_ddmmyyyy>
```

#### ATTENTION

Completing this step ensures that you have valid backup copies of the security certificates for restoring in case of an upgrade abort or rollback or for disaster recovery purposes.

- 5 Use the following table to determine your next step:

If	Do
you want to make backup copies of the security certificates to a remote server	Ensure that the remote host that will store the security related files is secure, that the host is unavailable to general users, and offers restricted access to personnel with security related responsibilities. Proceed to <a href="#">step 6</a>
you do not want to make backup copies of the security certificates to a remote server	This procedure is complete.

- 6 Secure copy the files to the remote server:

```
cd <SNxx_ddmmyyyy>
scp * <user>@<remote_server>:</path>
```

where

**user**

is a valid user ID on the remote server

**remote\_server**

is the IP address of the remote server

**/path**

is where the file will be located on the remote server

*The files are copied to the remote server.*

- 7 You have completed this procedure.



---

## Saving the Ethernet Routing Switch 8600 boot configuration file

---

The Ethernet Routing Switch 8600 boot configuration can be saved to a file using the Boot Monitor Command Line Interface (CLI). You must have access to the Boot Monitor CLI through a direct connection to the switch or a Telnet connection. For more information on accessing the Boot Monitor CLI, refer to “Managing the Ethernet Routing Switch 8000 Series Switch Using the Command Line Interface Release 3.2,” 313194-A.

**Note:** You must be directly connected to the switch to initiate a Boot Monitor session. You can connect using a Telnet connection only if the Boot Monitor CLI is already active.

### Save the boot configuration

#### *At the Boot Monitor CLI*

- 1 Issue the save command by typing

```
monitor# save <save_type> [file <value>]
[verbose] [standby <value>] [backup <value>]
```

where

**save\_type**

specifies what to save. Possible values for this parameter are config, bootconfig, log, and trace.

**file <value>**

is a filename in one of the following formats:

- [a.b.c.d]: <file>
- /pcmcia/<file>
- /flash/<file>

**verbose**

saves default and current configuration. if you omit this parameter, only parameters you have changed are saved.

**standby <value>**

saves the specified file name to the standby CPU (currently not supported)

**backup <value>**

saves the specified file name and identifies the file as a backup file

**Example**

```
save config file ralph.cfg backup 2
```

**Note:** To save a file to the standby CPU, you must enable TFTP on the standby CPU. To enable TFTP, enter flags tftpd true in the Boot Monitor CLI or config bootconfig flags tftpd true in the Run-Time CLI.

- 2** You have completed this procedure.

---

## Backing up UAS configuration files

---

All configuration data supporting the operation of the UAS is stored in configuration files. The configuration files include:

- uas.conf - containing configuration parameters that support the function of the UAS, including CG6000C card settings, Call Agent definition, APS hostname definition, network element settings, and conferencing service state definition
- ugw.conf - containing trunk configuration information for PRI Solutions
- snmpd.cnf - containing parameters that support the SNMP function, including management station address, SNMP user names, community names, and trap version
- hosts - containing parameters that support the function of the APS, including APS hostname and IP address
- atmhard.con - containing ATM bearer interface settings that link a local port ATM address to a particular ATM interface port
- atmconn.con - containing ATM bearer connections settings that provide the UAS with a remote gateway's name and ATM address
- mainsa.conf - containing Main Subagent program settings specifying the kinds of error and log messages to be sent to the management station
- atmSvcProfile.con - containing data on Switched Virtual Channel (SVC) traffic parameters associated with AAL2 SVCs
- atmhardloop.con - containing information associated with the loopback of SVCs

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network, all UAS nodes in the network can be backed up to the APS node. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server. This procedure enables you to set up automatic backup to a remote server.

## Backing up UAS configuration files

### *At the Windows desktop interface*

- 1 This step, which applies specifically to a Sun Solaris system, enables you to set up automatic configuration file system backup to a remote server.

- a Open a command interface by performing the following steps:

- i select **Start -> Run**

- ii type cmd in the window that displays

- iii press Enter

- b Open a telnet session to the remote UNIX server and log in as the Root user. Then enter:

```
cd /;mkdir /opt;chmod 777 opt
```

```
cd /opt;
```

```
mkdir uas;chmod 777 uas
```

```
cd uas;
```

```
mkdir uas_conf_backup;chmod 777
```

```
uas_conf_backup
```

```
cd /
```

```
cd /opt/uas/uas_conf_backup
```

- c Configure NFS to share the "/opt/uas" filesystem and start the NFS server:

```
echo "share -F nfs /opt/uas" >>
```

```
/etc/dfs/dfstab
```

**Note:** The commands from this point forward are specific for a Sun Solaris system.

```
/etc/init.d/nfs.server start
```

- d Create a user login called "Administrator" that does not require a password:

```
/usr/sbin/useradd -d
```

```
/export/home/Administrator -g 1 -s /bin/ksh
```

```
-m -u 1002 Administrator 2> /dev/null
```

```
passwd -d Administrator 2> /dev/null
```

- 2 At the local system console, enter the IP address of the remote server in the "Backup Storage IP" field of the Local Configuration Interface GUI screen, using the procedure "Modifying

configuration parameters through the Local Configuration Interface GUI” in the document, NN10095-511, entitled “UAS Configuration Management.”

- 3** You have completed this procedure.



---

## Configuring automated INI file backups

---

This procedure enables you to configure automated INI file backups.

**Note:** This procedure pertains to both the Media Server 2010 and the Media Server 2020.

### ***At the Windows desktop interface***

**1** Open a telnet connection to the CS 2000 Management Tool.

**2** Log in with the appropriate user name.

**Note:** The user name must be a member of the “succssn” and “emsadm” groups.

**3** Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

**4** When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

```
1) Display list of MS 2000 series nodes
```

```
2) Node Maintenance and Configuration
```

```
3) Backup INI file for all nodes
```

```
4) Copy a file to the SDM/CBM
```

```
5) Configure Automated INI file backup
```

```
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

**5** Press 5 to configure automated INI file backups.

The current automated INI backup settings display:

```
Current Automated INI Backup Settings
=====
```

```
Automated INI Backup Time= 02:00
```

```
Automated INI Backup Enabled= true
```

```
Would you like to change the Automated INI
Backup Settings? (y/n)
```

- 6** Follow the prompts to change the automated INI backup settings or press Enter to return to the Media Server 2000 series CLUI main menu.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 7** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 8** Enter exit to close the telnet session.
- 9** You have completed this procedure.



## Changing the SNMP community string password for a Media Server 2010 node

This procedure enables you to change the SNMP community string password for a Media Server 2010 node.

**Note:** After making configuration changes, execute a soft reset of the Media Server to burn the new configuration to flash memory. Refer to the *Performing a soft reset on a Media Server 2000 series node* section of this document.



### CAUTION

For proper operation with the IEMS, the SNMP community string must match the community string used when adding the Media Server 2010 node to the IEMS topology.

### At the Windows desktop interface

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.  
**Note:** The user name must be a member of the “succssn” and “emsadm” groups.
- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5** Enter 2 to access Node Maintenance and Configuration menu.
- 6** When prompted, enter the IP address of the Media Server node.  
The *Main Menu* displays.
- ```
*** Main Menu for MS2010 at 172.17.40.230 ***
1) Maintenance Menu
2) Configuration Menu
x) EXIT
Enter selection (1 - 2, x)
```
- 7** Enter 2 to access the Configuration Menu.  
The *Main Configuration Menu* displays.
- ```
*Main Configuration Menu for MS2010 at
172.17.40.230*
1) Display this nodes current configuration
2) General node configuration
3) Configure Network Time settings
4) SNMP configuration and security
x) EXIT
Enter selection (1 - 4, x)
```
- 8** Press 4 to access the SNMP configuration and security menu.  
The *SNMP Configuration and Password Management Menu* displays.
- ```
*** SNMP Configuration and Password Menu for
MS2010 at 172.17.40.230 ***
1) Setup Trusted SNMP Managers
2) Configuring SNMP Trap Destinations
3) Change SNMP Community String password
4) Change File Upload and Download user and
password
?) Help
x) EXIT
Enter selection (1 - 4, ?, x)
```
- 9** Press 3 to change the SNMP community string password.

The following message displays:

```
** SNMP Community String Password Management **  
Would you like to change the SNMP Community  
password for this node? (y/n)  
>
```

- 10** Press y to change the SNMP community password, or enter 'n' to return to the SNMP Configuration and Password Management menu.

The following message displays.

```
*** WARNING ***  
This password will be written to the MS2010 and  
is the only password that can be used for either  
reading from or writing to the node via SNMP. If  
there are other managers that must communicate  
to this MS2010 node then you will need to go to  
that manager and reconfigure the community  
strings it uses to communicate with this MS2010  
node. The password you are entering here will be  
used for both the read and write SNMP community  
strings.
```

Press <enter> to continue

- 11** Press Enter. The following message displays.

```
Enter the SNMP password for the CLUI to use when  
communicating with the 172.17.40.230 MS2010  
node. The password must be alpha numeric and can  
be up to 255 characters long. Return to exit.  
>
```

- 12** Enter the new SNMP community password. The following message displays.

```
Re-enter the Password  
>
```

- 13** Enter the new SNMP community password again. The following message displays.

```
Save the SNMP password change? (y/n)  
>
```

- 14** Enter y to save the new community password. The *SNMP Configuration and Password Management Menu* displays.
- ```
*** SNMP Configuration and Password Menu for
MS2010 at 172.17.40.230 ***
```
- 1) Setup Trusted SNMP Managers
  - 2) Configuring SNMP Trap Destinations
  - 3) Change SNMP Community String password
  - 4) Change File Upload and Download user and password
  - ? ) Help
  - x) EXIT
- Enter selection (1 - 4, ?, x)
- 15** Follow the prompts to return to the *Media Server 2000 Series CLUI Main Menu*.
- 16** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 17** Enter exit to close the telnet session.
- Note:** After making configuration changes, execute a soft reset of the Media Server to burn the new configuration to flash memory. Refer to the *Performing a soft reset on a Media Server 2000 series node* section of this document.
- 18** You have completed this procedure.

## Changing the SNMP community string password for a Media Server 2020 node

This procedure enables you to change the SNMP community string password for a Media Server 2020 node.

**Note:** After making configuration changes, execute a soft reset of the Media Server to burn the new configuration to flash memory. Refer to the *Performing a soft reset on a Media Server 2000 series node* section of this document.



### CAUTION

For proper operation with the IEMS, the SNMP community string must match the community string used when adding the Media Server 2020 node to the IEMS topology.

### **At the Windows desktop interface**

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.

**Note:** The user name must be a member of the “succssn” and “emsadm” groups.

- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5** Enter 2 to access Node Maintenance and Configuration menu.
- 6** When prompted, enter the IP address of the Media Server node.

The *Main Menu* displays.

```
*** Main Menu for MS2020 at 172.17.40.221 ***
```

- 1) Maintenance Menu
- 2) Configuration Menu
- x) EXIT

Enter selection (1 - 2, x)

- 7** Enter 2 to access the Configuration Menu.

The *AAL2 Main Configuration Menu* displays.

```
*** AAL2 Main Configuration Menu for MS2020 at  
172.17.40.221 ***
```

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- 5) Configure ATM loopback table
- 6) Display SVC Connection table
- 7) Configure ATM port table
- 8) Configure Remote Gateway table
- 9) Configure AAL2 PVC table
- 10) Configure SVC Profile table
- x) EXIT

Enter selection (1 - 10, x)

- 8** Press 4 to access the SNMP configuration and security menu.

The *SNMP Configuration and Password Management Menu* displays.

```
*** SNMP Configuration and Password Menu for  
MS2020 at 172.17.40.221 ***
```

- 1) Setup Trusted SNMP Managers
- 2) Configuring SNMP Trap Destinations
- 3) Change SNMP Community String password

4) Change File Upload and Download user and password

? ) Help

x) EXIT

Enter selection (1 - 4, ?, x)

**9** Press 3 to change the SNMP community string password.

The following message displays:

```
** SNMP Community String Password Management **
```

```
Would you like to change the SNMP Community password for this node? (y/n)
```

```
>
```

**10** Press y to change the SNMP community password, or enter 'n' to return to the SNMP Configuration and Password Management menu.

The following message displays.

```
*** WARNING ***
```

```
This password will be written to the MS2020 and is the only password that can be used for either reading from or writing to the node via SNMP. If there are other managers that must communicate to this MS2020 node then you will need to go to that manager and reconfigure the community strings it uses to communicate with this MS2020 node. The password you are entering here will be used for both the read and write SNMP community strings.
```

```
Press <enter> to continue
```

**11** Press Enter. The following message displays.

```
Enter the SNMP password for the CLUI to use when communicating with the 172.17.40.221 MS2020 node. The password must be alpha numeric and can be up to 255 characters long. Return to exit.
```

```
>
```

**12** Enter the new SNMP community password. The following message displays.

```
Re-enter the Password
```

```
>
```

- 13** Enter the new SNMP community password again. The following message displays.
- ```
Save the SNMP password change? (y/n)
>
```
- 14** Enter y to save the new community password. The *SNMP Configuration and Password Management Menu* displays.
- ```
*** SNMP Configuration and Password Menu for
MS2020 at 172.17.40.221 ***
1) Setup Trusted SNMP Managers
2) Configuring SNMP Trap Destinations
3) Change SNMP Community String password
4) Change File Upload and Download user and
password
?) Help
x) EXIT
Enter selection (1 - 4, ?, x)
```
- 15** Follow the prompts to return to the *Media Server 2000 Series CLUI Main Menu*.
- 16** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 17** Enter exit to close the telnet session.
- Note:** After making configuration changes, execute a soft reset of the Media Server to burn the new configuration to flash memory. Refer to the *Performing a soft reset on a Media Server 2000 series node* section of this document.
- 18** You have completed this procedure.



---

## Backing up INI files for all nodes

---

This procedure enables you to back up the INI files for all nodes.

**Note:** This procedure pertains to both the Media Server 2010 and the Media Server 2020. The example screens in this procedure show a Media Server 2010.

### ***At the Windows desktop interface***

**1** Open a telnet connection to the CS 2000 Management Tool.

**2** Log in with the appropriate user name.

**Note:** The user name must be a member of the “succssn” and “emsadm” groups.

**3** Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

**4** When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

```
1) Display list of MS 2000 series nodes
```

```
2) Node Maintenance and Configuration
```

```
3) Backup INI file for all nodes
```

```
4) Copy a file to the SDM/CBM
```

```
5) Configure Automated INI file backup
```

```
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

**5** Press 3 to back up the INI files for all nodes.

The following is an example message display:

### **Example**

```
Backup of .ini for node 172.17.40.230 completed  
and copied to SDM
```

```
Press <enter> to continue
```

**6** Press Enter.

The *Media Server 2000 Series CLUI Main Menu* displays.

\*\*\* Media Server 2000 Series CLUI Main Menu \*\*\*

- 1) Display list of MS 2000 series nodes
- 2) Node Maintenance and Configuration
- 3) Backup INI file for all nodes
- 4) Copy a file to the SDM/CBM
- 5) Configure Automated INI file backup
- x) EXIT CLUI

Enter selection (1 - 5, x)

- 7** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 8** Enter exit to close the telnet session.
- 9** You have completed this procedure.

---

## Displaying Media Server 2010 node current configuration

---

This procedure enables you to display the current configuration of the Media Server 2010 node.

### ***At the Windows desktop interface***

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.  
**Note:** The user name must be a member of the “succssn” and “emsadm” groups.
- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5 Enter 2 to access Node Maintenance and Configuration menu.
- 6 When prompted, enter the IP address of the Media Server node.

The *Main Menu* displays.

```
*** Main Menu for MS2010 at 172.17.40.230 ***
```

- ```
1) Maintenance Menu
2) Configuration Menu
x) EXIT
```

```
Enter selection (1 - 2, x)
```

- 7 Enter 2 to access the Configuration Menu.

The *Main Configuration Menu* displays.

```
*Main Configuration Menu for MS2010 at
172.17.40.230*
```

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- x) EXIT

Enter selection (1 - 4, x)

- 8** Press 1 to display the current configuration for this node.

The current configuration datafill displays:

**Example**

```
*Current configuration for MS2010 at
172.17.40.230*
```

```
IP Address: 172.17.40.230
```

```
Subnet Address: 255.255.248.0
```

```
Default Gateway: 172.17.40.1
```

```
MG Control Protocol: controlPtotocol-MEGACO(2)
```

```
Software Version: 4.40.9.14
```

```
Lock State: unlocked(2)
```

```
Megaco Call Agent IP Address: 172.17.40.36
```

```
Is Megaco Call Agent Used: yes(1)
```

```
Number of Conference Ports: 60
```

```
Number of TestTrunk Ports: 2
```

```
Number of Lawful Intercept Ports: 8
```

```
Number of Announcement Ports: 50
```

```
APS IP Address: 47.142.89.70
```

```
Primary Language: isoLangEnglish(2)
```

```
Secondary Language: isoLangEnglish(2)
```

```
Syslog Server IP: 47.142.89.221
```

```
Press <enter> to continue
```

- 9** Press enter. The *Main Configuration Menu* displays.  
\*Main Configuration Menu for MS2010 at  
172.17.40.230\*  
1) Display this nodes current configuration  
2) General node configuration  
3) Configure Network Time settings  
4) SNMP configuration and security  
x) EXIT  
Enter selection (1 - 4, x)
- 10** Follow the prompts to return to the *Media Server 2000 Series CLUI Main Menu*.
- 11** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 12** Enter exit to close the telnet session.
- 13** You have completed this procedure.



---

## Displaying Media Server 2020 node current configuration

---

This procedure enables you to display the current configuration of the Media Server 2020 node.

### ***At the Windows desktop interface***

- 1 Open a telnet connection to the CS 2000 Management Tool.
- 2 Log in with the appropriate user name.  
**Note:** The user name must be a member of the “succssn” and “emsadm” groups.
- 3 Invoke the MS 2000 Series CLUI by entering the following on the command line:

```
/opt/nortel/NTsesm/bin/ms2000.sh
```

- 4 When prompted, enter the appropriate user name and password.

The *Media Server 2000 Series CLUI Main Menu* displays.

```
*** Media Server 2000 Series CLUI Main Menu ***
```

- ```
1) Display list of MS 2000 series nodes
2) Node Maintenance and Configuration
3) Backup INI file for all nodes
4) Copy a file to the SDM/CBM
5) Configure Automated INI file backup
x) EXIT CLUI
```

```
Enter selection (1 - 5, x)
```

- 5 Enter 2 to access Node Maintenance and Configuration menu.
- 6 When prompted, enter the IP address of the Media Server node.

The *Main Menu* displays.

```
*** Main Menu for MS2020 at 172.17.40.221 ***
```

- ```
1) Maintenance Menu
2) Configuration Menu
x) EXIT
```

```
Enter selection (1 - 2, x)
```

- 7 Enter 2 to access the Configuration Menu.

The *AAL2 Main Configuration Menu* displays.

```
*** AAL2 Main Configuration Menu for MS2020 at
172.17.40.221 ***
```

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- 5) Configure ATM loopback table
- 6) Display SVC Connection table
- 7) Configure ATM port table
- 8) Configure Remote Gateway table
- 9) Configure AAL2 PVC table
- 10) Configure SVC Profile table
- x) EXIT

Enter selection (1 - 10, x)

**8** Press 1 to display the current configuration for this node.

The current configuration datafill displays:

**Example**

```
*Current configuration for MS2020 at
172.17.40.221*
```

```
IP Address: 172.17.40.221
```

```
Subnet Address: 255.255.248.0
```

```
Default Gateway: 172.17.40.1
```

```
MG Control Protocol: controlPtotocol-MEGACO(2)
```

```
Software Version: 4.40.0.1
```

```
Lock State: unlocked(2)
```

```
Megaco Call Agent IP Address: 172.17.40.68
```

```
Is Megaco Call Agent Used: yes(1)
```

```
Number of Conference Ports: 30
```

```
Number of TestTrunk Ports: 30
```

```
Number of Lawful Intercept Ports: 30
```

```
Number of Announcement Ports: 30
```



```
APS IP Address: 47.142.89.70
Primary Language: isoLangEnglish(2)
Secondary Language: isoLangEnglish(2)
Syslog Server IP: 47.142.89.27
ATM Default Application Type: aal2-i-366-2(2)
Transmission mode : sonet(1)
Press <enter> to continue
```

**9** Press enter. The *AAL2 Main Configuration Menu* displays.

```
*** AAL2 Main Configuration Menu for MS2020 at
172.17.40.221 ***
```

- 1) Display this nodes current configuration
- 2) General node configuration
- 3) Configure Network Time settings
- 4) SNMP configuration and security
- 5) Configure ATM loopback table
- 6) Display SVC Connection table
- 7) Configure ATM port table
- 8) Configure Remote Gateway table
- 9) Configure AAL2 PVC table
- 10) Configure SVC Profile table
- x) EXIT

```
Enter selection (1 - 10, x)
```

- 10** Follow the prompts to return to the *Media Server 2000 Series CLUI Main Menu*.
- 11** Enter x to exit the *Media Server 2000 Series CLUI Main Menu*.
- 12** Enter exit to close the telnet session.
- 13** You have completed this procedure.



---

## Backing up the APS-specific Oracle database and application files

---

To ensure successful recovery from a system problem that causes database file corruption, it is recommended that you periodically back up the database files that support operation of the APS. These files include:

- Oracle database
- Root database files
- non-Root database files

The Succession Server Platform Foundation Software (SSPFS) base software provides two utilities that enable you to back up these files: “bkfullora” and “bkfullsys”.

The “bkfullora” utility backs up the Oracle database. This utility runs automatically each day at 1:00 am and backs up the database to a 4mm DAT tape. The utility can also be run manually to back up the database to a disk file.

The “bkfullsys” utility backs up the UNIX file system, including all of the “Root” and “non-Root” database files. This utility can only be run manually.

Instructions for performing the “bkfullora” and “bkfullsys” backup procedures are found in ATM/IP Configuration Management, NN10261-600.

In addition to these two utilities, two additional APS-specific utilities enable you to back up selected files, when only files required for APS operation must be restored. The “ips\_export\_db.sh” utility backs up the APS Oracle database. The “backup\_appl\_data.sh” utility backs up only the non-Root application files, “/audio\_files,” “PROV\_data,” “/user\_audio\_files,” and Root application file, “/etc/inet/hosts.” Both of these utilities can only be run manually.

This procedure enables you to perform a complete manual backup of the APS-specific Oracle database files and application files. It is recommended that this procedure be performed once per week.

### Backing up the APS-specific Oracle database and application files

#### *In a telnet connection to the APS server*

- 1 Open an xterm window, and log in using the “maint” login and password.

- 2 Become the “root” user by entering:  

```
su - root
```
- 3 Enter the following command to start the backup:  

```
ips_export_db.sh -diskonly
```

The system displays a log of the backup activity.
- 4 To ensure that the backup was successful, list the content of the tape on the terminal screen by entering the following commands:  

```
cd /audio_files/aps_db_backup  
ls -l
```

A listing of the backed-up files displays. Look in this list for “dmp” files.

```
more README
```

A timestamp displays, which should show the time and date of this backup.

**Note:** At this point, you have completed the disk-only portion of the backup. Continue with the next step to complete the backup of the application files. The application files are backed up on tape.
- 5 Insert a write-enabled (white or grey tab is moved to the right where it can be seen) DAT tape into the 4mm DAT drive on the APS server, and then rewind the tape by entering the following command:  

```
mt -f /dev/rmt/0c rewind
```
- 6 Enter the following command to start a backup of the application file systems on a single tape:  

```
/usr/ntdb/uas/scripts/backup_appl_data.sh
```

The system displays a log of the backup activity.
- 7 Rewind the backup tape by performing the following command:  

```
mt -f /dev/rmt/0c rewind
```
- 8 To ensure that the backup was successful, list the content of the tape on the terminal screen by entering the following command:  

```
tar tvf /dev/rmt/0c | more
```
- 9 Eject the backup tape, label it, and move the write-enable tab to the “read-only” position (white or grey tab is moved to the left where it cannot be seen), to prevent the data on the tape from being accidentally over-written. Store the tape for use later. Insert another write-enabled DAT tape into the drive to be used

for the automatic Oracle system back up that runs daily at 1:00 a.m.

- 10** You have completed this procedure.



---

## USP OAM&P Workstation Backup

---

You can perform two types of backup on your OAM&P workstation, manual and automatic. Manual backups are performed from the desktop by manually initializing the backup process. Automatic backups are performed according to the settings defined in the tape drive application.

**Note:** Nortel Networks recommends that you use the automatic backups to ensure that the data that is stored on the tapes is up-to-date.

The OAM&P workstation is equipped with a tape drive, software to support tape backup, and five blank data tapes. These tapes will allow approximately one month's worth of backups to be kept on-site.

**Note:** Nortel Networks recommends that you label the tapes to indicate the OAM&P workstation associated with the backups to ensure that any recovery operations are performed from the correct tape.

### Backup Schedule

You should create a schedule for your automatic backups to ensure up-to-date storage of the system configuration of your OAM&P workstation.

**Note:** Nortel Networks recommends that you perform a full system backup once a week and modified (differential) backups once a day.

### Performing a Manual Backup

Nortel Networks recommends that you perform a manual backup of your OAM&P workstation after initial installation.

To perform a manual backup of the system configuration for your OAM&P workstation, perform the following steps:

#### ***At the OAM&P workstation***

- 1 Reboot the workstation.
- 2 Insert a tape to which the workstation will save your data.
- 3 Double-click the Backup Exec icon on the desktop if you are running a Veritas program, or the Colorado Backup II icon if you are running a Colorado program.
- 4 Select Open an existing backup job.

- 5 Click OK.
- 6 Select Automatic Full Backup.
- 7 Click Open.
- 8 If you want to schedule a regular backup, click Schedule.
  - a If you clicked Schedule, a popup window appears. Select the time and frequency of the regular backup.
- 9 Click Start. The backup procedure begins.

**Note:**

This procedure takes approximately 10-15 minutes.

This procedure is complete.

## Configuring for Automatic Backup

There are two types of automatic backup, full system backup and modified (differential) system backup.

The full system backup saves all of the files contained in the hard disk on your OAM&P workstation.

The modified (differential) system backup saves only the files on the hard disk that have been modified since the last full system backup.

**Note:** When you are using automatic backup, you must leave your OAM&P workstation turned on with Windows running and ensure that there is a tape in the tape drive.

During the initial installation of your system, the tape drive application was configured to perform an automatic full system backup once a week, every Saturday at 1:00am. However, you can modify the settings in the tape drive application to suit your needs.

**Note 1:** If you do not change the default setting for automatic full system backup, you will need to swap out the tape every Friday.

**Note 2:** In order for automatic backups to work, the tape drive scheduler icon must be active in the notification box in the taskbar with the automated daily backups option enabled, your OAM&P workstation must remain on with Windows active, and a tape must be in the tape drive.

## Verifying the Current Modified System Backup Settings

There is a tape drive configuration file associated with the modified system backup. To verify that the current settings in the configuration file matches the system requirements, refer to the tape drive documentation provided with the OAM&P workstation.



### **Viewing the Current Automatic Backup Schedule**

To view the current settings for automatic backup in the tape drive application, refer to the tape drive documentation provided with the OAM&P workstation.



---

## Backing up a Multiservice Switch or Media Gateway device

---

This section describes using Service Data Backup and Restore to perform a basic back up of service data.

Backup copies only the configuration data of the Multiservice Switch 7400/15000 or Media Gateway 7400/15000. The service data views that make up the configuration data are found on the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk in a set of files in individual directories under the directory /provisioning. Backup also copies the special files that are found under the directory /provisioning/netsentry.

Service Data Backup and Restore provide three types of backup.

- A full backup copies all service data on the selected device or devices.
- An incremental backup copies only service data changed or created since the last backup. Like the full backup, you can perform an incremental backup on either one or multiple devices.
- A selective backup copies specific service data that you select. You can perform a selective backup on either one or multiple devices.

The following information applies to using the Service Data Backup and Restore tool to backup Multiservice Switch 7400/15000 or Media Gateway 7400/15000 nodes:

- [Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the backup list](#)
- [Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the backup list](#)
- [Viewing the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 backup repository](#)
- [Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 in the backup list](#)
- [Changing the Default User Authentication](#)
- [Performing a full backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Performing an incremental backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Performing a selective backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)

## Using the command line interface to perform backups

You can use the command line to perform full, incremental, or selective backups. You can perform multiple backups on multiple devices in a single command. You have the option of obtaining the backup information from a file.

Before you perform a backup, you need to start up the Backup Controller and Providers.

To display online help for this command, use the -h option on the command line.

### Procedure steps

Enter the following command as one continuous command:

```
/opt/MagellanNMS/bin/nsbck
[-full <devtype> <devname> <devaddr> <id> <pw>]
[-incr <devtype> <devname> <devaddr> <id> <pw>]
[-view <viewname> <devtype> <devname> <devaddr>
<id> <pw>] [-cdir <backup_dir_path> [-f
<backup_info_file>] [-chost <controller_address>]
[-nolog] | [-log [<logfile>]]
[-nc <#_concurrent_connections>]
```

where:

-full

indicates a full backup.

-incr

indicates an incremental backup.

-view

indicates a selective backup.

devtype

is the name of the device type, such as PASSPORT.

devname

is the name of the device.

devaddr

is the IP address of the device and has the format n.n.n.n.

id

is the userID for a Passport and the READ community string for a Passport 4400/4460.

pw

is the user password for a Passport and the WRITE community string for a Passport 4400/4460.

viewname

is the name of the view file for a selective backup.

-cdir

is the backup directory used for this backup operation.

-f

indicates that the backup information is obtained from a file.

backup\_info\_file

is the name of the file containing backup information. Each line in the file has the same format as the -full, incr, or -view options.

-chost

indicates the remote Controller to be used in place of the Controller running on the local host.

controller\_address

is the address of the Controller and has the format host[:port]

-nolog

indicates that output messages are to be discarded.

-log

indicates that output messages go to stdout/stderr or to a log file. The default is stdout/stderr.

logfile

is the name of the file to which output messages go. If not specified, the messages go to the file mbrbackup.log in the current directory (where the tool runs).

-nc

indicates the number of concurrent backups to be performed. By default, SNMP Devices Backup tries to back up 5 different devices concurrently. This parameter is useful when you are backing up a large number of devices.

#\_concurrent\_connections

is the number of concurrent backups.

## Backup file naming convention

The service data backup files have the following naming convention:

```
./<devtype>/<devname>/<timestamp>.<dataset>/ \
<datafiles...>
```

**Note:** The period (.) represents the SNMP Devices Backup and Restore root directory.

where:

devtype

is the device type (PP4400, or PP4460).

devname

is the device name.

timestamp

has the format `yyyymmddhhmmss`

dataset

is the dataset name.

<datafiles...>

are the names of one or more files that are backed up.

## **Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the backup list**

Use this procedure to add devices to the list of devices that you wish to backup.

### ***Procedure steps***

- 1** Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
  - 2** Select the Backup Configuration tab.
  - 3** Select Add to launch the Add Devices Dialog.
  - 4** From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.
  - 5** From the drop down list, in the right pane, select a backup mode (Incremental or Full).
  - 6** If a specific userid and password is required for the device, enter the values in the user ID and Password fields and uncheck the Use default checkbox.
  - 7** If you wish to use the default userid and password, click the Use default checkbox.
  - 8** Click OK.
- The devices display in the Device List.

## **Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the backup list**

Use this procedure to remove devices from the list of devices that you wish to backup.

### ***Procedure steps***

- 1** Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2** Select the Backup Configuration tab.
- 3** In the Device List, select the devices you wish to remove.
- 4** Click Remove.

- 5 In the confirmation dialog, select Yes to confirm or No to cancel the removal.

## Viewing the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 backup repository

If the backup server is running locally, use the following procedure to view all the backup files in the backup repository.

### *Procedure steps*

- 1 Telnet into the remote workstation with the appropriate userid and password.
- 2 Navigate to the repository directory.
- 3 Use Unix directory commands to view the contents of the backup repository.

## Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 in the backup list

A specific userid and password can be defined when you add the node to the node list or you can set it later using the following procedure.

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select a node in the Device List section.
- 4 In the Device Details section, in the Authentication tab, enter a userid and password.
- 5 Clear the Use default checkbox.

## Changing the Default User Authentication

Use the following procedure to define a default userid and password which is used for all node access unless overridden by a specific userid and password for the node.

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.



- 2 Select Options ->Set default authentication.
- 3 Enter the userid and password in the appropriate fields.
- 4 Click OK.  
The new userid and password are used on the next node access.

## Performing a full backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select Add to launch the Add Devices dialog.
- 4 From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.
- 5 Select a device in the Device list:
- 6 Click in the Mode title and select Full from the drop-down list.
- 7 Click Backup.

The progress of the backup is displayed in the Messages area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure.

**Note:** To cancel a backup in progress click Cancel.

## Performing an incremental backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to backup only backup files that are not already in the repository.

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select Add to launch the Add Devices dialog.

- 4 From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.
- 5 Select a node in the nodes list.
- 6 In the Mode title, select Incremental from the drop-down list.
- 7 If you wish to specify a backup of views later than a specific date, enter the date in the date field. (for example July 3, 2003)
- 8 Click Backup.

The progress of the backup is displayed in the Status area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure.

**Note:** To cancel a backup in progress click Cancel.

## Performing a selective backup for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to backup only a single specified file to the repository.

### **Procedure steps**

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Backup Configuration tab.
- 3 Select Add to launch the Add Devices dialog.
- 4 From the left pane, select a group of devices or expand the group and use the Ctrl key to select a number of devices within a group.
- 5 Select a device in the Devices list.
- 6 In the Mode title, select Selective from the drop-down list.  
The Configuration column in the table is enabled.
- 7 Click in the Configuration cell to display a pull-down list that displays all the available views on the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.  
**Note:** This step may take a few seconds to complete because the application must access the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 and list all the views names.
- 8 Click Backup.

The progress of the backup is displayed in the Status area. If the backup is unsuccessful, an error dialog is displayed that specifies the device and the reason for the failure.

**Note:** To cancel a backup in progress click Cancel.



---

## Performing a backup of oracle data on an SSPFS-based server

---

### Application

Use this procedure to perform a backup of oracle data on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240).

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager

**Note:** An oracle data backup is not required when the SSPFS-based server is hosting the MG 9000 Manager.

- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

**Note:** An oracle data backup is not required when the SSPFS-based server is hosting the CBM.

If the SSPFS-based server is hosting the IEMS, it is highly recommended to purge the IEMS event and performance data prior to executing the data backup. This reduces the size of the oracle space used by the IEMS, and therefore, reduces the backup time, and possibility of a backup failure. The purge capability is only available in (I)SN07 onward.

You can schedule a full system backup that overwrites a previous one on a backup media or copy the last successful Oracle backup to DVD or tape when performing an automated data backup on an SSPFS-based server. This functionality is designed for use under 'dark office' conditions when you need to copy backup data to a backup media more than once before the media is ejected from the server. Refer to the procedure "Configuring dark office backups on an SSPFS-based server" in *ATM/IP Solution-level Configuration Management*, NN10409-500.

#### **ATTENTION**

It is recommended that provisioning activities be put on hold during the time of the data backup.

## Prerequisites

This procedure has the following prerequisites:

- For a Sun Netra t1400, you need a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data.
- For a Sun Netra 240, you need one or more blank CD-R, DVD-R, CD-RW or DVD-RW to store the data

**Note:** The backup utility limits the storage to 4 GB on a DVD-R and DVD-RW.

If you are using a new CD-RW or DVD-RW, or want to reuse a CD-RW or DVD-RW by erasing the contents, perform procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

### ATTENTION

The database must be in sync with the Communication Server 2000 and the MG 9000 Manager (if present). Therefore, ensure you have the appropriate images before you proceed. Performing a restore from the Oracle database alone can cause data mismatches at the Communication Server 2000 and the MG 9000 Manager (if present).

## Action

### ATTENTION

In a two-server configuration, execute this procedure on the active server.

### *At the server*

- 1 Insert the blank tape, CD or DVD into the drive. In a two-server configuration, insert the blank CD or DVD into the drive of the active server.

### *At your workstation*

- 2 Log in to the server by typing  
> **telnet <server>**  
and pressing the Enter key.  
where

**server**

is the IP address or hostname of the SSPFS-based server on which you want to perform the backup

In a two-server configuration, enter the physical IP address of the active server.

- 3 When prompted, enter your user ID and password.
- 4 Change to the root user by typing  
**\$ su -**  
and pressing the Enter key.
- 5 When prompted, enter the root password.
- 6 If the server is hosting the IEMS, and you want to purge the event and performance data, do step [step 7](#), otherwise proceed to step [10](#).

7

**ATTENTION**

This step stops the IEMS server application. Ensure it is acceptable at this time to stop the IEMS server application.

Stop the IEMS server by typing

```
# servstop IEMS
```

and pressing the Enter key.

- 8 Run the script to purge the data by typing  
**#**  
**/opt/nortel/iems/current/bin/purgeTempData.sh**  
and pressing the Enter key.

- 9 Start the IEMS server by typing

```
# servstart IEMS
```

and pressing the Enter key.

- 10 Use the following table to determine your next step.

<b>If you are using</b>	<b>Do</b>
a tape for backup	step <a href="#">11</a>
a CD or DVD for backup	step <a href="#">12</a>

- 11 Rewind the tape by typing

```
# mt -f /dev/rmt/0 rewind
```

and pressing the Enter key.

- 12** Back up the data by typing  
**# /opt/nortel/sspfs/bks/bkdata**  
and pressing the Enter key.

Example response:

```
Backup Completes Successfully
```

- 13** Use the following table to determine your next step.

If you are using	Do
a tape for backup	step <a href="#">14</a>
a CD or DVD for backup	step <a href="#">16</a>

- 14** List the content of the tape by typing

```
# tar tvf /dev/rmt/0
```

and pressing the Enter key.

Example response:

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:16 2005  
backup/oracle.dmp.gz  
-rw-rw-rw- 0/1 1007616 Mar 2 10:16 2005  
opt/critdata.cpio
```

- 15** Remove the tape from the drive, label it, write-protect it, and store it in a safe place.

Proceed to step [21](#).

- 16** Reinsert the backup CD or DVD into the drive.

- 17** List the content of the CD or DVD by typing

```
# tar tvf /cdrom/*bkdata*/*.tar
```

and pressing the Enter key.

*Example response:*

```
-rw-rw-rw- 0/1 1874917 Mar 2 10:17 2005  
backup/oracle.dmp.gz  
-rw-rw-rw- 0/1 1007616 Mar 2 10:17 2005  
opt/critdata.cpio
```

*When a DVD backup spans more than one disk, all the DVDs with the exception of the last one produce a file error during the verification process. This error message does not interfere with the backup process but can reappear several times as the backup spans multiple disks.*



- 18 Ensure you are at the root directory level by typing  
**# cd /**  
and pressing the Enter key.
- 19 Eject the CD by typing  
**# eject cdrom**  
and pressing the Enter key.  
*If the DVD drive tray does not open after you have determined that the DVD drive is not busy and is not being read from or written to, enter the following commands in the order listed:*  
**# /etc/init.d/volmgt stop**  
**# /etc/init.d/volmgt start**  
*Then press the eject button located on the front of the DVD drive.*
- 20 Remove the CD or DVD from the drive, label it, and store it in a safe place.
- 21 You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.  
**Note:** To restore the data from this backup tape, CD or DVD, refer to procedure “Restoring the oracle data on an SSPFS-based server” in *ATM/IP Security and Administration*, NN10402-600.



---

## Performing a backup of file systems on an SSPFS-based server

---

### Application

Use this procedure to perform a backup of the file systems on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240).

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

### Prerequisites

This procedure has the following prerequisites:

- You must perform a data backup prior to performing this procedure. Refer to procedure [Performing a backup of oracle data on an SSPFS-based server on page 173](#) to complete this task.

**Note:** The data backup is not required prior to this procedure for the Core and Billing Manager (CBM) or the MG 9000 Manager.

- For a Sun Netra t1400, use a blank 4mm Digital Data Storage (DDS-3) tape of 125m and 12 GB to store the data.
- For a Sun Netra 240, use one or more blank DVD-R or DVD-RW disks to store the data.

**Note 1:** The backup utility limits the storage to 4 GB on a DVD-R and DVD-RW.

**Note 2:** If you are using a new DVD-RW, or want to reuse a used DVD-RW and need to erase the contents, complete procedure “Preparing a CD-RW or DVD-RW for use” in *ATM/IP Security and Administration*, NN10402-600.

## Action

### ATTENTION

In a two-server configuration, execute this procedure on the active server.

#### *At the server*

- 1 Insert the blank tape DVD into the drive. In a two-server configuration, insert the blank DVD into the active server.

#### *At your workstation*

- 2 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

#### **server**

is the IP address or host name of the SSPFS-based server on which you are performing the backup

In a two-server configuration, enter the physical IP address of the active server.

- 3 When prompted, enter your user ID and password.

- 4 Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- 5 When prompted, enter the root password.

In a two-server configuration, ensure you are on the active server by typing **ubmstat**. If ClusterIndicatorSTBY is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display ClusterIndicatorACT, which indicates you are on the active server.

- 6 Use the following table to determine your next step.

If you are using	Do
a tape for backup	step <a href="#">7</a>
a DVD for backup	step <a href="#">8</a>

- 7 Rewind the tape by typing  
**# mt -f /dev/rmt/0 rewind**  
 and pressing the Enter key.
- 8 Back up the file systems by typing  
**# /opt/nortel/sspfs/bks/bkfullsys**  
 and pressing the Enter key.  
 Example response:  
 Backup Completed Successfully
- Note:** If you are using DVD, the system will prompt you to insert another blank disk if more than one is needed.
- 9 Use the following table to determine your next step.
- | If you are using  | Do                      |
|-------------------|-------------------------|
| a tape for backup | step <a href="#">10</a> |
| a DVD for backup  | step <a href="#">12</a> |
- 10 List the contents of the tape by typing  
**# gtar -tvMf /dev/rmt/0**  
 and pressing the Enter key.
- 11 Eject and remove the tape from the drive, label it, write-protect it, and store it in a safe place.  
 Proceed to step [19](#).
- 12 Insert the backup DVD into the drive. If the backup resides on multiple DVDs, insert the first backup DVD.
- 13 List the contents of the DVD by typing  
**# gtar -tvMf /cdrom/\*bkfullsys\*/\*.tar**  
 and pressing the Enter key.
- | If you  | Do                      |
|---|-------------------------|
| receive a prompt to prepare another volume        | step <a href="#">14</a> |
| do not receive a prompt to prepare another volume | step <a href="#">16</a> |
- 14 Press the Return key.
- 15 Stop the gtar process by pressing the Ctrl and C keys.

- 16** Ensure you are at the root directory level by typing  
**# cd /**  
and pressing the Enter key.
- 17** Eject the DVD by typing  
**# eject cdrom**  
and pressing the Enter key.  
If the disk drive tray will not open after you have determined that the disk drive is not busy and is not being read from or written to, enter the following commands:  
**# /etc/init.d/volmgt stop**  
**# /etc/init.d/volmgt start**  
Then, press the eject button located on the front of the disk drive.
- 18** Remove the DVD from the drive, label it, and store it in a safe place.
- | <b>If the backup</b>    | <b>Do</b>  |
|-------------------------|--|
| resides multiple DVDs   | Insert the next backup DVD in the disk drive and go to step <a href="#">13</a> . |
| resides on a single DVD | step <a href="#">19</a>  |
- 19** You have completed this procedure. If applicable, return to the high-level task or procedure that directed you to this procedure.

---

## Backing up the central security server

---

### Application

Use this procedure to back up the central security server. When the Security Services component is installed, the generic backup and restore script (brr\_security.sh) are registered with servman (bkmgr).

The NDS database and all files under the following directories are backed up using this procedure:

- /opt/nortel/config/3rd\_party/netscape
- /opt/nortel/config/3rd\_party/security/s1is
- /opt/nortel/config/applications/security
- /opt/nortel/data/3rd\_party/netscape
- /opt/nortel/data/3rd\_party/security/s1is
- /opt/nortel/data/applications/security

**Note 1:** The backup of the security services is not required for an upgrade from (I)SN07.

**Note 2:** The restore of the security services is not required for an upgrade from (I)SN07.

**Note 3:** The backup of the security services, when performed in an upgrade from (I)SN08, must be performed on the active side of the cluster.

### Prerequisites

You must have root user privileges to perform this procedure.

### Action

#### *In a telnet connection to the security server*

- 1 Telnet to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the server where IEMS resides
- 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 Verify the status of the SESM server application by typing  
**servman query -status -group SESMService**  
and pressing the Enter key.
- 6 Use the following table to determine your next step.

---

<b>If the response indicates</b>	<b>Do</b>
not running	<a href="#">step 7</a>
running	<a href="#">step 8</a>

---

- 7 Start the SESM server application by typing  
**servstart SESMService**  
and pressing the Enter key.
- 8 Enter the following command:  
**/opt/bkresmgr/cbm/bkmgr**
- 9 Enter the following command to start the backup:  
**backup full**
- 10 Enter the following command to exit the security server:  
**quit**
- 11 The Security Services configuration settings and data are backed up to the following file:  
**/data/bkresmgr/<date><time>backupSS1.1<host\_name>.tar**
- 12 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



---

## Backing up an SSPFS-based security client

---

### Application

Use this procedure to obtain a list of the files that will be backed up from the client machine. To enable backup and restore of the security client, the files to be backed up are registered with servman during installation. The files backed up depend on the packages installed.

### Prerequisites

You must have root user privileges to perform this procedure.

### Action

#### *In a telnet connection to the security server*

- 1 Telnet to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the server where IEMS resides
- 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 Enter the following command:  

```
cat etc/critdata.conf
```

*The system returns a list of all non-oracle data files that will be backed up from the client machine.*
- 6 Use the Synchronous Backup Restore Manager (SBRM) to backup the central security client data. When SBRM is run, all of the SSPFS data, including the security client data and oracle data, is backed up. For details, see the procedure for “Starting or stopping the automated synchronous backup restore manager service” in ATM/IP Solution-level Security and Administration, NN10402-600.
- 7 You have completed this procedure.



## Create a backup of the GWC load file

### Purpose of this procedure

This procedure is used to log onto the CS 2000 Core Manager or Core and Billing Manager (CBM) and manually make a backup copy of one or more existing GWC load images stored on the CS 2000 Core Manager or CBM.

### When to use this procedure

Use this procedure prior to saving an image of a GWC load if you wish to save a backup of the original GWC load stored on the CS 2000 Core Manager or CBM.



#### CAUTION

If a backup is not created, the process of taking a GWC load image overwrites the existing image stored on the CS 2000 Core Manager or CBM, preventing a rollback.

### Prerequisites

There are no prerequisites to this procedure.

### Action

#### *At the CS 2000 Core Manager or CBM console*

- 1 Log in to the CS 2000 Core Manager or CBM as the root user.

```
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: root
root's Password: <password>
```

- 2 Change directory to the GWC software directory by typing  
**# cd /swd/gwc**  
and pressing the Enter key.
- 3 Type **ls** and press the Enter key to list the contents of the directory.

- 4 Locate the load file name that corresponds to the load you wish to back up.

There are likely to be multiple load file names. Ensure that you select the correct load filename. If you are saving the load file of a specific GWC card or node, refer to procedure “View the operational status of a GWC” in Gateway Controller Configuration Management, NN10205-511, to locate the load filename associated with a specific GWC card.

- 5

**CAUTION**

Be sure to use the command `cp` in this step. Failure to use the `cp` command can cause problems with the general upgrade process.

Make a copy of the existing GWC software load file by typing

```
# cp <load_filename>.imag <load_filename>.imag.bak
```

and pressing the Enter key.

where

**<load\_filename>**

is the GWC load filename that you want to copy.

You can use any name for the backup file name. You can also include the date in this filename, for example:

```
<load_filename>.imag.031201
```

- 6 Change the permissions for the image file by typing

```
# chmod 755 <load_filename>.imag.bak
```

and pressing the Enter key.

where

**<load\_filename>**

is the GWC load filename

- 7 You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

---

## USP Backup

---

If you change the external IP address of an RTC system node in your system, you should immediately perform a backup operation and delete any data snapshots that were made before you changed the IP address. This will ensure proper communication with your OAM&P workstations. Refer to the Modifying RTC System Node Provisioning Data section of this document for more information on changing the external IP addresses.

### Performing a Backup Operation

To do a backup operation, perform the following steps:

#### *At the OAM&P workstation*

- 1 Open the Backup Active RTC window by clicking Administration in the main menu and clicking Backup in the Administration window.
- 2 Enter a description of the data snapshot in the Description box. You can enter up to 32 characters.
- 3 Click Backup to create the data snapshot. An hourglass appears while the current system configuration is saved. This can take several minutes, depending on system activity.

The Backup Status box indicates when the data snapshot has been successfully saved on the active RTC system node. The data snapshot is named for the date and time of its creation.

- 4 Click Close to close the Backup Active RTC window and return to the Administration window.
- 5 At the Administration window, click File Manager. The File Manager window appears.
- 6 Select the disk drive in your alternate boot server to which you want to copy the data snapshot from the Source list.
- 7 Select the active RTC system node from the Destination list.
- 8 Select the new data snapshot from the Snapshot box in the Destination portion of the window. Make note of the timestamp of the data snapshot.
- 9 Copy the snapshot to your alternate boot server by clicking <--. An hourglass appears while the data snapshot is copied. The boxes in the Source portion of the window will be updated with

the information for the copied data snapshot when the copy operation is complete.

**Note:** These files are large and can take several minutes to copy from an RTC system node to your alternate boot server.

- 10 When the files transferred, click Close to return to the Administration window.
- 11 Open the Alternate Boot Server (ABS) Configuration Manager window by clicking ABS Config on the Administration window.
- 12 From the menu bar, select File --> Login.
- 13 Enter your password in the Password window and click OK.
- 14 From the menu bar, select File --> ABS Configuration.
- 15 Select the system name from the Site Name list.
- 16 Select the data snapshot from the Alternate Boot Data Snapshot list.
- 17 Click OK.
- 18 From the menu bar, select File --> Logout.

---

## Creating system image backup tapes (S-tapes) manually

---

### Purpose

Use this procedure to create a system backup image manually.

### Prerequisites

You must be a user authorized to perform config-manage actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, refer to the procedures in the following table.

#### Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	<a href="#">217</a>
Displaying actions a user is authorized to perform	<a href="#">205</a>

### Application

Create a system image backup tape (S-tape) manually.

**Note:** If you want to schedule automatic system image backups, refer to SDM Security and Administration document.

The system image includes the following:

- boot (startup) files
- AIX operating system
- system configuration data
- core manager software

## Prerequisites

**ATTENTION**

This procedure must be performed a trained AIX system administrator authorized to perform config-manage actions.

**ATTENTION**

All volume groups on the core manager must be fully mirrored (Mirrored) before performing this procedure. If not, an error message is displayed.

**ATTENTION**

If your system includes the SuperNode Billing Application (SBA), you must use tape drive DAT0 to perform this procedure.

**ATTENTION**

The files under the /data file system are temporary files only, and are excluded from system image backup.

Perform a system image backup after the following events:

- initial installation and commissioning of the core manager
- changes to the configuration of disks or logical volumes
- installation of a new version of core manager platform software
- installation of new hardware
- changes or upgrades to existing hardware

A system image backup takes a minimum of 10 minutes to complete, depending on the size of your file systems.

**Recommended tapes**

To complete this procedure, use one of the digital audio tape (DAT) drive tapes approved by Nortel.

The brands approved by Nortel are: Hewlett Packard (HP), Maxell, Verbatim, Imation.



The tape lengths approved by Nortel are:

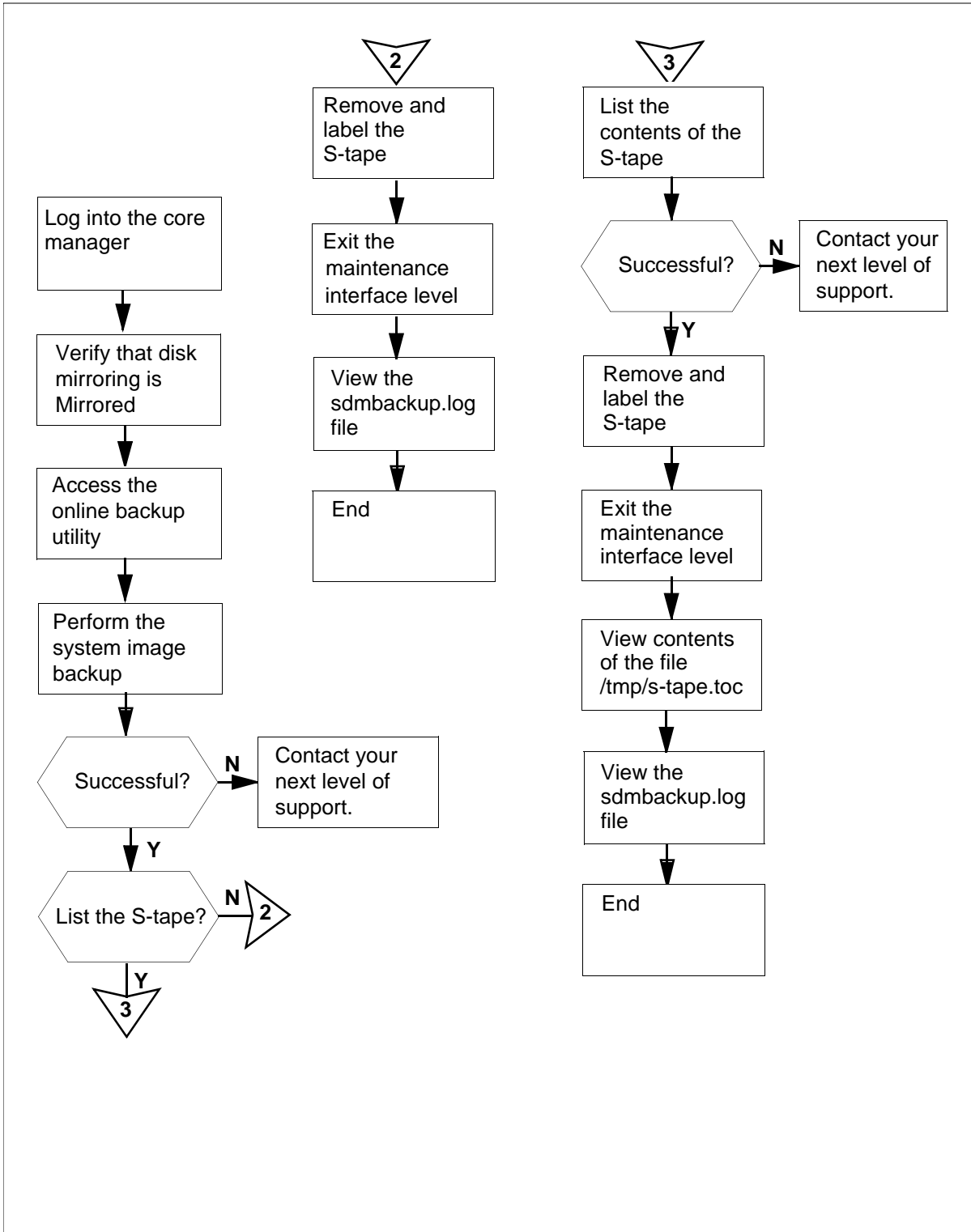
- 90-meter (90M)
- 125-meter (125M)
- 120-meter (120M)

The 125M tape is approved for UMFIOs only, assuming that your system is equipped with DDS3-capable devices to read the content of the tape.

## Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the procedure.

### Summary of creating system image backup tapes (S-tapes)



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Creating system image backup tapes (S-tapes)

### At the local VT100 console

1 Log into the core manager as a user authorized to perform config-manage actions.

2 Access the maintenance interface:

```
sdmmtc
```

3



### CAUTION

System mirroring must be **MIRRORED**

You cannot perform this procedure until disk mirroring of all volume groups is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

Access the storage menu level:

```
storage
```

*Example response:*

Volume Group	Status	
Free (MB)		
rootvg	Mirrored	608

Logical Volume	Location	Size (MB)	
%full/threshold	1 /	rootvg	20
25/ 80			
2 /usr	rootvg	192	85/ 90
3 /var	rootvg	64	11/ 80
4 /tmp	rootvg	24	6/ 90
5 /home	rootvg	300	4/ 70

```

6 /sdm          rootvg          300          44/ 90
Logical volumes showing: 1 to 6 of 6

```

If the disks	Do
are "Mirrored"	step <a href="#">4</a>
are not "Mirrored"	contact next level of support

- 4** Access the administration (Admin) menu level of the RMI:

**admin**

- 5** Access the System Image Backup and Restore Menu:

**backup**

*Example response:*

```

Currently there is a backup running on
bnode73.Please execute yours later.
Exiting . . .

```

**Note:** If another operator attempts to use the Backup and Restore utility when it is in use, an error message is displayed.

- 6** From the System Image Backup and Restore Menu, select Create a System Image on Tape (S-tape):

**2**

After you select option 2, you are prompted to select the tape drive.

*Example response:*

```

Select the tape drive you wish to use:

```

```

Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main Chassis-Slot
2
Enter 2 for tape drive DAT1 in Main Chassis-Slot
13
( 0, 1 or 2 ) ==>

```

**Note:** Use tape drive DAT0 (option 1) if your system also includes SBA.

- 7** Select the tape drive to use:

**<n>**

where

<n>

is the option (1 or 2) for the tape drive you wish to use

**Note:** If your system includes SBA, and you wish to use tape drive DAT1 (option 2), the following message is displayed:

*Example response:*

```
You have selected DAT 1. This is the default DAT
drive for the Billing application, and may
currently be in use for the emergency storage of
billing records.
```

```
If you continue to use DAT 1, make sure that the
correct tape is in the drive, and that billing
records will not be lost during the backup
restore operation.
```

```
Do you wish to continue with DAT 1? ( y | n )
```

If you	Do
wish to continue using DAT1	enter y press the Enter key
do not wish to use DAT1	enter n press the Enter key

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

After you select the tape drive, you are prompted to insert a tape in the drive you have selected.

*Example response:*

```
Please insert a 4mm DAT tape into the tape drive
DAT0.
```

Caution:

```
This action will overwrite the content on the
inserted tape.Do you want to proceed? ( y | n )
==>
```

**At the core manager****8****CAUTION****System image backup tape**

Creating a system image overwrites the contents of the inserted tape. Ensure that you are using the correct tape before starting the system image backup. If your system includes SBA and you are using DAT1, ensure that the tape drive does not contain an SBA tape.

Ensure that the appropriate core manager tape drive contains a 4-mm digital audio tape (DAT) either 90 m or 120 m long. This tape will be designated as the system image backup tape (S-tape).

**Note:** For the complete list of approved tapes, refer to the [Recommended tapes on page 192](#).

**At the local console**

**9** When you are certain you are using the correct tape, enter:

**y**

**10** Read the system message to determine if there is enough room on the temporary directory for the system image backup to proceed.

**Note:** If there is not enough room on the temporary directory, an error message appears.

*Example response:*

```
Rewinding the tape...
```

```
The /tmp directory is not big enough.  
Trying to expand /tmp by 6600KB...
```

```
Failed to expand the /tmp directory because  
there isn't enough free disk space left on the  
rootvg.
```

```
Please erase some files under /tmp directory to  
create at least 6600KB for the full system image  
backup.
```

Enter any key and return to exit ==>

If there is	Do
enough disk space	step <a href="#">14</a>
not enough disk space	step <a href="#">11</a>

- 11** Erase enough files from the temporary directory to create the required amount of disk space specified in the error message:

```
rm -rf /tmp/<filenames>
```

**Note:** If you have trouble erasing files from the temporary directory to free up disk space, contact the personnel responsible for your next level of support.

- 12** Execute the system image backup again.

The system image backup begins.

*Example response:*

```
Rewinding the tape...
```

```
Starting the system image backup on bnode73.
```

```
The backup takes a minimum of 10 minutes,
depending on the size of your file systems.
```

```
When the backup is complete, you will be asked
to remove the tape from the tape drive.
```

```
System image backup is in progress ...
```

**Note:** This backup process takes approximately 10 minutes to complete, depending on the amount of data stored on the disk.

- 13** Read the system message.

If the backup	Do
is successfully completed	step <a href="#">14</a>
fails	contact your next level of support

- 14** The system informs you if the backup is successful. When the backup is complete, the system prompts you to remove the tape and label it as an S-tape.

*Example response:*

```
The tape backup started on Wed Oct 16 08:21:15
EDT 1997
completed successfully on Wed Oct 16 08:37:37
EDT 1997.
```

```
The log for this session has been added to
"/var/adm/sdmbackup.log".
```

```
Please remove the backup tape from the tape
drive.
```

```
Label the tape as shown below and store it in a
safe place.
```

```
System Image Tape (S-tape)
The Machine Node Id: bnode73
Date: Wed Oct 16 08:37:37 EDT 1997
```

```
Eject the S-tape from the tape drive? ( y | n )
==>
```

- 15** Determine if you wish to eject the S-tape. Enter
- y to eject the tape, or
  - n if you do not wish to eject the tape, and wish to list its contents.

If you	Do
you wish to list the S-tape	step <a href="#">28</a>
protect and label the tape	step <a href="#">16</a>

If you eject the tape, the screen displays "Tape ejected." below the information displayed in step [14](#). You are then prompted to return to the System Image Backup and Restore Main Menu.

*Response:*

```
Tape ejected.
```

```
Would you like to return to the previous
menu? ( y | n)
```

- 16** Place the write-protected tab of the S-tape in the open position, to prevent accidental erasure.



- 17** When you are ready for the system to return to the System Image Backup and Restore Main Menu, enter
- y**
- 18** Determine if the backup is successful.
- The system informs you if the system image backup is successful, as shown in the response in step [14](#). You may also wish to view the `/var/adm/sdmbbackup.log` file or list the files on the S-tape.

If	Do
you wish to view the <code>/var/adm/sdmbbackup.log</code> file	step <a href="#">19</a>
you wish to list the S-tape	step <a href="#">28</a>
the backup is successful	step <a href="#">36</a>
the backup fails	contact your next level of support

- 19** Exit the System Image Backup and Restore Main Menu:

**0**

- 20** Exit the RMI:

**quit all**

- 21** Access the `sdmbbackup.log` file:

**cd /var/adm**

- 22** Scroll through the file:

**more sdmbbackup.log**

This screen informs you that the system image backup was completed successfully.

*Example response:*

```

bosboot:  Boot image is 5881 512 byte blocks.
0+1 records in.
1+0 records out.

```

```

Backing up the system...

```

```

.....
.....

```

```

0512 038 mksysb: Backup Completed Successfully.

```

The S-tape backup started on Wed Oct 16 09:24:07  
EDT 1997

completed successfully on Wed Oct 16 09:36:03  
EDT 1997

- 23** Determine if you wish to list the S-tape.

If you	Do
wish to list the S-tape	step <a href="#">24</a>
do not wish to list the S-tape	step <a href="#">40</a>

- 24** Return to the login directory:

**cd**

- 25** Access the RMI:

**sdmmtc**

- 26** Access the administration (Admin) menu level of the RMI:

**admin**

- 27** Access the System Image Backup and Restore Menu:

**backup**

- 28** From the System Image Backup and Restore Menu, select List Contents of the System Image Tape (S-tape):

**3**

- 29** After you select option 3, you are prompted to select the tape drive.

*Example response:*

Select a tape drive you wish to use:

```

Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
( 0, 1 or 2 ) ==>

```

**Note:** Use tape drive DAT0 (option 1) if your system also includes SBA.

**30** Select the tape drive:

<n>

where

<n>

is the number (1 or 2) for the tape drive you wish to use

*Example response:*

You have selected DAT 1. This is the default DAT drive for the Billing application, and may currently be in use for the emergency storage of billing records.

If you continue to use DAT 1, make sure that the correct tape is in the drive, and that billing records will not be lost during the backup restore operation.

Do you wish to continue with DAT 1? ( y | n )

If you do not wish to use DAT1, the system prompts you to return to the System Image Backup and Restore Menu.

If you wish to	Enter
continue using DAT1	y
not continue	n

**Note:** If your system includes SBA, and you still wish to use DAT1 (option 2), the following message is displayed:

**31** After you select the tape drive, you are prompted to insert the S-tape into the tape drive that you selected in step [30](#).

*Example response:*

Please insert your System Image Backup tape (S-tape) into the tape drive DAT0 and allow at least 5 minutes to complete the listing.

A log file will be saved in /tmp/s-tape.toc

Are you ready to proceed? ( y | n )

***At the core manager***

- 32** Insert the S-tape into the tape drive.

**Note:** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

***At the local VT100 terminal***

- 33** When you are ready to continue this procedure, enter:

**y**

- 34** The contents of the S-tape are displayed. When the listing is complete, the system prompts you to return to the System Image Backup and Restore Menu.

*Example response:*

```
Would you like to return to the previous menu?  
( y | n )
```

- 35** Return to the System Image Backup and Restore Menu:

**y**

***At the core manager***

- 36** If you have not already done so, remove the S-tape from the tape drive by pressing the eject button on the tape drive.
- 37** Label the tape according to your office practices, and store it in a safe location.
- 38** If you ejected an SBA tape, reinsert the tape.

***At the local VT100 terminal***

- 39** Exit the System Image Backup and Restore Menu,:

**0**

**Note:** If you wish to exit the RMI, enter QUIT ALL.

- 40** You have completed this procedure.

---

## Displaying actions a user is authorized to perform

---

### Purpose

Use this procedure in a standalone system to display the actions a user in a particular role group is authorized to perform.

### Prerequisites

You must be a user authorized to perform security-view actions.

For information on how to log in to the core manager or how to display other information about a user or role group, review the procedures in the following table.

#### Procedures related to this procedure

Procedure	Page
Logging in to the core manager	<a href="#">217</a>
Displaying information about a user or role group	<a href="#">211</a>

## Application

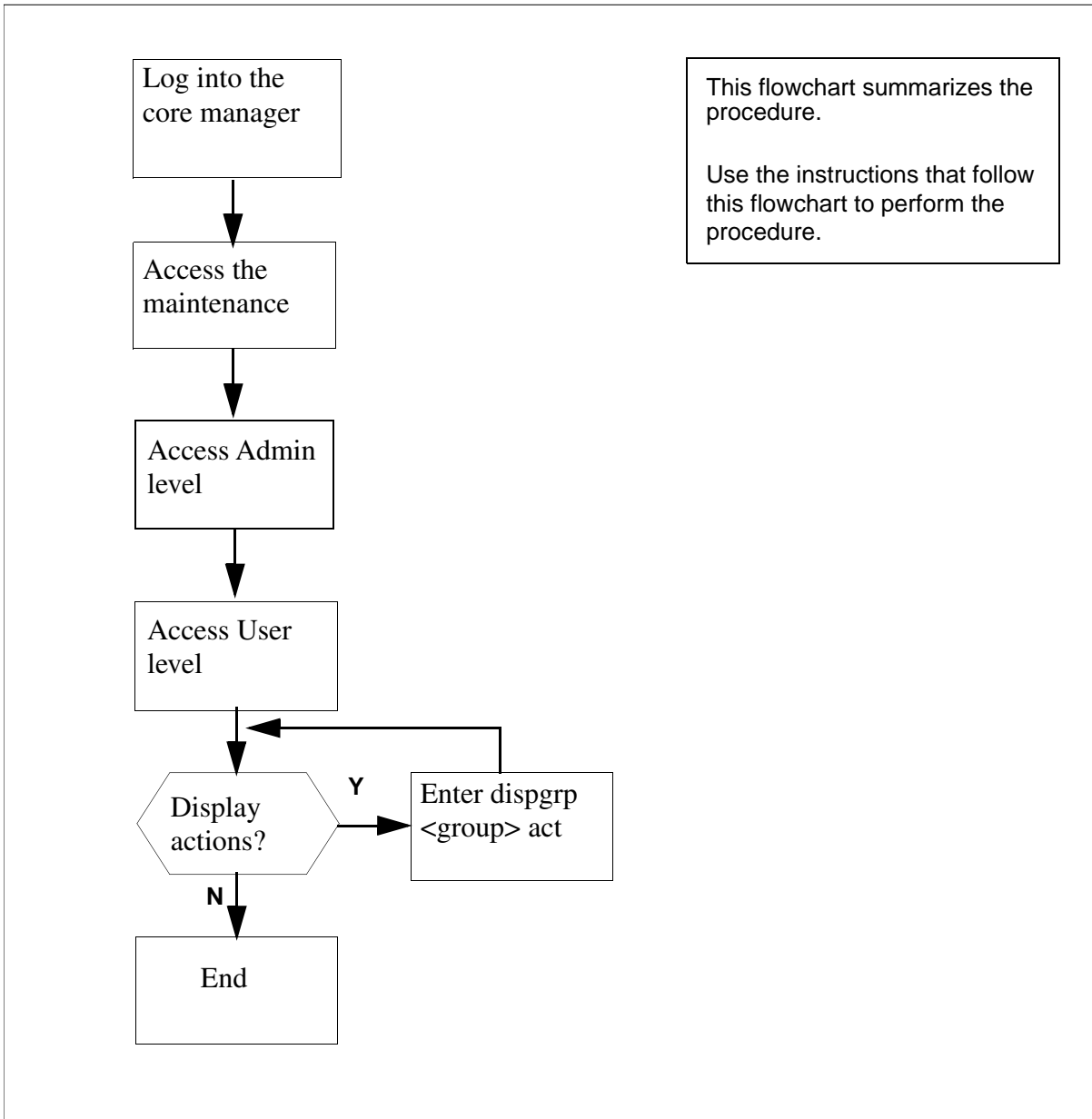
Role groups allow you to group individual users according to the task each user has to complete. The following table lists the standard actions for each role group in a standalone system.

Role Group	Standard Action
root (user)	all actions
emsadm	fault-view, fault-manage, fault-admin, accounting-admin, config-view, config-manage, config-admin, accounting-view, accounting-manage, accounting-admin, performance-view, performance-manage, performance-admin
secadm	security-view, security-manage, security-admin
maint	fault-view, fault-manage, config-view, config-manage, accounting-view, accounting-manage, performance-view, performance-manage
passthru	
Gr740Oss	performance-manage

## Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

### Summary of Displaying actions a user is authorized to perform



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Displaying actions a user is authorized to perform

### *At the local or remote VT100 console*

- 1 Log into the core manager as a user authorized to perform security-view actions.
- 2 Access the maintenance interface:  
**sdmmtc**
- 3 Access the Admin level:  
**admin**
- 4 Access the User level:  
**user**

*Example response:*

```

SDM   CON   512   NET   APPL   SYS   HW CLLI: SNMO
ISTb  ISTb   .C    ISTb  ISTb   Host: wcar8e9
M                                           Fault Tolerant
User
0 Quit
2
3 PassThru      Role Group      Users
4               maint         maint, fred, ty
5               secadm        cal, peter
6               emsadm         task1, task2
7
8               Role Groups: 1 to 3 of 3
9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16
17 Help
18 Refresh
   cal
Time 12:54 >

```



- 5 Display actions a user in a particular role group is authorized to perform:

```
dispgrpr <group> act
```

*where*

```
<group>
```

is maint, secadm, or emsadm

*Example response:*

```
Authorized actions for secadm
```

```
security-admin
```

```
security-manage
```

```
security-view
```

- 6 Exit the maintenance interface:  

```
quit all
```
- 7 You have completed this procedure.



---

## Displaying information about a user or role group

---

### Purpose

Use this procedure in a standalone system to display information about a user or role group.

In this procedure you can display the following information about users and groups:

- a list of users in a role group
- a list of all role groups and users
- shell, location, and group associated with a user
- a list of all users and role groups

### Prerequisites

You must be a user authorized to perform security-view actions.

For information on how to log in to the CS 2000 Core Manager or how to add or remove a user, review the procedures in the following table.

#### Procedures related to this procedure

Procedure	Page
Logging in to the CS 2000 Core Manager	<a href="#">217</a>
Displaying actions a user is authorized to perform	<a href="#">211</a>

## Application

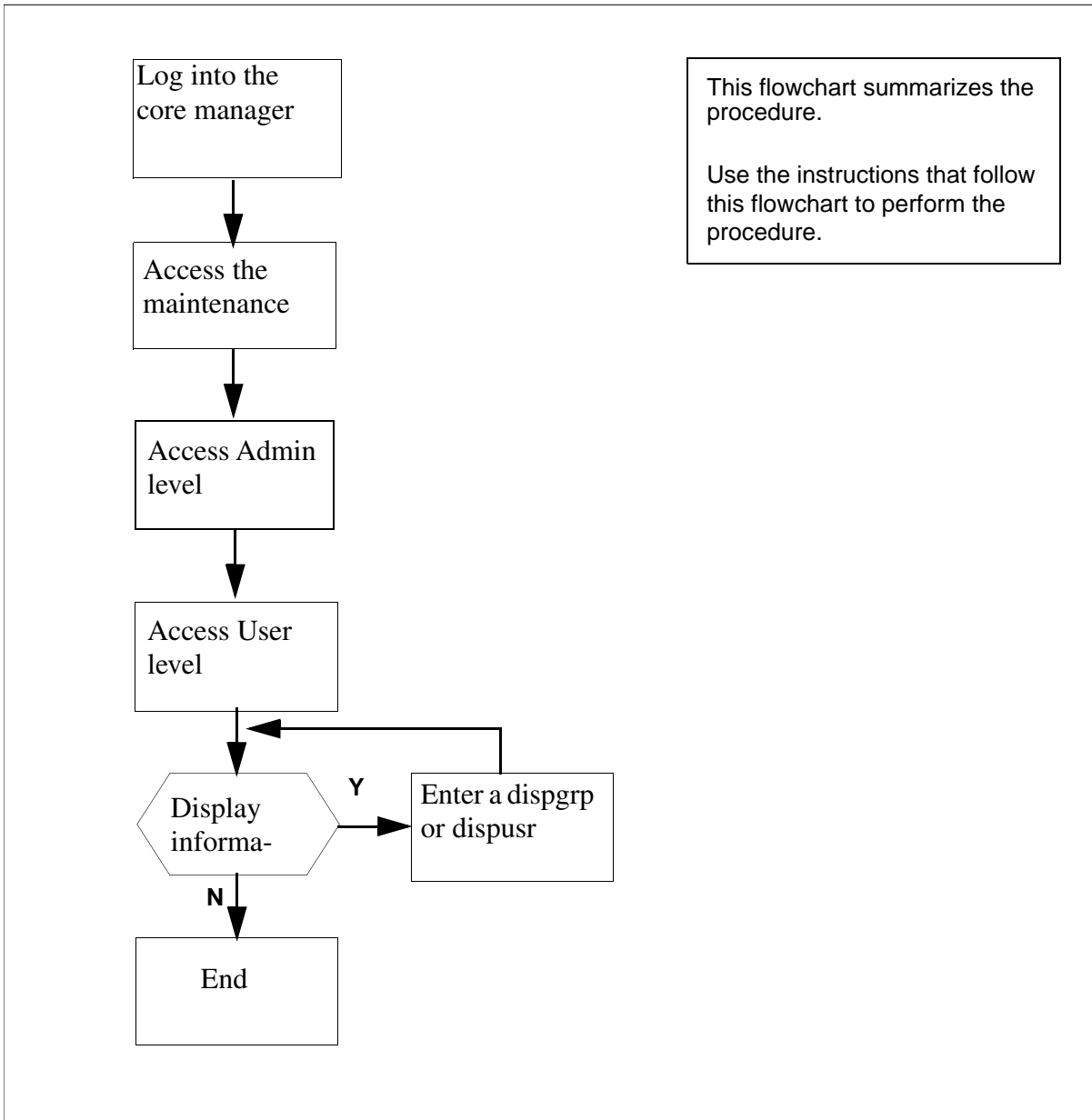
Role groups allow you to group individual users according to the task each user has to complete. The following table lists the standard actions for each role group in a standalone system.

Role Group	Standard Action
root (user)	all actions
emsadm	fault-view, fault-manage, fault-admin, accounting-admin, config-view, config-manage, config-admin, accounting-view, accounting-manage, accounting-admin, performance-view, performance-manage, performance-admin,
secadm	security-view, security-manage, security-admin
maint	fault-view, fault-manage, config-view, config-manage, accounting-view, accounting-manage, performance-view, performance-manage
passthru	
Gr740Oss	performance-manage

## Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

### Summary of Displaying information about a user or role group



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Displaying information about a user or role group

### *At the local or remote VT100 console*

- 1 Log into the core manager as a user authorized to perform security-view actions.
- 2 Access the maintenance interface:  
**sdmmtc**
- 3 Access the Admin level:  
**admin**
- 4 Access the User level:  
**> user**

*Example response:*

```
SDM   CON   512   NET   APPL   SYS   HW CLLI: SNMO
ISTb  ISTb   .C    ISTb  ISTb   Host: wcar8e9
M                                           Fault Tolerant

User
0 Quit
2
3 PassThru      Role Group      Users
4               maint         maint, fred, ty
4               secadm        cal, peter
5               emsadm         task1, task2
6
7
8               Role Groups: 1 to 3 of 3
9
10 Dispgrp
11 DispUsr
12 Up
13 Down
14
15
16
17 Help
18 Refresh
   cal
Time 12:54 >
```

If you want to	Do
display a list of users in a role group	step <a href="#">5</a>
display a list of all role groups and users	step <a href="#">7</a>
display information about a user	step <a href="#">9</a>
display a list of all users and role groups	step <a href="#">11</a>
exit	step <a href="#">12</a>

**5** Display a list of users in a particular role group:

**dispgrp <group>**

*where*

**<group> is maint, secadm, or emsadm**

*Example response:*

```
emsadm Users
1 task1
2 task2
```

**6** Go to step [12](#).

**7** Display a list of all role groups and users:

**dispgrp**

*Example response:*

```
Role Group      Users
1 maint          maint, fred, tyl
2 secadm         cal, peter
3 emsadm         task1, task2
```

Role Groups: 1 to 3 of 3

**8** Go to step [12](#).

**9** Display information about a particular user:

**dispusr <userID>**

*where*

**<userID>** is the userID of the new user

*Example response:*

```
pgrp      emsadm
groups    emsadm
home      /home/task1
shell     /bin/fash
```

- 10 Go to step [12](#).
- 11 Display a list of all users and groups:

***dispusr***

*Example response:*

User	Groups
maint	maint
bob	emsadmm
jo	secadm
fred	secadm, emsadm
sue	maint, secadm, emsadm

- 12 Exit the maintenance interface:  
**quit all**
- 13 You have completed this procedure.



---

## Logging in to the CS 2000 Core Manager

---

### Purpose

Use this procedure in a standalone system to log in to the CS 2000 Core Manager.

### Prerequisites

You must be a user authorized to perform actions associated with the procedure.

For information on how to display actions a user is authorized to perform or how to display information about a user or role group, refer to the procedures in the following table.

#### Procedures related to this procedure

Procedure	Page
Displaying actions a user is authorized to perform	<a href="#">205</a>
Displaying information about a user or role group	<a href="#">211</a>

### Application

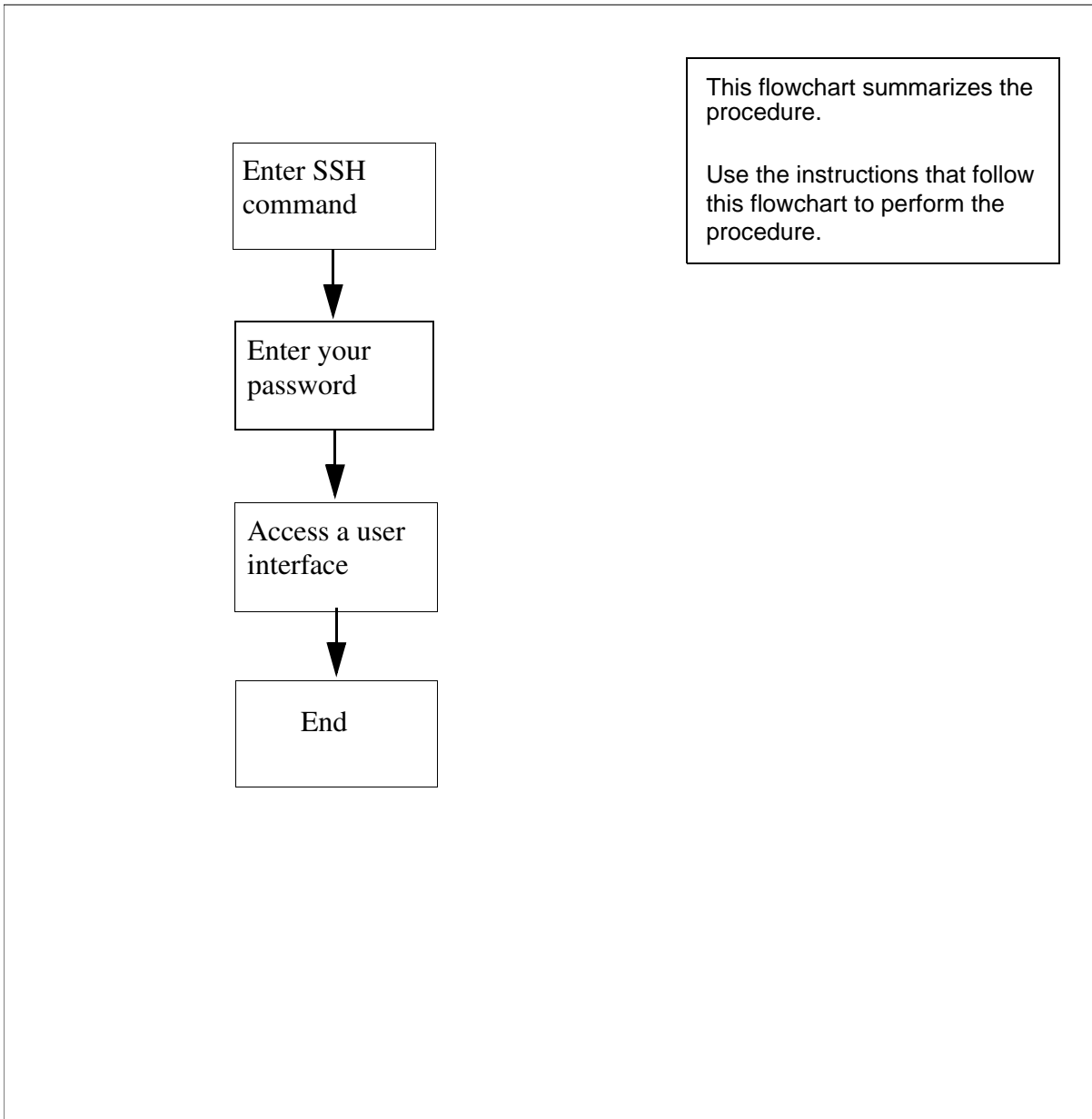
It is recommended that you log in to the CS 2000 Core Manager through SSH (secure shell) using a password.

For a complete description of login methods, refer to CS 2000 Core Manager Basics, NN10018-111.

## Procedure

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the task.

### Summary of Logging in to the CS 2000 Core Manager



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Logging in to the CS 2000 Core Manager

### *At the local or remote VT100 console*

- 1 Log in to the CS 2000 Core Manager using one of the following commands for SSH access:

```
ssh <userID>@<IPaddress | hostname>
```

or

```
ssh -l <userID> <IPaddress | hostname>
```

where

**<userID>**

is your userID

**<IPaddress>**

is the IP address of the CS 2000 Core Manager

**<hostname>**

is the host name for the CS 2000 Core Manager

*Example response:*

Don\_secu's Password:

- 2 Enter your password.

*Example response:*

(put example here)

- 3 Access a user interface, for example, access the maintenance interface:

```
sdmmtc
```

*Example response:*

(put example here)

- 4 Exit the maintenance interface:

```
quit all
```

- 5 You have completed this procedure.



## Configuring SBA backup volumes on the core

### Purpose

Use this procedure to configure backup volumes on IOP, 3PC, DDU, or SLM disks on the core for a billing stream. The maximum number of volumes that can be configured for a billing stream is either 69 or the maximum supported by the underlying hardware, whichever is less per stream.

The following table lists the disk drive backup volumes that you can configure for the BRISC and XA-core platforms.

Platform	Backup volume(s)
BRISC	DDU or SLM
XA-core (for releases prior to SDM16 or CS2E03)	DDU or IOP
XA-core (for SDM16 or CS2E0 and higher)	IOP

### Prerequisites

Prior to starting this procedure, you must be aware of the following:

- you must configure additional backup storage to prevent a temporary problem that forces the SBA into long-term backup mode
- the billing stream is aware that the replaced volumes exist, and recovers files from both the swapped-out and swapped-in sets of volumes as part of the recovery process
- the billing stream loses track of swapped-out volumes when a switch of activity (SwAct) or a restart is performed on the DMS or Communication Server 2000 prior to the completion of the recovery of the files
- there is a risk of losing some billing records when you reconfigure or swap-out backup volumes of a stream that is in backup mode during the transition process
- you must allow recovery to complete prior to a switch outage when you choose to swap out an active backup volume during an emergency situation. If not, the billing stream does not recognize the swapped-out volumes.

If you are using or migrating to a XAC16 system, your backup volumes must be on IOP volumes. If your current backup volumes

are on SLM or DDU volumes and you are running a previous release, you must migrate to IOP volumes before upgrading to this release.

**ATTENTION**

**Ensure the size for backup volumes is sufficient.**

Refer to [Disk space requirements](#) (Calculation of core disk space requirements) in procedure [Preparing for SBA installation and configuration](#). The absolute minimum size for backup volumes is 30MB.

**ATTENTION**

Backup volumes must be configured evenly across the available disks of the same disk type in your system.

## Procedures

Use the following procedures to configure SBA backup volumes on the core.

**Note:** Instructions for entering commands in the following procedures do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Calculate disk space to contain backup volumes

#### *At your system*

- 1 Write down the `dms_disk_space` value from the procedure [Preparing for SBA installation and configuration](#) (answer 28), which shows the amount of disk space required for the backup volumes.
- 2 Determine the amount of disk space of each disk type in your system to be used for storing the backup volumes. Divide the value you recorded in [step 1](#) by the maximum volume size

supported for the appropriate disk types for your system, obtained from the table below. Record these values.

Disk type	Maximum disks per core	Maximum volumes per device	Maximum volumes configurable for SBA	Maximum volume size
IOP	2	32	64	2GB
3PC	2	32	64	2GB
DDU	10	32	69	64MB
SLM	2	32	64	

- 3** Ensure that the backup volumes can fit on the disks in your system. Compare the values that you recorded in [step 2](#) with the maximum number of volumes supported for the disk types in your system, obtained from the table in [step 2](#). Determine the next step to perform:

If the number of volumes obtained in <a href="#">step 2</a>	Do
is less than or equal to the maximum number allowed	<a href="#">step 4</a>
is greater than the maximum number allowed	contact the next level of support

- 4** Determine the next steps to perform.

To configure disk type	Use this procedure
DDU	<a href="#">Configuring DDU disk drive backup volumes on page 224</a>
IOP	<a href="#">Configuring IOP disk drive backup volumes on page 228</a>
SLM	<a href="#">Configuring SLM disk drive backup volumes on page 231</a>
3PC	<a href="#">Configuring 3PC disk drive backup volumes on page 234</a>

## Configuring DDU disk drive backup volumes

### *At the MAP*

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream

- 2 Obtain information about the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream

**Note:** SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3 Quit out of the MAPCI level:

```
quit all
```

- 4 Display and record the size of a volume and its number of free blocks:

```
diskut;sv <volume name>
```

where

**<volume name>**

is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat step [step 5](#) for each volume name that you recorded in [step 2](#).

- 6 Create an eight-character, alphanumeric name for each of the new backup volumes that you determined in the procedure, [Calculate disk space to contain backup volumes on page 222](#) and record each of these names for future reference.

**Note 1:** DDU volume names can be up to eight alphanumeric characters in length, with the first four characters reserved for the disk prefix.



**Note 2:** Logical volumes must be configured evenly across the disks.

- 7 Access the IOD level:  
**mapci;mtc;iod**
  - 8 Locate the DDUs:  
**listdev ddu**
  - 9 Record the DDU numbers and their respective IOC, CARD, and PORT locations for future reference.
  - 10 Begin to busy a DDU:  
**ioc <ioc>**  
*where*  
**<ioc>**  
is the IOC controlling the respective DDU
  - 11 Display the DDU card:  
**card <ddu\_card>**  
*where*  
**<ddu\_card>**  
is the DDU card number
  - 12 Complete the busy process:  
**bsy**
  - 13 Confirm the DDU card number that you selected in [step 11](#) indicates a status of ManB.
  - 14 Display the free space for this DDU:  
**dskalloc <ddu #>**  
*where*  
**<ddu #>**  
is the DDU card number
- Note:** Record the free space amount from the dskalloc command that is displayed, for future reference.

- 15 Determine DDU disk space availability.

If you have	Do
located a DDU with sufficient disk space for the new backup volumes	<a href="#">step 19</a>
not located a DDU with sufficient disk space for the new backup volumes	<a href="#">step 16</a>

- 16 Return the DDU to service:

```
rts
```

- 17 Return to the IOC level:

```
quit
```

- 18 Repeat [step 10](#) through [17](#) until you locate a DDU with sufficient space for the new backup volumes.

- 19 Create a new logical volume:

```
add <volume> <blocksize>
```

where:

**<volume>**

is the backup volume name

**<blocksize>**

is the size of the volume. Calculate this by multiplying the maximum volume size allowed for the DDU disk, which is shown in the table in [step 2](#) of the procedure [Calculate disk space to contain backup volumes on page 222](#), by 1024.

#### Example

```
add AMA8 51200
```

This example prompts the system to create the logical volume D000AMA8, consisting of 51200 1024-byte blocks (50 Mbyte) of available disk space.

**Note:** If you receive an error message while updating the last DDU volume with 64 Mbyte, this volume must be configured with a size less than 32767 blocks.

- 20 Verify the names of the volume identifiers:

```
display
```

- 21 Add an allocation volume to the root directory:  
`diradd <backup_volume>`  
*where:*  
    **<backup\_volume>**  
        is the backup volume name
- 22 Update the volume identifiers:  
`update`
- 23 Repeat [step 19](#) through [22](#) until each new logical volume has been created.
- 24 Exit the disk administration level:  
`quit`
- 25 Return the DDU to service:  
`mapci;mtc;iod;ddu <#>;rts`  
*where:*  
    **<#>**  
        is the DDU disk drive number (0 or 1) that you busied in [step 12](#)
- 26 Return to the MAPCI level:  
`quit`
- 27 Configure the billing stream of the logical volumes you created in [step 19](#) through [23](#) once you receive confirmation that the files are successfully created. Performing the procedure, [Configuring SBA backup volumes on a billing stream on page 265](#).
- 28 Exit back to the command prompt:  
`quit all`  
**Note:** You must alert all operating company personnel who work on the core, and provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must understand that any restarts or activity switch (SwAct) that occurs before the billing stream returns to normal mode can cause a loss of billing records.  
  
It is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.
- 29 You have completed this procedure.

## Configuring IOP disk drive backup volumes

### *At the MAP*

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream

- 2 Obtain information about the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream

**Note:** SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3 Quit out of the MAPCI level:

```
quit all
```

- 4 Display and record the size of a volume and its number of free blocks:

```
diskut;lv <volume name>
```

where

**<volume name>**

is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).

- 6 Create an alphanumeric name, consisting of a maximum of twelve characters, for each of the new backup volumes that you determined in the procedure [Calculate disk space to contain backup volumes on page 222](#). Record each of these names for future reference.

**Note 1:** IOP volume names on the IOP disks can be up to twelve alphanumeric characters in length, with the first four characters reserved for the disk prefix.

**Note 2:** Logical volumes must be configured evenly across the disks.

- 7 Access the disk administration level:

**diskadm <disk prefix>**

where

**<disk prefix>**

is one of the prefixes assigned to the two disks; for example, F02L or F17D.

- 8 Determine the free disk space:

**dd**

- 9 Note the following example, which is a response to the command performed in [step 8](#), choosing the F02L disk name.

Disk drive information for F02L

```
Date last formatted      : 2000/01/01 01:00:50.145 THU.
Date last modified      : 2001/09/26 11:22:38.587 WED.
Total space for volumes : 4095 Mbytes
Total free space        : 1014 Mbytes
Size of largest free segment : 1014 Mbytes
Total number of volumes : 14
```

1 Block = 512 bytes

- 10 Determine the size of the largest free segment.

If the size of the largest free segment is	Do
greater than or equal to the maximum allowable volume size for the IOP disk type	<a href="#">step 11</a>
less than the maximum allowable volume size for the IOP disk type	contact your next level of support before proceeding with this procedure

- 11 Create a new logical volume:

**cv <volume> <size> ftfs**

where

**<volume>**

is the backup volume name

**<size>**

is the size of the volume. Compare the size recorded in [step 1](#) of the procedure [Calculate disk space to contain backup volumes on page 222](#), with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

**Example**

cv AMA8 50 ffs

This entry prompts the system to create the logical volume F17LAMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12 Exit the disk administration level at the prompt:

**quit**

- 13 Repeat [step 7](#) through [12](#) until all new logical volumes have been created.

- 14 Exit to the command prompt:

**quit all**

- 15 Configure the billing stream of the logical volumes you created in [step 11](#) through [14](#) once you receive confirmation that the files are successfully created. Perform the procedure [Configuring SBA backup volumes on a billing stream on page 265](#).

- 16 Exit back to the command prompt:

**quit all**

**Note:** You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

- 17 You have completed this procedure.

## Configuring SLM disk drive backup volumes

### At the MAP

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream

- 2 Obtain the names of the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream

**Note:** SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3 Quit out of the MAPCI level:

```
quit all
```

- 4 Display and record the size of a volume and its number of free blocks:

```
diskut;lv <volume name>
```

where

**<volume name>**

is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).

- 6 Create an eight-character, alphanumeric name for each of the new backup volumes that you determined in the procedure [Calculate disk space to contain backup volumes on page 222](#). Record each of these names for future reference.

**Note 1:** SLM volume names on the SLM disks can be up to eight alphanumeric characters in length for the core manager, with the first four characters reserved for the disk prefix.

**Note 2:** Logical volumes must be configured evenly across the disks.

- 7 Busy SLM 0:  
**mapci;mtc;iod;slm 0;bsy**
- 8 Access the disk administration level:  
**diskadm <disk prefix>**  
where  
**<disk prefix>**  
is one of the prefixes assigned to the two disks; for example, S00D or S01D
- 9 Determine the free disk space:  
**dd**
- 10 Note the following example, which is a response to the command you performed in [step 9](#), choosing the S00D disk name.

```
Disk drive information for S00D
Drive name: S00D
Vendor Information           : SEAGATE ST31051N 9470
Date last formatted         : 2000/01/01 05:38:44.718
THU.
Date last modified         : 1998/04/23 17:46:59.754
THU.
Total space for volumes     : 1000 Mbytes
Total Free space            : 174 Mbytes
Size of largest free segment : 174 Mbytes
```

1 Block = 512 bytes

If the size of the largest free segment is	Do
greater than or equal to the maximum allowable volume size for the SLM disk type	<a href="#">step 11</a>
less than the maximum allowable volume size for the SLM disk type	contact your next level of support

- 11 Create a new logical volume:  
**cv <volume> <volume\_size> std**  
*Where*



**<volume>**

is the backup volume name

**<volume\_size>**

is the size of the volume. Compare the size recorded in [step 1](#) of the procedure [Calculate disk space to contain backup volumes on page 222](#) with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

**Example**

```
cv AMA8 50 std
```

This entry prompts the system to create the logical volume S00DAMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12 Exit the disk administration level at the prompt:

```
quit
```

- 13 RTS the SLM 0 disk drives that you busied in [step 7](#) to an InSv state:

```
mapci;mtc;iod;slm 0;rts
```

- 14 Exit to the command prompt:

```
quit all
```

- 15 Repeat [step 7](#) to [14](#) until all volumes have been created.

- 16 Configure the billing stream of the logical volumes you created in [step 11](#) through [14](#) once you receive confirmation that the files are successfully created, by performing the procedure [Configuring SBA backup volumes on a billing stream on page 265](#)

- 17 Exit back to the command prompt:

```
quit all
```

**Note:** You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

- 18 You have completed this procedure.

## Configuring 3PC disk drive backup volumes

### *At the MAP*

- 1 Post the billing stream:

```
mapci;mtc;appl;sdbil;post <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream

- 2 Obtain information about the existing backup volumes for the billing stream:

```
conf view <stream_name>
```

where

**<stream\_name>**

is the name of the billing stream

**Note:** SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.

The system displays the name of each backup volume in the stream. Record each backup volume name for future reference.

- 3 Quit out of the MAPCI level:

```
quit all
```

- 4 Display and record the size of a volume and its number of free blocks:

```
diskut;lv <volume name>
```

where

**<volume name>**

is the name of one of the volumes that you obtained and recorded in [step 2](#)

- 5 Repeat [step 4](#) for each volume name that you recorded in [step 2](#).

- 6 Create a twelve-character, alphanumeric name for each of the new backup volumes that you determined in the procedure [Calculate disk space to contain backup volumes on page 222](#). Record each of these names for future reference.

**Note 1:** 3PC volume names on the 3PC disks can be up to twelve alphanumeric characters in length, with the first four characters reserved for the disk prefix.

**Note 2:** Logical volumes must be configured evenly across the disks.

- 7 Access the disk administration level:

**diskadm <disk prefix>**

where

**<disk prefix>**

is one of the prefixes assigned to the two disks; for example, FD00 or FD01

- 8 Determine the free disk space:

**dd**

- 9 Note the following example, which is a response to the command performed in [step 8](#), choosing the FD00 disk name.

Disk drive information for FD00

```
Date last formatted       : 2000/01/01 01:00:50.145 THU.
Date last modified       : 2001/09/26 11:22:38.587 WED.
Total space for volumes  : 4095 Mbytes
Total free space         : 1014 Mbytes
Size of largest free segment : 1014 Mbytes
Total number of volumes  : 14
```

1 Block = 512 bytes

- 10 Determine the size of the largest free segment.

If the size of the largest free segment is	Do
greater than or equal to the maximum allowable volume size for the IOP disk type	<a href="#">step 11</a>
less than the maximum allowable volume size for the IOP disk type	contact your next level of support before proceeding with this procedure

- 11 Create a new logical volume:

**cv <volume> <size> ftfs**

where

**<volume>**

is the backup volume name

**<size>**

is the size of the volume. Compare the size recorded in step [1](#) of the procedure [Calculate disk space to contain backup volumes on page 222](#) with the allowable size for the IOP disk type (obtained from the table under [step 2](#) of the same procedure. The lesser of the two values must be entered as this size.

**Example**

cv AMA8 50 ffs

This entry prompts the system to create the logical volume FD00AMA8, consisting of 50 Mbyte (102400 512-byte blocks) of available disk space.

- 12 Exit the disk administration level at the prompt:

**quit**

- 13 Repeat [step 7](#) through [12](#) until all new logical volumes have been created.

- 14 Exit to the command prompt:

**quit all**

- 15 Configure the billing stream of the logical volumes you created in [step 11](#) through [14](#) once you receive confirmation that the files are successfully created, by performing the procedure [Configuring SBA backup volumes on a billing stream on page 265](#)

- 16 Exit back to the command prompt:

**quit all**

**Note:** You must alert all operating company personnel who are associated with the DMS switch. Provide the names of the old and new backup volumes and the procedure you used to swap the volumes. They must be made aware of that any RESTARTs or SwActs that occur before the billing stream returns to normal mode can cause a loss of billing records.

Also, it is imperative that the mode of the billing stream must be closely monitored to ensure that it returns to normal mode without an intervening RESTART or SwAct.

- 17 You have completed this procedure.

---

## Preparing for SBA installation and configuration

---

The following procedure contains a series of questionnaires that you must complete before you install and configure the SuperNode Billing Application (SBA) on the core manager for the first time.

In some cases, you may have been directed to this procedure from another procedure to complete or verify the information in one or more of the questionnaires, which include

- [General stream information on page 238](#)
- [AMADNS filename and header values on page 243](#)
- [File closure limits on page 244](#)
- [Disk space requirements on page 248](#)
- [Outbound file transfer destinations on page 251](#)
- [Outbound file transfer protocol on page 260](#)
- [Outbound file transfer schedule on page 260](#)

## General stream information

The following table contains a list of questions concerning general stream information. Record your answers in the spaces provided.

### General stream information (Sheet 1 of 6)

#	Question	Explanation	Answer
1	What is the name of this stream?	<p>stream_name</p> <p>The stream name on the SBA must match the stream name on the DMS Switch.</p> <p><b>Note:</b> This name must match a stream name in the CM table CRSFMT.</p> <p>Type: string Range: 1 to 4 characters. Example: AMA (not case sensitive)</p>	
2	Is this a filter stream?	<p>filter_stream</p> <p>The filter stream parameter specifies whether the stream is a CM billing stream (Yes) or a filtered stream (No).</p> <p>Type: Boolean Range: Yes or No (not case sensitive)</p>	
3	What is the associated stream name?	<p>associated_stream</p> <p>This question applies only for filter streams.</p> <p>The associated stream name parameter specifies the name of the associated CM billing stream.</p> <p>Type: string Range: 1 to 4 characters Example: AMA, OCC (not case sensitive)</p>	

## General stream information (Sheet 2 of 6)

#	Question	Explanation	Answer
4	What is the name of the Filter Criteria file?	<p>filter_criteria_file This question is applicable only for filter streams.</p> <p>Enter the filter criteria file name that contains the expression to be applied for the filtered stream.</p> <p>Type: string Range: 1 to 255 characters (case sensitive)</p>	
5	What is the record format of this stream?	<p>record_format The stream record format on the SBA must match the record format of the DMS Switch stream. The only record formats supported by this product and release are</p> <ul style="list-style-type: none"> <li>• BC (Bellcore AMA format) and</li> <li>• SMDR (Station Message Detail Recording)</li> <li>• CDR300</li> <li>• CDR250</li> </ul> <p>Type: enumeration Range: BC, SMDR, CDR300, CDR250 (not case sensitive)</p>	
6	What is the file format of this stream?	<p>file_format This is the format of the billing files that SBA creates on the core manager.</p> <p>Type: enumeration Range: DNS, DIRP (not case sensitive)</p> <p><b>Note:</b> The core manager does not support an SMDR stream in DIRP format.</p>	

**General stream information (Sheet 3 of 6)**

#	Question	Explanation	Answer
7	What is the name of the logical volume on the core manager for storing the billing files for this stream?	<p>logical_volume_name</p> <p>The logical volume is the name of the directory where the billing files are stored for this stream.</p> <p>Type: string</p> <p>Range: 1 to 255 characters</p>	
8	<p>Will file transfers for this stream be initiated by</p> <ul style="list-style-type: none"> <li>• SBA (Outbound), or</li> <li>• the downstream destination (Inbound)</li> </ul>	<p>file_transfer_mode</p> <p>Billing files always move from SBA to the downstream destination, but the file transfers can be initiated by</p> <ul style="list-style-type: none"> <li>• SBA (this is called outbound) or</li> <li>• the downstream destination (this is called inbound)</li> </ul> <p>If Outbound is chosen, the SBA must be configured with additional file transfer information. The outbound file transfer questionnaires must be completed.</p> <p>If Inbound is chosen, the outbound file transfer questionnaires are not needed.</p> <p>Type: enumeration</p> <p>Range: Inbound, Outbound</p> <p>Default: Outbound</p> <p>(not case sensitive)</p>	



## General stream information (Sheet 4 of 6)

#	Question	Explanation	Answer
9	What is the desired state for the stream?	<p>sba_stream_state The stream state controls where the records are sent.</p> <ul style="list-style-type: none"> <li>• ON: records are sent only to the SBA</li> <li>• OFF: records are sent only to an existing DIRP system</li> <li>• BOTH: records are sent to both SBA and to an existing DIRP system</li> </ul> <p><b>Note 1:</b> The BOTH state is intended for startup verification of SBA processing against DIRP processing. Extended use of the BOTH state can result in SBA performance problems.</p> <p><b>Note 2:</b> An MTX XA-Core system generating more than 175000 CDRs per hour does not support BOTH or OFF mode.</p> <p>Type: enumeration Range: On, Off, Both (not case sensitive)</p>	
10	Do you want the files renamed with close date?	<p>files_renamed_with_close_date This question is applicable only if the file format is DIRP.</p> <p>Type: Boolean Range: Yes, No Default: No (not case sensitive)</p>	

**General stream information (Sheet 5 of 6)**

#	Question	Explanation	Answer
11	Do you want to reset DIRP sequence number at midnight?  <i>This question appears only when you answer No to the question, "Do you want the files renamed with close date?"</i>	Reset_DIRP_sequence_number_at_midnight This parameter enables resetting the DIRP sequence number to zero after midnight, before opening a new billing file.  Type: Boolean Range: Yes, No Default: No (not case sensitive)	
12	Do you want the files closed for file transfer and writetape?	files_closed_on_file_transfer This question is applicable only if the file format is DIRP  Type: Boolean Range: Yes, No Default: No (not case sensitive)	

## General stream information (Sheet 6 of 6)

#	Question	Explanation	Answer
13	<p>Do you want DIRP blocks closed based on time (applicable only for DIRP file format)</p> <p><i>This question appears only when file_type=DIRP and record_format=BAF or CDR250.</i></p>	<p>DIRP_blocks_closed_based_on_time</p> <p>This parameter specifies whether the DIRP blocks are to be closed after a defined elapsed time.</p> <p><b>Note 1:</b> SBA block flushing does not support customized DIRP file formats that do not allow hex AA padding at the end of a block. This type of DIRP file expects CDRs to be of equal size, and each block ends with a special event record. Therefore, GSP and MCI CDR DIRP files are not supported.</p> <p><b>Note 2:</b> It is recommended that block flushing be used with real-time transfer mechanisms such as Real-Time Billing (RTB)</p> <p>Type: Boolean Range: Yes, No Default: No (not case sensitive)</p>	
14	<p>File DIRP block closure time limit (in seconds)</p> <p><i>This question appears only when you answer Yes to DIRP_blocks_closed_based_on_time (question 13)</i></p>	<p>DIRP_block_closure_time_limit</p> <p>This parameter specifies the maximum amount of time in seconds that a DIRP block is kept open before it is closed.</p> <p>Type: Integer Range: 1 through 120 Default: 1</p>	

## AMADNS filename and header values

The following table contains a list of configuration questions concerning AMADNS filename and header values. The values selected are used in

the headers and names of the AMADNS files that SBA creates for this stream. Record your answers in the spaces provided.

**Note:** The source component id and type are not configured per stream and their values will be used by every enabled AMADNS stream on this SBA.

### AMADNS filename and header values

#	Question	Explanation	Answer
15	What is the destination component id for this stream?	destination_id Type: String Range: 0000 to 4095 Default: 0002	
16	What is the destination component type for this stream?	destination_type Type: String Range: 01 to 15 Default: 03	
17	What is the source component id for this SBA?	source_id Type: String Range: 0000 to 4095 Default: 0001	
18	What is the source component type for this SBA?	source_type Type: String Range: 01 to 15 Default: 02	
19	What is the standard file type for this stream?	standard_file_type Type: Number Range: 1, 6 to 31 Default: 1 (BC), 11 (SMDR)	
20	What is the error file type for this stream?	error_file_type Type: Number Range: 1, 6 to 31 Default: 2 (BC), 12 (SMDR)	

### File closure limits

The following table contains a list of configuration questions concerning limits that control automatic closing of billing files by SBA. Note that the

first of these settings that are reached, triggers the closing of the file.  
Record your answers in the spaces provided.

### File closure limits (Sheet 1 of 4)

#	Question	Explanation	Answer
21	Do you want the files for this stream to be closed after a defined elapsed time?	<p>close_on_timer This controls whether SBA closes billing files based on how long the files have been open.</p> <p>If the answer is Yes, SBA will leave a file open no longer than the value specified in question #22.</p> <p>If the answer is No, skip question #22 and go to question #23.</p> <p>Type: Boolean Range: Yes, No Default: No (not case sensitive)</p>	
22	What is the maximum time that a file can be open for this stream?	<p>file_open_time_limit This controls the maximum time SBA keeps a file open. It is enabled only if Yes is the answer to question #21.</p> <p>If the answer to question #21 is Yes, enter the maximum time that a file can be open for this stream, then go to question #25.</p> <p>If the answer to question #21 is No, skip this question and go to question #23.</p> <p>Type: number Units:minutes Range: 5 to 10080 Default: 10080</p>	

**File closure limits (Sheet 2 of 4)**

#	Question	Explanation	Answer
23	Do you want Files closed at scheduled intervals from midnight?	<p>file_closed_at_scheduled_intervals_from_midnight</p> <p>The response to this prompt determines whether SBA closes billing files at scheduled intervals calculated relative to midnight.</p> <p>If the answer to this question is Yes, you will be prompted the options as shown in question #24.</p> <p>If the answer is No, skip question #24 and go on to question #25.</p> <p>Type: Boolean Range: Yes, No Default: No (not case sensitive)</p>	
24	What is the scheduled file closure time option for this Stream?	<p>scheduled_file_closure_time_option</p> <p>The response to this prompt determines the closure of billing files at the scheduled interval. This will be prompted along with the following options, if the answer to question #23 is Yes. Skip this question if the answer to question #23 is No.</p> <p>Options:</p> <ol style="list-style-type: none"> <li>1) Close billing files every 24 hours</li> <li>2) Close billing files every 12 hours</li> <li>3) Close billing files every 6 hours</li> <li>4) Close billing files every 2 hours</li> <li>5) Close billing files every hour</li> <li>6) Close billing files every 30 minutes</li> <li>7) Close billing files every 15 minutes</li> <li>8) Close billing files every 10 minutes</li> <li>9) Close billing files every 5 minutes</li> </ol> <p>Type: number Range: 1 through 9 Default: 5</p>	

**File closure limits (Sheet 3 of 4)**

#	Question	Explanation	Answer
25	What is the maximum number of records generated each day for this stream?	<code>records_per_day</code> This is used to calculate the maximum number of <ul style="list-style-type: none"><li>• records per file, and</li><li>• bytes per file</li></ul> Type: number Units: Records per day Range: none	
26	What is the maximum size of a record?	<code>bytes_per_record</code> This is used to calculate a value for the maximum number of bytes per file. Type: number Units: Bytes per record Range: none	
27	What is the maximum number of records per billing file for this stream?	<code>records_per_file</code> This controls the maximum number of records a billing file can contain before SBA automatically closes the file.  The recommended value based on a target of 300 files a day will be calculated and provided as the default value, if the average number of records per day is one or more. Type: number Units: records per file Range: BC 10000 to 500000 SMDR 1000 to 500000	

**File closure limits (Sheet 4 of 4)**

#	Question	Explanation	Answer
28	What is the maximum number of bytes per billing file for this stream?	<p>bytes_per_file This controls the maximum size (in bytes) of a billing file before SBA automatically closes it.</p> <p>A recommended value may be calculated with the following formula:</p> $\text{Records per day} * \text{average record size} / 300 = \text{Bytes per file}$ <p>Type: number Units: bytes per file Range: BC:1000000 to 20000000 SMDR: 100000 to 20000000</p>	
29	What is the average record size? (not applicable if the number of records per day is 0)	<p>average_record_size This parameter specifies the maximum size of a record. The default value is 80, but depends on the record type and the record size as defined on the CM.</p> <p>This prompt appears when the Number of records per day parameter is set to a value other than zero (0).</p>	

**Disk space requirements**

The following table contains a list of configuration questions related to core manager and DMS-switch disk space required by the SBA. Record your answers in the spaces provided.

Disk space sizing requirements are calculated using the DMS switch value billable Busy Hour Call Attempts (BBHCA). This value is the total number of billing-record-generating calls that are processed within the busiest one hour window of a typical 24-hour day.

For information on the BBHCA estimation factor and its use in calculating required disk space, refer to [Calculation of core manager](#)



[Disk Space Requirements](#) and [Calculation of DMS Switch Disk Space Requirements](#).

### Disk space requirements

#	Question	Explanation	Answer
30	How much disk space on the core manager is needed for the billing files for this stream?	<p><code>logical_volume_size</code></p> <p>If the core manager is unable to send the billing files to the downstream processor, they accumulate on the core manager disk space. The allocated disk space must be capable of holding at least 5 days of SBA billing files.</p> <p>The formula for calculating SBA-required disk space on the core manager is described in <a href="#">Calculation of core manager Disk Space Requirements</a>.</p> <p>Type: number Units: Mbytes Range: NA Default: none Space is allocated in 16 Mb increments.</p>	
31	How much disk space is needed for backup of billing records on the DMS Switch for this stream?	<p><code>dms_disk_space</code></p> <p>If the DMS switch is unable to send the billing records to the core manager, they are backed up to the DMS disk space. The allocated DMS disk space must be capable of holding at least a one day accumulation of SBA billing records.</p> <p>The formula for calculating SBA-required disk space on the DMS switch is described in <a href="#">Calculation of core manager Disk Space Requirements</a>.</p> <p>Type: number Units: Mbytes Range: NA Default: none</p>	

### Calculation of core manager Disk Space Requirements

The formula for calculating megabytes of disk space needed for SBA billing streams is:

$$\frac{\text{BBHCA} * \text{ALCR} * 10 \text{ hours} * \text{CRRD}}{1048576} / \text{disk utilization}$$

- BBHCA (Billable busy hour call attempts), multiplied by the ALCR
- ALCR (average length of a call record in bytes), multiplied by
- 10 hours, multiplied by
- CRRD (Call-record retention days), divided by
- 1048576 (the number of bytes in a megabyte), divided by
- the desired disk utilization.

For this calculation, the desired disk utilization is a percentage that is expressed as a decimal from 0.1 and 0.9.

This formula must be applied to each billing stream with the total of all streams representing the total megabytes of disk space required.

**Note:** The maximum number of files to hold billing records for a billing stream is 15000.

The calculation of 10 hours multiplied by BBHCA is an experience-based factor that can be used to estimate 24 hours of call traffic. If you know that the stream has a high BBHCA for more or less than 10 hours per day, increase or decrease the hours value.

### Calculation Example

Assumptions:

- BBHCA = 150000
- Average length of call records = 85 bytes
- Call retention days = 10
- Desired disk utilization = 0.6 (60%)

Calculation:

$$150000 * 85 * 10 * 10 / 1048576 / .6 = 2026 \text{ Megabytes (2 Gbytes)}$$

### Calculation of DMS Switch Disk Space Requirements

Regardless of the volume size determined in this procedure, XA-CORE users cannot configure a backup volume size greater than 2GB. For non-XA-CORE users, the maximum volume size that can be configured is limited to the size of the physical disk.

The recommended formula for calculating the DMS disk space needed for an SBA billing stream is:

$BBHCA * ALCR * 10 \text{ hours} * CRRD$

- BBHCA (Billable busy hour call attempts) multiplied by
- ALCR (Average length of a call record in bytes), multiplied by
- 10 hours, multiplied by
- CRRD (Call-record retention days)

This formula must be applied to each billing stream with the total of all streams representing the total DMS Switch disk space required.

The calculation of 10 hours multiplied by BBHCA is an experience-based factor that can be used to estimate 24 hours of call traffic. If you know that the stream has a high BBHCA for more or less than 10 hours per day, increase or decrease the hours value.

### Calculation Example

Assumptions:

- BBHCA = 150000
- Average length of call records = 85 bytes
- Call retention days = 2

Calculation:

$$150000 * 85 * 10 * 2 / (1024 * 1024) = 243 \text{ Mbytes of disk space}$$

## Outbound file transfer destinations

The following table contains a list of stream configuration questions relating to transferring files from SBA to one or more destinations. This table requires specific configuration information for the destinations, IP addresses, user ids, passwords, and directories. The SBA uses this configuration information to log in, and to transfer the files to the downstream destination. Record your answers in the spaces provided.

**Note:** The downstream destination (billing server) must comply with the following FTP commands and successful return codes, in order for the destination to successfully receive billing files:

FTP states/commands	Return Codes
OPEN	220
USER	230

---

PASS	230
TYPE	200
STRU	200, 250
CWD	250
STOR	226, 200, 250, 150
CLOSE	221
RNTO	250

QUIT

221

**Outbound file transfers (Sheet 1 of 6)**

#	Question	Explanation	Answer
32	What is the destination to transfer the billing files?	<p>destination</p> <p>The combination of the values for stream name, file format type, and destination acts as the key to the schedule tuple.</p> <p>The destination cannot contain unprintable characters or blanks.</p> <p>Type: numeric String Range: 1 to 15 characters Default: none Example: Eventure</p>	

## Outbound file transfers (Sheet 2 of 6)

#	Question	Explanation	Answer
33	Which protocol is to be used to transfer billing files from the SBA?	<p>protocol</p> <p>FTPW uses the File Transfer Protocol</p> <p>RFTPW (real time file transfer protocol wrapper) is used for the Real-Time Billing (RTB) application. RFTPW is supported only if the RTB application is configured.</p> <p><b>Note:</b> If you configure RFTPW for a schedule tuple, then you must configure RTB for the corresponding stream. Use the procedure <a href="#">Configuring RTB for a billing stream on page 267</a>.</p> <p>SFTPW (secure file transfer protocol wrapper) provides secure outbound file transfer using the OpenSSH sftp client. SFTPW is supported only if OpenSSH is installed on the core manager.</p> <p><b>Note:</b> The initial host key acceptance of the downstream processor must be performed manually before the SFTP is used to transfer files. This must be performed for each downstream destination.</p> <p>Type: enumeration Range: FTPW, RFTPW, SFTPW, KSFTP Default: FTPW (not case sensitive)</p> <p>KSFTP (key-based secure file transfer protocol wrapper) provides secure outbound file transfer with public key authentication, using the OpenSSH sftp client. KSFTP is supported only if OpenSSH is installed on the core manager.</p>	

**Outbound file transfers (Sheet 3 of 6)**

#	Question	Explanation	Answer
34	What is the IP address of the primary destination for this stream?	<p>primary_destination</p> <p>The primary destination is the IP address that the SBA logs into, and transfers the billing files.</p> <p>Type: IP Address Range: 0.0.0.0 to 255.255.255.255 Example: 47.202.35.189</p>	
35	What is the Port for the primary destination?	<p>primary_port</p> <p>The primary port number is associated with the primary IP address.</p> <p>Type: numeric Range: SFTPW: 22, 1025 to 65535 FTPW or RFTPW: 21, 1025 to 65535 Default: 22, for SFTPW 21, for FTPW or RFTPW Example: 22</p>	
36	What is the IP address of the alternate destination for this stream?	<p>alternate_destination</p> <p>The alternate destination is the IP address that the SBA logs into and transfers the billing files if SBA encounters problems in connecting to the primary destination.</p> <p>If there is no alternate destination, make this entry identical to the primary IP address.</p> <p>Type: IP Address Range: 0.0.0.0 to 255.255.255.255 Example: 47.202.35.189</p>	



**Outbound file transfers (Sheet 4 of 6)**

#	Question	Explanation	Answer
37	What is the Port for the alternate destination?	<p>alternate_port The alternate port number is associated with the alternate IP address.</p> <p>Type: numeric Range: SFTPW: 22, 1025 to 65535 FTPW or RFTPW: 21, 1025 to 65535 Default: 22, for SFTPW 21, for FTPW or RFTPW Example: 22</p>	
38	What is the login for the downstream destination for this stream?	<p>remote_login This login is the SBA user id to login to the downstream destination, and to transfer the billing files.</p> <p>Type: string Range: 1 to 20 alphanumeric characters Default: none Example: amadns (case sensitive)</p>	
39	What is the password for the login ID in question 24 for this stream?	<p>remote_password This is the SBA password used to log into the downstream destination to transfer the billing files.</p> <p>Type: string Range: 1 to 20 alphanumeric characters Default: none Example: abracadabra (case sensitive)</p> <p>The prompt for this entry is not generated if the KSFTP (key-based file transfer authentication) protocol is selected)</p>	

**Outbound file transfers (Sheet 5 of 6)**

#	Question	Explanation	Answer
40	What is the directory path on the downstream destination where the transferred billing files are to be stored?	<p>remote_storage_directory</p> <p>This is the full path to the directory on the downstream destination where SBA transfers the billing files.</p> <p>If this value is a period (.), the SBA FTP client does not issue a change working directory (CWD) command when a file transfer occurs.</p> <p>Type: string Range: 1 to 255 characters. Example: /users/amadns/billing (case sensitive)</p>	

**Outbound file transfers (Sheet 6 of 6)**

#	Question	Explanation	Answer
41	What is the desired field separator character for this stream?	<p>field_separator</p> <p>This is a single character that the SBA uses to separate the components of billing file names when they are transferred to the downstream destination.</p> <p>If the downstream destination is a UNIX system, the recommended field separator is a period (.); this results in a file name such as 020001.030002.00001.01.2.</p> <p>If the downstream destination is a system that does not allow more than one period (.) in the filename, the recommended field separator is an underscore (_); this results in a file name such as 020001_030002_00001_01_2.</p> <p>Type: character Range: any printable character Default: . (period) (case sensitive)</p>	
42	What is the desired filename extension for this stream?	<p>file_extension</p> <p>This is the short character string that SBA uses as an extension for the billing file names when it transfers them to the downstream destination.</p> <p>If the downstream destination is a UNIX system, do not use a filename extension.</p> <p>If the downstream destination is a system that does not allow more than one period (.) in the filename, the filename extension cannot be used.</p> <p>Type: string Range: 0 to 3 characters Default: blank (0 chars) (case sensitive)</p>	

## Outbound file transfer protocol

The following table contains a list of configuration questions relating to transferring files from SBA to the downstream destination. This table requires specific configuration limits information to control how the SBA reacts when it encounters problems in connecting to the downstream destination. Record your answers in the spaces provided.

### Outbound file transfer protocol

#	Question	Explanation	Answer
43	What is the maximum number of times SBA attempts to complete a failed session with the downstream destination for this stream?	protocol_max_retries Type: number Range: 0 to 10 Default: 3	
44	After a session for this stream fails, what is the maximum time in seconds that SBA must wait before attempting re-connection to the downstream destination?	protocol_retry_wait_time Type: number Units: seconds Range: 1 to 60 Default: 1	

## Outbound file transfer schedule

The following table contains a list of stream configuration questions relating to transferring files from SBA to the downstream destination. This table specifically addresses configuration information concerning

when SBA initiates a connection to the downstream destination to transfer billing files. Record your answers in the spaces provided.

### Outbound file transfer schedule (Sheet 1 of 2)

#	Question	Explanation	Answer
45	Are scheduled file transfers to the downstream destination required for this stream?	<p>schedule_active This controls whether SBA automatically initiates file transfers to the downstream destination.</p> <p>If set to Yes, SBA automatically transfers files to the downstream destination at the times defined by the answers to questions 46, 47 and 48.</p> <p>If this value is set to No, manual file transfers can be made using the sendfile command.</p> <p>Type: Boolean Range: Yes, No Default: No</p> <p>If No, use 0:00 for Answers 46 and 47 and 120 for Answer 48.</p>	
46	When should SBA start initiating file transfers to the downstream destination each day?	<p>schedule_start_time This setting determines the time of day when SBA starts file transfers to the downstream destination. See the examples following this table for more information.</p> <p>Type: Time of Day Units: hh:mm Range: 00:00 to 23:59 Default: none</p>	

**Outbound file transfer schedule (Sheet 2 of 2)**

#	Question	Explanation	Answer
47	When should SBA stop initiating file transfers to the downstream destination each day?	<p>schedule_stop_time This setting determines the time of day when SBA ends file transfers to the downstream destination. See the examples following this table for more information.</p> <p>Type: Time of Day Units: hh:mm Range: 00:00 to 23:59 Default: none</p>	
48	Within the daily time window defined in questions 46 and 47, how often should the SBA transfer files to the downstream destination?	<p>schedule_interval This specifies the interval, in minutes, at which SBA is to initiate billing file transfers to the downstream destination. This interval is only active during the window of time specified by the start time (question 46) and stop time (question 47). See the examples following this table for more information.</p> <p>Type: Number Units: Minutes Range: 5 to 1440 Default: 120</p>	

The following are some examples that show different answers to questions for the start time (question 46), stop time (question 47), and the interval (question 48) and the resulting SBA file transfer times.

**Note:** If your start time and stop time are identical, then SBA is setup for continuous outbound file transfer.

Start Time	Stop Time	Interval	SBA Actions	Resulting Transfers
0:00	0:00	240	The SBA transfers files every four hours, at the beginning of the hour, starting at midnight.	The SBA initiates file transfers at 12:00 midnight, 4:00 am, 8:00 am, 12:00 noon, 4:00 pm and 8:00 pm
22:10	2:00	30	The SBA transfers files every thirty minutes at 10 minutes and 40 minutes after the hour, between 10:10 pm and 2 am.	The SBA initiates file transfers at 10:10 pm, 10:40 pm, 11:10 pm, 11:40 pm, 12:10 am, 12:40 am, 1:10 am and 1:40 am
3:15	3:15	300	The SBA transfers files every five hours at 15 minutes after the hour, starting at 3:15 am.	SBA initiates file transfers at 3:15 am, 8:15 am, 1:15 pm, 6:15 pm and 11:15 pm.





## Configuring SBA backup volumes on a billing stream

### Purpose

Use this procedure either to add new SBA backup volumes to a billing stream or to remove SBA backup volumes from a billing stream.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Procedure

#### Configuring SBA backup volumes on a billing stream

##### *At the MAP*

- 1 Access the billing level by typing  
`mapci;mtc;appl;sdmbil`  
and pressing the Enter key.
- 2 Determine the next step to perform.

To	Do
Add volumes to a billing stream	step <a href="#">3</a>
Remove volumes from a billing stream	step <a href="#">4</a>

- 3 Add volumes by typing  
`addvol <stream_name> <volume1> ... <volume5>`  
and pressing the Enter key.

*Where:*

**<stream\_name>**

is the name of the billing stream

**<volume1> ... <volume5>**

is the volume name. Up to five volumes (with each entry separated from the preceding entry or succeeding entry by spaces) can be added at one time.

#### **Example**

To add five volumes, the command would appear as:

```
addvol AMA S00DAMA1 S01DAMA2 S00DAMA3  
S01DAMA4 S00DAMA5
```

Repeat this step until all of the volumes have been added to the stream, and then proceed to step [5](#).

**4** Remove volumes by typing

```
remvol <stream_name> <volume1> ... <volume5>
```

and pressing the Enter key.

*Where:*

**<stream\_name>**

is the name of the billing stream

**<volume1> ... <volume5>**

is the volume name. Up to five volumes (with each entry separated from the preceding entry or succeeding entry by spaces) can be removed at one time.

**Example**

To remove five volumes, the command would appear as:

```
remvol AMA S00DAMA1 S01DAMA2 S00DAMA3  
S01DAMA4 S00DAMA5
```

Repeat this step until all of the volumes that you wish to remove have been removed from the stream, and then proceed to step [5](#).

**5** You have completed this procedure.

---

## Configuring RTB for a billing stream

---

### Real Time Billing Overview

Real Time Billing (RTB) allows billing records to be available for transfer from the core manager 30 seconds after the time the billing records are generated. RTB downloads a small group of records to the DIRP billing file at the downstream destination as they are added to the open billing file on the core manager. RTB uses file transfer protocol (FTP) through an Ethernet connection to deliver the records.

### Terminology

To understand how the SBA processes and routes the billing records it receives for RTB, the following terminology must be understood:

- **Stream** - A stream, or billing stream, can be conceptualized as a pipeline through which billing records received from the core pass. For each stream component that exists on the core, a corresponding stream component exists on the core manager. Billing records created by calls pass through the stream from their point of origination on the core to the core manager, where they are stored on disk.
- **Sub-stream** - A stream is further divided into Primary and Recovery sub-streams. The Primary sub-stream handles the current records being sent by the core. The Recovery sub-stream is only active after the SBA is unable to transfer records from the core to the core manager and temporarily stores the records on the core. When the core is once again able to re-establish the connection to the core manager, the stored records are sent to the core manager in a Recovery sub-stream while, concurrently, the current records are sent in the Primary sub-stream.
- **Active file state** - When records are written to a file that is open on the core manager, the file name on the core manager is prefixed with an "A", which means "active". When a billing file's content is being written to a file on a downstream processor, the name of the file on the downstream processor is also prefixed with an "A".
- **Unprocessed file state** - After the file on the core manager receives all of its billing records, the file is closed and the name of the file is prefixed with a "U", which means "unprocessed". In the same manner, after the file content has been transferred to a downstream processor, the file receiving this content on the downstream processor is also prefixed with a "U".
- **Processed file state** - When a billing file on the core manager is closed and its content has been received by all designated downstream destinations, the file is then eligible for removal in order

to free up disk space. The file name prefix then changes from "U" to "P", meaning "processed".

### **SBA file transfer subsystem**

The SBA file transfer system uses a schedule tuple for scheduled file transfers. This schedule tuple is specified by stream name, file format, and destination. For each tuple, different file transfer parameters can be specified, such as start time, stop time, and file transfer interval. There can be only one tuple for each combination of stream, file format, and destination.

The tuple contains a field indicating whether it is active. Scheduled file transfers occur only when the tuple is active. An interval setting in the schedule tuple determines how often SBA checks to see whether there are unprocessed files waiting to be sent downstream. When this interval is exceeded, the files are transferred downstream.

### **Real Time Billing file transfer**

The RTB rts (return to service) command, which is issued from the billing maintenance interface (billmtc), is used to initiate the transfer of open billing files to the downstream customer site. The command specifies the stream, file format, and destination. RTB uses the appropriate fields in the schedule tuple corresponding to this stream. RTB attempts to transfer records to the active billing file at the primary destination IP address of the downstream destination specified in the schedule tuple. For the procedure used to perform this command, see "Returning RTB stream instance to service" in the Accounting document for your core manager.

While RTB is transferring an open file, on the downstream processor the file name is prefixed with an "A" indicating an open, "active" file. When the file transfer is complete, the file prefix on the downstream processor is changed to a "U", the same file prefix used when scheduled file transfers succeed.

When RTB is in service (InSV), the RTB Bsy (busy) command stops the current open file transfer by first closing the current open file on the core manager, sending the remainder of the file downstream, and then closing the FTP connection with the downstream processor. The procedure used for querying the current operational state of RTB is "Querying the status of RTB for a billing stream", in the Accounting document for your core manager.

The schedule tuple must be active for a stream in order for the stream to be processed. When the two file transfer applications, scheduled transfer and Real Time Billing, are configured both must acknowledge

an unprocessed file (“U” file prefix) before the file can become processed (“P” file prefix). Thus, after RTB transfers a file, the file state will remain “unprocessed” until the next scheduled transfer event. When that transfer event occurs, the scheduler examines all unprocessed files and treats them according to whether they have already been transferred by RTB. The files that have not been transferred by RTB are transferred and moved to the “processed” file state after a successful transfer. The files that have been transferred by RTB are moved directly to the “processed” file state without retransmission.

### Connection management

In normal operation, open files transferred by Real Time Billing are sent only to the Primary IP destination specified in the schedule tuple for each destination. If a problem occurs with that destination and open file transfer fails, the current file is closed. RTB will be tried again on the next open files based on the RTB MIB value `RTBMaxConsecutiveFailures`. After all file transfers allowed by the `RTBMaxConsecutiveFailures` RTB MIB value have been attempted, a critical alarm is raised, a log is issued, and RTB is moved to the SYSB state. In this state, open file transfer is not active.

The retry behavior of RTB differs from that of a scheduled transfer. In the case of a scheduled transfer the primary address is tried first, and if it fails, attempts to re-transmit the file are repeated until the number of retries is exhausted. The retry attempts alternate between the primary and alternate destinations indicated in the schedule tuple. In the case of an RTB transfer, however, RTB will not attempt to re-transmit the file since that impacts the ability to send current records. Thus, RTB closes the file and retries transfer on the next file opened. In addition, unlike scheduled transfer, RTB only uses the primary destination.

**Note:** When RTB closes billing files, it cannot send the billing files downstream. The billing files are, however, automatically transferred from the core manager during the next scheduled transfer when the schedule tuple is active. The billing files can also be transferred manually. For the procedure used to transfer the billing files manually, see “Sending billing files from disk” in NN10363-811, in the Accounting document for your core manager.

Manual intervention is required to restore RTB when it is in the SYSB state. The problem can often be attributed to a network connection that is no longer functioning properly. The RTB `IPTest` command can be used to “ping” the primary downstream address indicated in the schedule tuple to determine this. A SYSB state may also occur if the protocol has been changed in the schedule tuple to something other than RFTPW, the required protocol for RTB. When the problem that

forced RTB into the SYSB state is resolved, the RTB Bsy and Rts commands can be used to bring RTB into service.

## Purpose

Use this procedure to perform the following real time billing (RTB) functions:

- add RTB to a billing stream
- change the RTB configuration for a billing stream
- delete RTB from a billing stream

## Prerequisites

This procedure has the following prerequisites:

- Configure the billing stream. Perform the procedure [Configuring a billing stream on the core manager on page 279](#). RTB requires outbound file transfer and DIRP file format.
- Configure outbound file transfer for the stream. Perform the procedure [Configuring the outbound file transfer schedule on page 289](#). RTB only supports Real-time File Transfer Protocol Wrapper (RFTPW)

This procedure requires the following information:

- maximum number of retry attempts after RTB fails to transfer a billing file before RTB raises a critical alarm
- directory location on the data processing and management system (DPMS) of the RTB test file and partial file

You must be a user in a role group authorized to perform accounting-manage actions.

For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	Core and Billing Manager 850 Security and Administration, NN10358-611
Displaying actions a role group is authorized to perform	Core and Billing Manager 850 Security and Administration, NN10358-611

## Logging on to the CS 2000 Core Manager

You must be a user authorized to perform security-admin actions in order to perform this procedure.

For information on how to log in to the CS 2000 Core Manager as an authorized user or how to display other information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CS 2000 Core Manager	CS 2000 Core Manager Security and Administration, NN10170-611
Displaying information about a user or role group	CS 2000 Core Manager Security and Administration, NN10170-611

## Logging on to the Core and Billing Manager 850

You must have the root user ID and password to log into the server.

### Procedure

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

### Configuring RTB for a billing stream

#### *At any workstation or console*

- 1 Log into the core manager. Refer to [Prerequisites on page 270](#) for details.
- 2 Log into the core manager as a user authorized to perform accounting-manage actions.
- 3 Access the BILLMTC interface:

```
billmtc
```

*Example response:*

*The BILLMTC interface opens at the main level.*

- 4 Access the schedule level:  
**schedule**  
*Example response:*  
*BILLMTC accesses the SCHEDULE level.*
- 5 Display and verify the schedule tuple:  
**display <stream\_name>**  
 where  
     **<stream\_name>**  
     is the name of the configured billing stream  
 Verify the following fields:
- File\_Format\_Type: DIRP
  - Protocol: RFTPW
  - Active: No
- Note:** Before configuring RTB ensure that the fields contain the values shown in this list.
- 6 Access the RTB level:  
**rtb**  
*Example response:*  
*BILLMTC accesses the RTB level.*
- 7 Access the CONFRTB level:  
**confrtb**  
*Example response:*  
*BILLMTC accesses the CONFRTB level.*

If you want to	Do
add RTB to a billing stream	step <a href="#">8</a>
change the RTB configuration for a billing stream	step <a href="#">16</a>
delete RTB from a billing stream	step <a href="#">24</a>



**8** Add RTB to a billing stream:

```
add <stream_name> <file_format> <destination>
```

where

**<stream\_name>**

is the name of the configured billing stream

**<file\_format>**

is the file format of the configured billing stream

**<destination>**

is the destination that SBA will transfer the billing files

**Note:** Scheduled outbound file transfer and real time billing (RTB) allow for multiple destinations for a single billing stream.

*Example response:*

```
Please enter the RTBMaxConsecutiveFailures  
(0...10 [3]):
```

**Note:** You are unable to abort from this command until a value is provided for the prompt above.

**9****ATTENTION**

If auto recovery is turned on, do not configure multiple RTB destinations with the same Test File Location or Partial File Location on the DPMS.

Enter the desired maximum retry attempts before RTB raises a critical alarm, and press the Enter key.

**Note:** The default value is 3.

*Example response:*

```
Please enter the RTBRemoteTestFileLocation:
```

**10** Enter the directory on the DPMS where the RTB test file will reside and press the Enter key.

**Note:** The default directory is the Remote\_Storage\_Directory as configured in the Schedule tuple for this stream.

*Example response:*

```
Please enter the RTBRemotePartialFileLocation
```

- 11** Enter the directory on the DPMS where the RTB remote partial file resides, and press the Enter key.

**Note:** The default directory is the Remote\_Storage\_Directory as configured in the Schedule tuple for this stream.

*Example response:*

You entered:

RTB Max Consecutive Failures: 5

RTB Remote Test File Location: /sba/autorec

RTB Partial File Location: /sba/autorec

Commit? [Save] {Save Edit Abort}:

If the displayed values are	Do
not correct	step <a href="#">12</a>
correct	step <a href="#">13</a>

- 12** Edit and correct the displayed values:  
**edit**
- 13** Save the information you entered:  
**save**
- 14** Activate the schedule tuple for the stream by performing [Configuring the outbound file transfer schedule on page 289](#)
- 15** Use the following table to determine your next action.

If you	Do
want to add RTB to another billing stream	step <a href="#">8</a>
do not want to add RTB to another billing stream	step <a href="#">27</a>

- 16 Change the RTB configuration for a billing stream:

```
change <stream_name> <file_format>
<destination>
```

where

**<stream\_name>**

is the name of the configured billing stream

**<file\_format>**

is the file format of the configured stream

**<destination>**

is the billing file transfer destination

*Example response:*

```
Please enter the RTBMaxConsecutiveFailures
(0...10 [3]):
```

**Note:** You are unable to abort from this command until a value is provided for the prompt above.

- 17

**ATTENTION**

If auto recovery is turned on, do not configure multiple RTB destinations with the same Test File Location or Partial File Location on the DPMS.

Enter the desired maximum retry attempts before RTB raises a critical alarm, and press the Enter key.

**Note:** The default value is 3.

*Example response:*

```
Please enter the RTBRemoteTestFileLocation:
```

- 18 Enter the directory on the DPMS where the RTB test file resides, and press the Enter key.

**Note:** The default directory is the Remote\_Storage\_Directory as configured in the Schedule tuple for this stream.

*Example response:*

```
Please enter the RTBRemotePartialFileLocation
```

- 19** Enter the directory on the DPMS where the RTB remote partial file resides, and press the Enter key.

**Note:** The default directory is the Remote\_Storage\_Directory as configured in the Schedule tuple for this stream.

*Example response:*

You entered:

RTB Max Consecutive Failures: 5

RTB Remote Test File Location: /sba/autorec

RTB Partial File Location: /sba/autorec

Commit? [Save] {Save Edit Abort}:

If the displayed values are	Do
not correct	step <a href="#">20</a>
correct	step <a href="#">21</a>

- 20** Edit and correct the displayed values:  
**edit**
- 21** Save the information you entered:  
**save**
- 22** Activate the schedule tuple for the stream by performing [Configuring the outbound file transfer schedule on page 289](#)
- 23** Use the following table to determine your next action.

If you	Do
want to change the RTB configuration on another billing stream	step <a href="#">16</a>
do not want to change the RTB configuration on another billing stream	step <a href="#">27</a>

- 24** Deactivate the schedule tuple for the stream by performing [Configuring the outbound file transfer schedule on page 289](#)

- 25** Delete the RTB configuration from a billing stream:

```
delete <stream_name> <file_format>
<destination>
```

*where*

**<stream\_name>**

is the name of the configured billing stream

**<file\_format>**

is the file format of the configured stream

**<destination>**

is the billing file transfer destination

*Example response:*

```
Are you sure you want to delete the RTB tuple?
(Y/N) .
```

- 26** Confirm the delete command:

```
y
```

If you	Do
want to delete RTB from another billing stream	step <a href="#">24</a>
do not want to delete RTB from another billing stream	step <a href="#">27</a>

- 27** Quit the BILLMTC interface:

```
quit all
```

- 28** You have completed this procedure.



---

## Configuring a billing stream on the core manager

---

### Purpose

Use this procedure to add, change, or delete a billing stream on the core manager.

### Application

SBA only supports SMDR streams in DNS file format. SBA does not support an SMDR stream in DIRP file format.

The core manager allows you to configure an SMDR stream in DIRP file format. However, when you try to activate the SMDR stream from the Core (with DIRP file format) by using the command **sdbmctrl smdr on** or **sdbmctrl smdr both**, the command fails and the system displays the following error message: "The stream is not configured or not supported on the SDM."

### Prerequisites

You must be a user in a role group authorized to perform accounting-manage actions.

For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	Core and Billing Manager 850 Security and Administration, NN10358-611
Displaying actions a role group is authorized to perform	Core and Billing Manager 850 Security and Administration, NN10358-611

The following prerequisites apply to this procedure:

- The SBA must be in service when this procedure is performed.
- During this procedure, SuperNode Billing Application (SBA) will prompt you for information based on the task you are performing and the type of billing stream. This information is available in the

configuration questionnaire completed during the procedure  
[Preparing for SBA installation and configuration on page 237](#).

The table [Information prompts](#) lists the information from the questionnaire that may be required during this procedure.

### Information prompts (Sheet 1 of 2)

<b>CONFSTRM: Add command prompts</b>	<b>Values</b>	<b># in questionnaire</b>
Stream name	stream_name	1
Is this a filtered stream	filter_stream	2
Associated stream (not applicable to CM billing streams; used for filtered streams)	associated_stream	3
Filter criteria file (not applicable to CM billing streams; used for filtered streams)	filter_criteria_file	4
Stream record format	record format	5
File format	file_format	6
Please specify the logical volume	logical_volume_name	7
File transfer mode	file_transfer_mode	8
Destination component Id (applicable only for DNS file format)	destination_id	14
Destination component type (applicable only for DNS file format)	destination_type	15
Source component Id (applicable only for DNS file format)	source_id	16
Source component type ((applicable only for DNS file format)	source_type	17
Customer standard header file type (applicable only for DNS file format)	standard_file_type	18
Customer error header file type (applicable only for DNS file format)	error_file_type	19
Files renamed with close date (applicable only for DIRP file format)	files_renamed_with_close_date	10



**Information prompts (Sheet 2 of 2)**

<b>CONFSTRM: Add command prompts</b>	<b>Values</b>	<b># in questionnaire</b>
Files closed on file transfer and writetape (applicable for DIRP file format)	files_closed_on_file_transfer	11
Do you want DIRP blocks closed based on time (applicable only for DIRP file format)	DIRP_blocks_closed_based_on_time	12
File DIRP block closure time limit (in seconds) (applicable only for DIRP file format)	DIRP_block_closure_time_limit	13
Do you want files closed based on time	close_on_timer	20
File closure time limit (not applicable if you do not want files closed based on time)	file_close_time_limit	21
Maximum number of records per day	records_per_day	22
Average record size (not applicable if records per day is 0)	record_size	26
Maximum number of records per file	records_per_file	24
Maximum number of bytes per file	bytes_per_file	25

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Procedure

### Configuring a billing stream on the core manager

#### *At any workstation or console*

1

#### **ATTENTION**

SBA does not support the configuration of more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the billing stream that is saved.

Access the core manager as a user authorized to perform accounting-manage actions.

2 Access the BILLMTC interface:

**billmtc**

*Example response*

*BILLMTC opens at the main level.*

3 Access the CONFSTRM level:

**confstrm**

If you want to	Do
add a billing stream	step <a href="#">4</a>
change the configuration of a billing stream	step <a href="#">11</a>
delete a billing stream	step <a href="#">15</a>

4 Add a stream:

**add <stream\_name>**

*where*

**<stream\_name>**

is the name of the billing stream you want to add

- 5 Follow the prompts to add each value for the billing stream. Refer to table [Information prompts on page 280](#) for more information.
- 6 Verify that the values displayed are the correct values. Examples of DNS, DIRP, and filtered billing streams are displayed on the following pages.

*Example response: CONFSTRM Add for a DNS file format for a Core and Billing Manager*

```
Stream Name -> AMA2
Filter stream -> No
Stream Record Format -> BC
File Format Type -> DNS
Logical Volume Name -> /cbmdata/00/billing/ama2
File Transfer Mode -> OUTBOUND
Destination Component Id -> 2
Destination Component Type -> 3
Source Component Id -> 1
Source Component Type -> 2
Customer Standard Header File Type -> 1
Customer Error Header File Type -> 2
File Closed On Time Valid -> NO
File Closed On Time -> 10080
Number of Records Per Day -> 10080
Average Record Size -> 1000
Maximum number of records -> 10000
Maximum number of bytes -> 1000000

Commit? [Save] {Save Edit Abort}:
```

*Example Response: CONFSTRM Add for a DIRP file format for a Core and Billing Manager*

```
Stream Name -> OCC
Is this a Filter stream -> NO
Stream Record Format -> CDR250
File Format Type-> DIRP
Please specify the logical Volume ->
/cbmdata/00/billing/occ
File Transfer Mode -> OUTBOUND
Do you want the files renamed with close date ->
NO
Do you want the files closed for file transfer
and writetape -> NO
Do you want DIRP blocks closed based on time ->
YES
File DIRP block Closure time limit (in seconds)
-> 2
Do you want Files closed based on time -> NO
Number of Records Per Day -> 1000000
Average Record Size -> 130
Maximum number of records per file -> 100000
Maximum number of bytes per file -> 20000000

Commit? [Save] {Save Edit Abort}:
```

*Example response: CONFSTRM Add for a filtered stream file for a Core and Billing Manager*

```

Stream Name -> FLT1
Is this a Filter stream -> Yes
Associated Stream Name -> OCC
Filter Stream Criteria File ->
/sdm/cfdata/rtfilt/CDR.cdr
Stream Record Format -> CDR250
File Format Type -> DIRP
Logical Volume Name -> /cbmdata/00/billing/flt1
File Transfer Mode -> OUTBOUND
Files Renamed With Close Date -> NO
Files closed for file transfer and writetape ->
YES
Do you want DIRP blocks closed based on time ->
YES
File DIRP block Closure time limit (in seconds)
-> 2
Do you want files closed based on time? -> Yes
File Closure time limit -> 10
Number of Records Per Day -> 0
Average Record Size -> 80
Maximum number of records -> 500000
Maximum number of bytes -> 2000000

Commit? [Save] {Save Edit Abort}:

```

If displayed values are	Do
not correct	step <a href="#">7</a>
correct	step <a href="#">9</a>

- 7** Edit the displayed values:  
**edit**
- 8** Correct the values as necessary.

- 9** Save the displayed values:  
**save**  
*Example response:*  
Saving stream  
  
Configuration of stream is now complete.  
  
Press Return to continue.
- 10** Press the Enter key to return to the CONFSTRM level.

If you	Do
want to add another billing stream	step <a href="#">4</a>
do not want to add another billing stream	step <a href="#">18</a>

- 11** Change the configuration for a particular billing stream:  
**change <stream\_name>**  
*where*  
**<stream\_name>**  
is the name of the billing stream to change
- 12** Follow the prompts on the screen to change the value of the fields. Refer to table [Information prompts on page 280](#) for more information.  
  
**Note:** Changing the file format between DIRP and DNS is not supported. You must delete the stream and re-add using the desired format.
- 13** Save the displayed values:  
**save**  
*Example response:*  
Saving stream  
  
Configuration of stream is now complete.  
  
Press Return to continue.

- 14 Press the Enter key to return to the CONFSTRM level.

If you	Do
want to change the configuration of another billing stream	step <a href="#">11</a>
do not want to change the configuration of another billing stream	step <a href="#">18</a>

- 15

**ATTENTION**

You must turn off (deactivate) the billing stream from the Core before you can delete the stream on the core manager.

Delete the billing stream:

```
delete <stream_name>
```

*where*

```
<stream_name>
```

is the name of the billing stream to delete

- 16 Follow the prompts on the screen to change the value of the fields.

**Note:** Changing the file format between DIRP and DNS is not supported. You must delete the stream and re-add using the desired format.

- 17 Confirm the delete command:

```
yes
```

If you	Do
want to delete another billing stream	step <a href="#">15</a>
do not want to delete another billing stream	step <a href="#">18</a>

- 18 Exit the CONFSTRM level:

```
quit
```

**19** You have completed this procedure.



## Configuring the outbound file transfer schedule

### Purpose

Use this procedure to perform the following functions for outbound file transfer for a billing stream:

- add a schedule tuple
- change the schedule tuple
- delete a schedule tuple

### Prerequisites

You must be a user in a role group authorized to perform accounting-manage actions.

For information on how to log in to the CBM as an authorized user or how to display information about a user or role group, review the procedures in the following table.

Procedure	Document
Logging in to the CBM	Core and Billing Manager 850 Security and Administration, NN10358-611
Displaying actions a role group is authorized to perform	Core and Billing Manager 850 Security and Administration, NN10358-611

This procedure requires a configured billing stream. Perform the procedure [Configuring a billing stream on the core manager on page 279](#). The billing stream must support DIRP record format and outbound file transfer.

This procedure requires information from the configuration questionnaire completed during the procedure [Preparing for SBA installation and configuration on page 237](#). SBA will prompt for the appropriate information, based on the task you are performing and the type of billing stream. The following table [Required information](#) lists the

information from the questionnaire that may be required during this procedure.

### Required information (Sheet 1 of 2)

Prompt	Values	Question # from questionnaire
Enter stream	stream_name	1
Enter file_format_type	file_format	6
Enter destination	destination	29
Enter protocol	protocol	30
Enter primary_destination	primary_destination	31
Enter primary_port	primary_port	32
Enter alternate_destination	alternate_destination	33
Enter alternate_port	alternate_port	34
Enter start_time	schedule_start_time	43
Enter stop_time	schedule_stop_time	44
Enter interval	schedule_interval	45
Enter remote_storage_directory	remote_storage_directory	37
Enter remote_login	remote_login	35
	<b>Note:</b> Special characters may not work in all operating environments. Use special characters only when necessary for outbound file transfer schedules.	
Enter remote_password	remote_password	36
Enter maximum_retries	protocol_max_retries	40
Enter retry_wait_time	protocol_retry_wait_time	41
Enter file_extension	file_extension	39

**Required information (Sheet 2 of 2)**

Prompt	Values	Question # from questionnaire
Enter field_separator	field_separator	38
Enter active	schedule_active	42

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

**ATTENTION**

Special instruction after the customer upgrades the SDM/CBM from a previous release to 23 release:

After an upgrade of SDM/CBM to release 23, once a new SBA schedule is added or an existing SBA schedule is modified, the customer is not advised to fallback since the old password details (stored in PDM) are re-formatted and stored as a new file. In such scenario, if the customer falls back to a previous release, the old password details (stored in PDM) would not be available as the old data file would have been deleted, and hence the customer may have to reconfigure the schedules in order to get the Billing files transferred to downstream.

**Procedure****Configuring the outbound file transfer schedule*****At any workstation or console***

- 1 Log into the core manager.
- 2 Log into the core manager as a user authorized to perform accounting-manage actions.
- 3 Access the billing maintenance level:  
**billmtc**
- 4 Access the schedule level:  
**schedule**

**5** Determine schedule tuple action.

If you are	Do
adding a schedule tuple	step <a href="#">6</a>
changing a schedule tuple	step <a href="#">13</a>
deleting a schedule tuple	step <a href="#">18</a>

**6** Add a schedule tuple for a billing stream:**add****7****ATTENTION**

Do not configure multiple schedule tuples with the same destination, directory, file format, and file extension. Collisions between billing file names can occur.

Follow the prompts to each value for the schedule tuple. Refer to the table at the start of the procedure for more information. Press the Enter key after entering each value.

**Note:** If you select SFTPW/KSFTP protocol, for secure outbound data transfer, you must first complete the following tasks:

- OpenSSH must be installed on the core manager
- you must manually accept the known host key for the downstream OSS destination, by performing the procedure [Configuring SBA outbound connection security on page 299](#)

When you have completed all fields, SBA displays the values that you entered.

*Example response when FTPW protocol is selected*

```

Stream: `AMA`
File_Format_Type: `DNS`
Destination: `OSS`
Protocol: `FTPW`
Primary_Destination: `47.32.45.67`
Primary_Port: `21`
Alternate_Destination: `47.32.67.86`
Alternate_Port: `21`
Start_Time: `00:00`
Stop_Time: `00:00`
Interval: `120`
Remote_Storage_Directory:
`/home/amabilling/billingfiles`
Remote_Login: `amabilling`
Remote_Password: `*****`
Timeout: `30`
Maximum_Retries: `3`
Retry_Wait_Time: `1`
File_Extension: ``
Field_Separator: `.`
Active: `Yes`

```

Valid actions are {'Save', 'Edit', 'Abort'}.  
 Press Enter to accept 'Edit'.  
 Enter Action:

- 8** Verify that the values displayed are the correct values.

If the values displayed are	Do
not correct	step <a href="#">9</a>
correct	step <a href="#">11</a>

- 9** Press the Enter key to edit the tuple.
- 10** Enter the name of the field to change, or enter "all" and enter the corrected information for the appropriate field or fields.
- 11** Save the schedule tuple:  
**save**

*Example response:*

Schedule tuple saved

Press Return to Continue

- 12** Press the Enter key to return to the schedule level.

If you	Do
want to add another schedule tuple	step <a href="#">6</a>
do not want to add another schedule tuple	step <a href="#">21</a>

- 13**

**ATTENTION**

You can not change the stream name, file format, and destination fields in a schedule tuple.

If the schedule tuple supports real time billing (RTB), you can not change the value of the protocol.

Change the value of one or more fields in the schedule tuple for a particular stream:

**change** <stream\_name>

where

<stream\_name>

is the name of the billing stream associated with the schedule tuple you want to change

**Note:** If you select to change the protocol field, the primary and alternate ports is re-prompted.

If you	Do
receive the following warning	step <a href="#">14</a>
do not receive the following warning	step <a href="#">15</a>

*Example of warning*

Warning: Do not delete this Schedule tuple or proceed with the current modification if there exists a configured RTB destination which depends on it.

- 14** Offline and delete the corresponding RTB destination before continuing with this procedure. Contact your next level of support if you have any questions regarding the steps to take or the consequences of this action.

**15**

**ATTENTION**

Do not configure multiple schedule tuples with the same destination, directory, file format, and file extension. Collisions between billing file names can occur.

Follow the prompts on the screen to change the value of the desired fields.

**Note:** If you select SFTPW/KSFTP protocol, for secure outbound data transfer, you must first complete the following tasks:

- OpenSSH must be installed on the core manager
- you must manually accept the known host key for the downstream OSS destination, by performing the procedure [Configuring SBA outbound connection security on page 299](#)

When you have completed all fields, SBA displays the values that you entered.

- 16** When prompted, save the changed schedule tuple:

**save**

*Example response:*

Schedule tuple saved

Press Return to Continue

- 17 Press the Enter key to return to the schedule level.

If you	Do
want to change another schedule tuple	step <a href="#">13</a>
do not want to change another schedule tuple	step <a href="#">21</a>

- 18

**ATTENTION**

When the schedule tuple for a stream has a corresponding tuple with the same destination, you must delete the RTB tuple before you delete the schedule tuple.

Delete the schedule tuple for the billing stream:

```
delete <stream_name>
```

*where:*

**<stream\_name>**

is the name of the billing stream associated with the schedule tuple to delete

If you	Do
receive the following warning	step <a href="#">19</a>
do not receive the following warning	step <a href="#">20</a>

*Example of warning*

Warning: Do not delete this Schedule tuple or proceed with the current modification if there exists a configured RTB destination which depends on it.

- 19 Offline and delete the corresponding RTB destination before continuing with this procedure. Contact your next level of support if you have any questions regarding the steps to take or the consequences of this action.



**20** Confirm the delete command:

**yes**

If you	Do
want to delete another schedule tuple	step <a href="#">18</a>
do not want to delete another schedule tuple	step <a href="#">21</a>

**21** Exit the billing maintenance menu:

**quit all**

**Note 1:** You can test the file transfer settings by executing a manual file transfer by using the **Sendfile** command and checking that the billing file is transferred to the correct directory of the downstream destination. You can find the **Sendfile** command at position 7 of the FILESYS level from the BILLMTC menu.

**Note 2:** If you perform an action on the downstream server, for example, shut down the server. This action makes the ftp service on the server unavailable to the core manager. Always delete the associated schedule tuple on the core manager first. If you do not, an FTPW alarm is generated on the CM. Refer to procedure Clearing an FTPW alarm in the core manager documentation, to clear the alarm.

**22** You have completed this procedure.



---

## Configuring SBA outbound connection security

---

### Purpose

The SBA outbound connection security feature provides secure outbound file transfer using the OpenSSH SFTP (secure file transfer protocol) client. The SFTP client protects all data, including sensitive users' passwords, by encrypting the data before it leaves the core manager and decrypting the data after it arrives at the downstream OSS destination. The SFTP client also provides data integrity checking to ensure that the data has not been tampered with during the transfer.

Both password-based authentication and key-based (public key) authentication are supported for secure outbound file transfers using the OpenSSH SFTP.

### Prerequisites

The following prerequisites apply to the SBA outbound connection security feature:

- You must be the root user to perform this procedure.
- An SSH sftp server (SFTP server subsystem) that is compatible with the OpenSSH sftp client must be running on the downstream Operations Support System (OSS) in order for the SBA to transfer data with the OpenSSH sftp client.
- OpenSSH software, version 3.7.1p2 or later, and any dependent software must be installed on the core manager in order for SFTPW (Secure File Transfer Protocol wrapper) protocol for outbound file transfer to be used. There is no explicit check performed by the SBA software to determine whether this package or fileset is installed when the SFTPW is being configured. Thus, if the SBA SFTPW application fails to find the sftp program, an SFTPW alarm is raised and the application terminates any transfer event it is attempting to perform.
- For the CBM, the SBA outbound connection security feature depends on the OpenSSH packages as well as NTutil.
- For the SDM and CS 2000 Core Manager, the SBA outbound connection security feature depends on the SDM\_OpenSSH.base fileset, which must be installed manually, and the SDM\_BASE.util fileset.
- The initial host key acceptance of the downstream processor should be performed manually in order for the SFTPW to be used for file transfer from the core manager. The .ssh/known\_hosts file in the maint home directory is edited by SSH software to include the host key. After this is completed, sftp can be used to send files to the

downstream OSS. This step must be performed for each downstream destination prior to schedule tuple configuration for SFTPW.

### Limitations and restrictions

The following limitations and restrictions apply to the SBA outbound connection security feature:

- The SBA outbound connection security feature does not secure data transfer for the RTB application.
- SBA secure outbound file transfer (SFTPW/KSFTP) cannot re-send ClosedSent files when ClosedSent files already exist on the target directory in the downstream system. Therefore, it is important that existing ClosedSent (or processed) files at the downstream system be either moved to another directory or re-named before an attempt is made to re-send ClosedSent files from the core manager to the downstream system.
- The data transfers of AFT, RTB and sendtape applications are not secured
- Automatic dumping of the public key file on the remote system is not supported. Users have to manually dump the contents of the public key file into the user's authorization file on the remote system.

If the remote system is running OpenSSH server, the public key should be appended to `.ssh/authorized_keys` or `.ssh/authorized_keys2` file.

- The user SHELL (cshrc or bash) startup script at the downstream system must not contain ANY echo or print statements which will interfere the handshaking between sftp client and sftp-server. The symptom is that the sftp session terminated pre-maturely and the message "Received message too long <a long num> is printed".

### Procedure

To configure secure data transfer to a downstream OSS destination, it is necessary to first accept the known host key for the downstream OSS destination. Steps [1](#) through [10](#) of this procedure enable you to perform this task. This task must be performed whenever the destination downstream OSS is rebooted or whenever the SFTPD server on the OSS is restarted.

**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Configuring SBA outbound connection security

### At the PC or UNIX workstation

- 1 Establish a telnet connection to the core manager by completing the following substeps.
  - a Open a terminal window that is VT100 compatible.
  - b Log onto the core manager from the terminal window prompt:  
`telnet <ip_address>`  
 where:  
     `<ip_address>`  
     is the IP address of the core manager
  - c When prompted, enter the login ID and password for the root user.
- 2 Change directory to the maint home directory:  
`cd ~maint`
- 3 Look in the maint directory for the “.ssh” directory:  
`ls -lad .ssh`

If	Do
the .ssh file does not exist	step <a href="#">4</a>
the .ssh file does exist	step <a href="#">10</a>

- 4 Create the .ssh directory:  
`mkdir .ssh`
- 5 Change the .ssh directory ownership:  
`chown maint:maint .ssh`
- 6 Change the permissions associated with the .ssh directory:  
`chmod u+rwX .ssh`
- 7 Change to the maint user:  
`su maint`
- 8 Run the ssh client to the downstream OSS destination by providing a “maint” user name and IP address for the ssh client, by performing the following steps:

- a** Type
- ```
ssh -l maint <nn.nn.nn.nn>
```
- where
- <nn.nn.nn.nn> is the IP address of the ssh client
- Example of response
- The authenticity of host '10.10.10.10' can't be established.  
RSA key fingerprint is  
3a:d5:d7:6e:ee:6b:45:fc:b9:0b:92:a7:1c:d8:f1:be.  
Are you sure you want to continue connecting (yes/no)?
- b** Type
- ```
yes
```
- Example of response
- Warning: Permanently added '10.10.10.10' (RSA) to the list of known hosts.
- 9** Press ctrl + C to terminate the program.
- 10** Exit the telnet session:
- ```
exit
```
- 11** Configure the outbound file transfer schedule for secure data transfer. The protocol used for secure data transfer is SFTPW (secure file transfer protocol wrapper) for password-based authentication, or KSFTP for key-based authentication. For the procedure on how to configure an outbound file transfer schedule, refer to [Configuring the outbound file transfer schedule on page 289](#).
- 12** For KSFTP, if the downstream machine is running OpenSSH Server, append a public key to authorized\_keys of the user on the downstream machine. Use the following commands:
- On SDM/CBM:
- ```
login: root
root Password: xxxx
cd ~maint/.ssh
ssh user@47.135.214.66 'cat >>
.ssh/authorized_keys' < id_rsa.pub
Password:
```
- 13** You have completed this procedure.

## Troubleshooting

Possible error scenarios that may occur when you are performing this procedure and the steps to perform in addressing these problems are listed below:

- Connection refused

This error causes a “Down” status for the SSH Collector Status parameter.

### Example

Error : ssh; connect to host <hostname/hostip> port 22:  
Connection refused  
Connection closed.

To resolve this problem:

- Verify that the host machine is on the network.
- Verify that the SSH server on the host machine is running and that the configuration is correct (such as, the port number and fingerprint).

- SSH not found

This error is caused by the ssh not being installed on the core manager.

### Example

Error: /bin/ksh: ssh: not found.

To resolve this problem:

- Verify that the OpenSSH package is installed on the system.

**Note:** If your core manager is an AIX-based SDM or CS 2000 Core Manager, you can verify whether the OpenSSH package is installed by checking for the package at the SWIM level of the sdmmtc user interface.

If the package is not installed, contact your Nortel service representative for assistance in installing the OpenSSH package provided by Nortel.

**Note:** You should not install the OpenSSH package downloaded from the web unless you are instructed to do so by your Nortel service representative.

- known\_hosts file cannot be datafilled

This error is caused by the non-existence of, or incorrect permissions for, the `/home/maint/.ssh` (AIX-based SDM) or `/cbmdata/users/maint/.ssh` (CBM) directory.

To resolve this problem:

- Verify that you are logged in as the root user and that you switched user (`su`) to the maint user.
- Verify that the directory `/home/maint/.ssh` (AIX-based SDM) or `/cbmdata/users/maint/.ssh` (CBM) is present and has read/write permissions set for the maint user. If the directory doesn't exist, create it.
- Verify that the correct IP address is used for host key acceptance.

- SSH server's host key has changed

If the server's host key has changed, the client will notify you that the connection cannot proceed until the server's host key is deleted from the `known_hosts` file using a text editor. Before performing this task, you must contact the system administrator of the SSH server to ensure that the server operation will not be compromised.

To resolve this problem:

- Try to create an ssh connection to a different machine. If you receive an error message about a changed or incorrect public key, it is probably due to the host changing its public key. Edit the file `/home/maint/.ssh/known_hosts` using a text editor and delete any line containing the name of that host.
- Try to create an ssh connection to that host again and then accept a new public key for the host.

- SSH warns about "man-in-the-middle attack"

This problem is caused either by someone eavesdropping on your connection or by the host key having been changed.



To resolve this problem:

- Contact your system administrator to determine whether the host key has been changed or whether the ip address of the client has been changed.
- Edit the file `/home/maint/.ssh/known_hosts` using a text editor and delete any line containing the name of that host.
- Datafill the `known_host` keys with new information.
- sftp session terminated pre-maturely with the message "Received message too long <a long num>".

Ensure that the user SHELL (`cshrc` or `bash`) startup script at the downstream system does not contain any `echo` or `print` statements which will interfere the handshaking between sftp client and sftp-server.



---

## Creating USP Disaster Recovery Floppy Disks

---

The disaster recovery operation is used when it is necessary to restore the programs and data stored on your OAM&P workstation. The disaster recovery operation depends on the use of disaster recovery floppy disks. You can use the tape drive application to create the two disaster recovery floppy disks required to perform the disaster recovery operation.

To create the disaster recovery floppy disks, perform the following steps:

### ***At the OAM&P workstation***

- 1 Label two formatted floppy disks as Disaster Recovery Disk 1 and Disaster Recovery Disk 2.
- 2 Insert Disaster Recovery Disk 1 into the A: drive in your OAM&P workstation and follow the directions.

**Note 1:** The disaster recovery floppy disk creation process does not format the disks for you, but it does erase all of the data on the disks. Ensure that you have copied important data from the disks before proceeding.

**Note 2:** For more information on creating disaster recovery disks, refer to the tape drive documentation provided with the OAM&P workstation.





# Powering Down the Network

## Purpose of this procedure

This procedure details the sequence of steps necessary to power down all of the network elements in the office. Not all network elements covered in this procedure will apply to your office. The network elements covered by this procedure include:

- XA-Core
- 3rd Party Core
- Message Switch
- ENET
- Ethernet Routing Switch 8600
- LPP
- SDM, CS 2000 Core Manager, or Core and Billing Manager
- IEMS
- CS 2000 Management Tools
- MG 9000 Manager
- Border Control Point Manager
- SAM21 shelf and cards
- CICM
- USP
- Session Server
- Policy Controller
- Media Gateway 15000/7400 or Multiservice Switch 15000/7400
- MDM workstation
- SPM, MG 4000, IW-SPM, DPT-SPM
- MCS servers
- Border Control Point

- MS 2000 Series or UAS
- Packet Media Anchor
- MG 9000

### **When to use the procedure**

Use this procedure when it is necessary to power down the network office.

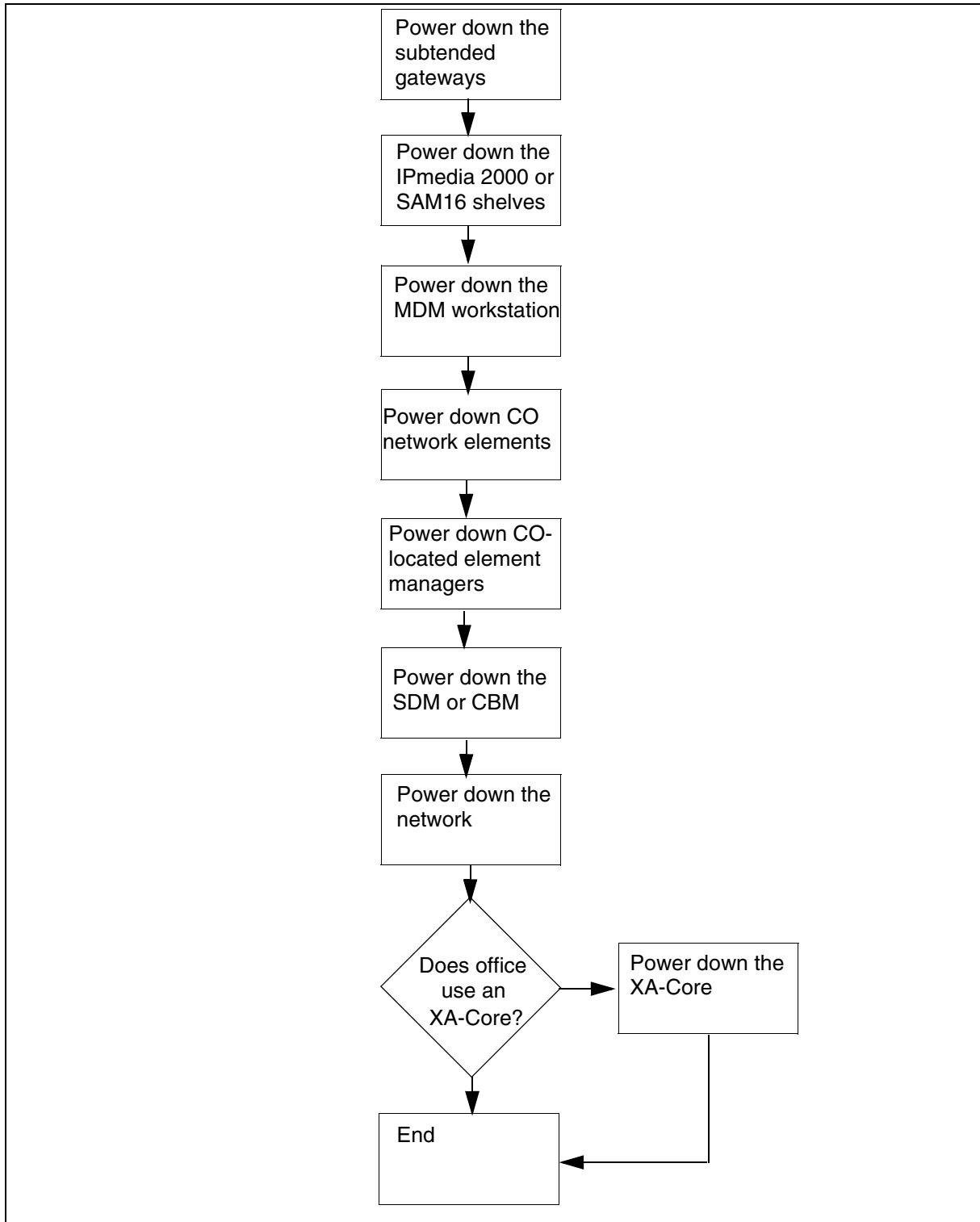
### **Prerequisites**

The network elements should be backed up before powering down if time permits.

### **Action**

This procedure contains a summary flowchart and a list of steps. Use the flowchart to review the procedure. Follow the steps to perform the recovery task.

**Figure 1 Summary of procedure**



***In the network office***

- 1** Power down the subtended gateways, such as the MG 9000 and MTA.

For the MG 9000, refer to [Powering down an MG 9000 device on page 315](#) or [Performing a partial power down of the MG 9000 on page 317](#).

For other third party devices, refer to the documentation for your device.

- 2** Power down the shelves that house the MS 2000 Series/UAS devices and the Packet Media Anchor.

If your system uses an MS 2000 Series device or Packet Media Anchor, refer to [Powering down the IPmedia 2000 shelves on page 319](#). If your system uses a UAS, refer to [Powering down the SAM16 shelves on page 321](#).

- 3** If equipped, power down the Border Control Point.

Refer to [Powering down an Border Control Point on page 323](#).

- 4** If equipped, power down the MCS Servers.

Refer to [Powering down the MCS servers on page 325](#).

- 5** Power down the MDM workstation.

Refer to [Powering down the MDM workstation on page 327](#).

- 6** Power down the CO network elements, including the SPMs, Multiservice Switch 15000/7400, Media Gateway 15000/7400, and USP.

Refer to the following procedures:

- [Powering down an SPM device on page 329](#) or [Performing a partial power down of the SPM on page 333](#)
- [Powering down a Media Gateway/Multiservice Switch 7400 on page 335](#)
- [Powering down a Media Gateway/Multiservice Switch 15000 on page 337](#) or [Performing a partial power down of the Media Gateway/Multiservice Switch 15000 on page 339](#)
- [Powering down a USP on page 343](#) or [Performing a partial power down of the USP on page 345](#)

- 7** Determine if you are powering down a CS 2000 or CS 2000-Compact-based office.

**If you are powering up a**

**Do**

CS 2000-based office

step [8](#)



If you are powering up a	Do
CS 2000-Compact-based office	step <a href="#">10</a>
<b>8</b>	Power down the SAMF frame. This will, in turn, power down the Session Server, Policy Controller, SAM21 SCs, and GWCs. Refer to <a href="#">Powering down the SAMF frame on page 357</a> .
<b>9</b>	Go to step <a href="#">11</a> .
<b>10</b>	Power down the Call Control Frame (CCF). This will, in turn, power down the Session Server, SAM21 SCs, GWCs, and CICM. Refer to <a href="#">Powering down the Call Control Frame on page 401</a> .
<b>11</b>	If equipped, power down the Border Control Point Manager. Refer to <a href="#">Powering down the Border Control Point Manager on page 413</a> .
<b>12</b>	Power down the CO located element managers, such as the IEMS, CS 2000 Management Tools, and MG 9000 Manager. Refer to <a href="#">Powering down an T1400 or N240 server on page 415</a> or <a href="#">Performing a partial power down of the N240 server on page 417</a> .
<b>13</b>	If equipped, power down the DNS server. Refer to the hardware documentation for your server for detailed instructions.
<b>14</b>	Power down the SDM or CBM. For the SDM, refer to <a href="#">Powering down the SDM on page 419</a> . For the CBM, refer to <a href="#">Powering down an T1400 or N240 server on page 415</a> or <a href="#">Performing a partial power down of the N240 server on page 417</a> .
<b>15</b>	Power down the IP network, including the Ethernet Routing Switch 8600 and the IP switches. Refer to <a href="#">Powering down a Ethernet Routing Switch 8600 on page 421</a> or <a href="#">Performing a partial power down of the Ethernet Routing Switch 8600 on page 423</a> .
<b>16</b>	Determine if you are powering down a CS 2000 or CS 2000-Compact-based office.
If you are powering up a	Do
CS 2000-based office	step <a href="#">17</a>
CS 2000-Compact-based office	step <a href="#">18</a>

- 17** If you are powering down a CS 2000-based office, power down the XA-Core.  
Refer to [Powering down the XA-Core on page 425](#) or [Performing a partial power down of the XA-Core on page 429](#).
- 18** You have completed this procedure.

## Powering down an MG 9000 device

### Purpose of this procedure

This procedure details the sequence of steps necessary to power down Media Gateway 9000 (MG 9000).

### When to use this procedure

Use this procedure when it is necessary to power down the MG 9000.

### Prerequisites

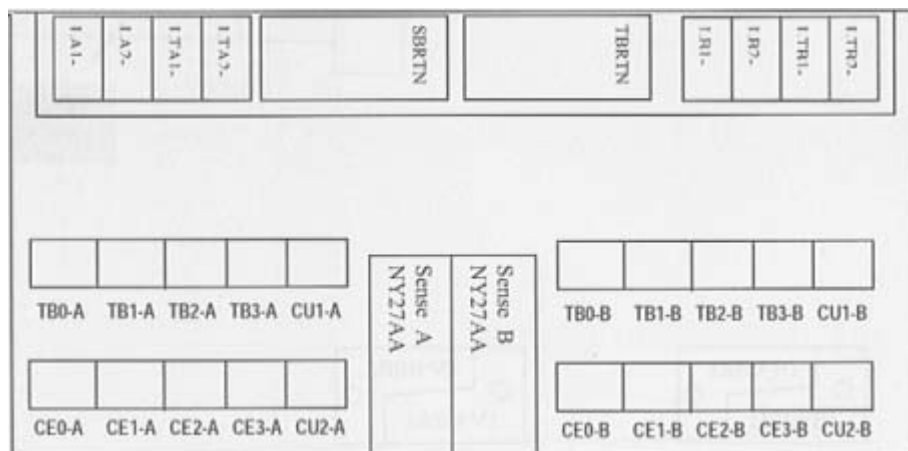
The optimal Power Threshold should be 43.7 volts. The minimum is 42.5.

### Action

#### *At the MG 9000 frame*

- 1 Remove the CE (SB) Fuses from the frame. Refer to the following figure to identify the fuse locations.

#### **MG 9000 frame**



**Note:** It is recommended to only unseat the fuses to allow for rapid restoration.

- 2 Remove the TB fuses from the frame.
- 3 Remove the CU fuses from the frame.
- 4 You have completed this procedure.



---

## Performing a partial power down of the MG 9000

---

### Purpose

This procedure is used to perform a partial power down of an MG 9000.

### Prerequisites

None

### Action

#### Performing a partial power down of the MG 9000

##### *At the MG 9000 Manager*

- 1 Determine the inactive Supercore, ITP, and ITX cards.
- 2 Lock each inactive card using the MG 9000 Manager.
- 3 Take the cards offline using the MG 9000 Manager.
- 4 Once the cards are offline, they can be manually unseated.
- 5 You have completed this procedure.



---

## Powering down the IPmedia 2000 shelves

---

### Purpose of this procedure

Use the following procedure to power down the IPmedia 2000 shelves that house the MS 2000 series devices and the Packet Media Anchor. The IPmedia 2000 shelves reside in either a SAMF frame or CCF, depending on whether or not your solution uses the CS 2000 or CS 2000-Compact.

### When to use this procedure

Use this procedure when it is necessary to power down the IPmedia 2000 shelves.

### Prerequisites

None

### Action

#### Powering down the Media Server 2000 servers

##### *At the CCF or SAMF frame*

- 1 Open the front door of the CCF/SAMF frame.
- 2 At the EBIP at the top of the frame, turn the breaker associated the Media Server to the OFF position.
- 3 You have completed this procedure.





---

## Powering down the SAM16 shelves

---

### Purpose of this procedure

Use the following procedure to power down the SAM16 shelves that house the UAS devices. The SAM16 shelves reside in either a SAMF frame or CCF, depending on whether or not your solution uses the CS 2000 or CS 2000-Compact.

### When to use this procedure

Use this procedure when it is necessary to power down the SAM16 shelves.

### Prerequisites

None

### Action

#### Powering down the SAM16 shelves

##### *At the CCF or SAMF frame*

- 1 Open the front door of the CCF/SAMF frame.
- 2 At the EBIP at the top of the frame, turn the breakers associated the SAM16 to the OFF position.
- 3 You have completed this procedure.



---

## Powering down an Border Control Point

---

### Purpose of this procedure

Use the following procedure to power down a Border Control Point. The Border Control Point shelves are powered from either a PDU or EBIP located at the top of the frame depending on if the frame is AC or DC powered.

### When to use this procedure

Use this procedure when it is necessary to power down the chassis that houses the Border Control Point.

### Prerequisites

None

### Action

#### Powering down the Border Control Point

##### *At the frame housing the Border Control Point*

- 1 Power down the shelf by switching the breaker on the back of the chassis to the OFF position.
- 2 For AC powered shelves, push the rocker located on the top of the AC outlet to apply power to the chassis. It should be switched to the "0" position.
- 3 For DC powered shelves, switch the circuit breakers at the EBIP that provide power to the shelf being powered to the OFF position. The breaker will have the '0' side (bottom) of the breaker depressed.
- 4 You have completed this procedure.



## Powering down the MCS servers

---

### Purpose of this procedure

This procedure details the steps needed to power down the 8 MCS servers.

### When to use this procedure

Use this procedure to power down the MCS servers.

### Prerequisites

None

### Action

#### *At the frame housing the MCS servers*

- 1 Power down the MCS servers by turning off the circuit breakers that provide power to the servers.
- 2 You have completed this procedure.



---

## Powering down the MDM workstation

---

### Purpose of this procedure

Use the following procedure to power down the MDM Sun Fire™ V480 workstation.

### When to use this procedure

Use this procedure when it is necessary to power down the MDM workstation.

### Prerequisites

It is recommended that you shut down the MDM workstation while on battery power.

### Action

#### Powering down the MDM workstation

##### *At the workstation terminal window*

- 1 Type the following commands followed by the Enter key:  
# `/bin/sync`  
# `/bin/sync`  
# `/sbin/init 0`
- 2 The workstation should shut down.
- 3 You have completed this procedure.





---

## Powering down an SPM device

---

### Purpose of this procedure

This procedure details the sequence of steps necessary to power down and a Spectrum Peripheral Module (SPM), Media Gateway 4000 (MG 4000), Interworking Spectrum Peripheral Module (IW-SPM), or Dynamic Packet Trunking Spectrum Peripheral Module (DPT-SPM).

### When to use this procedure

Use this procedure when it is necessary to power down the SPM/MG 4000/IW-SPM/DPT-SPM.

### Prerequisites

MG 4000s may or may not be located at the same location as the Call Server and therefore power conservation may or may not need to be considered separately from the core location.

### Action

#### *At the MAP terminal*

- 1 Post and busy the trunks for the SPM or MG 4000 to be powered down at the TTP level by typing

```
>MAPCI;MTC;TRKS;TTP;POST D SPM <spm_no>;BSY ALL
```

and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000

**Note:** This procedure is not necessary for the IW-SPM or DPT-SPM.

- 2 Busy all the trunks in the PRADCH level by typing

```
>PRADCH;POST AD SPM <spm_no>; BSY all
```

and pressing the Enter key.

where

**spm\_no**

is the number of the SPM or MG 4000

**Note:** This procedure is not necessary for the IW-SPM or DPT-SPM.

- 3 Access the carrier level by typing  
**>QUIT ALL;MAPCI;MTC;TRKS;CARRIER**  
and pressing the Enter key.
- 4 Post and busy the DS1P carriers by typing  
**POST SPM <spm\_no> DS1P; BSY ALL**  
and pressing the Enter key.  
where  
**spm\_no**  
is the number of the SPM/MG 4000/IW-SPM/DPT-SPM
- 5 Post and busy the VT15P carriers by typing  
**POST SPM <spm\_no> VT15P; BSY ALL**  
and pressing the Enter key.  
where  
**spm\_no**  
is the number of the SPM/MG 4000/IW-SPM/DPT-SPM  
**Note:** The VT15P and DS3P carriers may not both exist.
- 6 Post and busy the DS3P carriers by typing  
**POST SPM <spm\_no> DS3P; BSY ALL**  
and pressing the Enter key.  
where  
**spm\_no**  
is the number of the SPM/MG 4000/IW-SPM/DPT-SPM  
**Note:** The VT15P and DS3P carriers may not both exist.
- 7 Post and busy the STS1P carriers by typing  
**POST SPM <spm\_no> STS1P; BSY ALL**  
and pressing the Enter key.  
where  
**spm\_no**  
is the number of the SPM/MG 4000/IW-SPM/DPT-SPM
- 8 Post and busy the STS3cp carriers by typing  
**POST SPM <spm\_no> STS3cp; BSY ALL**  
and pressing the Enter key.  
where

**spm\_no**

is the number of the MG 4000/IW-SPM

**Note:** This step only applies to an MG 4000 or IW-SPM.

- 9 Post and busy the STS3L carriers by typing  
**POST SPM <spm\_no> STS3L; BSY ALL**  
and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 10 Post and busy the OC3s carriers by typing  
**POST SPM <spm\_no> OC3s; BSY ALL**  
and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 11 Access the PM level by typing  
**>QUIT ALL;MAPCI;MTC;PM;POST SPM <spm\_no>**

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 12 Select and BSY the inactive RMs by typing  
**>SELECT <rm\_type> <inactive\_rm\_number>; BSY**  
and pressing the Enter key.

where

**rm\_type**

is the type of RM to select (OC3, DSP, VSP, etc.)

**inactive\_rm\_number**

is the number of the inactive RM

- 13 Select and BSY FORCE the active RMs by typing  
**>SELECT <rm\_type> <active\_rm\_number>; BSY FORCE**  
and pressing the Enter key.

where

**rm\_type**

is the type of RM to select (OC3, DSP, VSP, etc.)

**active\_rm\_number**

is the number of the active RM

- 14** Select and BSY the inactive CEM by typing  
>**SELECT CEM <inactive\_cem\_number>; BSY**  
and pressing the Enter key.  
where

**inactive\_cem\_number**

is the number of the inactive CEM

- 15** Select and BSY FORCE the active CEM by typing  
>**SELECT CEM <active\_cem\_number>;BSY FORCE**  
and pressing the Enter key.  
where

**active\_cem\_number**

is the number of the active CEM

- 16** Power down the SIM cards using the switch on the front. Then pull the fuses from the PCIU.
- 17** Unseat hardware as required to avoid water damage, shorts, etc.
- 18** You have completed this procedure.

---

## Performing a partial power down of the SPM

---

### Purpose

This procedure is used to perform a partial power down of a DMS-SPM, MG 4000, IW-SPM, or DPT-SPM. In this procedure, SPM refers to the completed family of SPM devices unless otherwise noted.

### Prerequisites

None

### Action

#### Performing a partial power down of the SPM

##### *At the MAP*

- 1 Post the SPM to be powered down by typing  
**>POST SPM <spm\_no>**  
and pressing the Enter key.  
where  
**spm\_no**  
is the number of the SPM to be powered down
- 2 For a power down of the DMS-SPM or IW-SPM, identify which ENET plane was powered down.
- 3 Determine if the active CEM is lined up to the ENET plane that was taken down.
- 4 If necessary, SWACT to the inactive CEM to line it up to the inactive CEM.
- 5 Select and busy each inactive resource module by typing  
**>POST <rm\_type> ALL; BSY ALL**  
and pressing the Enter key.  
where  
**rm\_type**  
is SRM, OC3, ATM, GEM, DSP, VSP, ALM, or DLC
- 6 Manually unseat each RM once the BSY command has been completed.
- 7 Perform [step 5](#) for each RM type.

- 8 Post and busy the inactive CEM by typing  
**>POST CEM <inactive\_cem>; BSY**  
and pressing the Enter key.
- 9 Manually unseat the inactive CEM.
- 10 You have completed this procedure.

---

## Powering down a Media Gateway/Multiservice Switch 7400

---

### Purpose of this procedure

Use the following procedure to power down a Media Gateway/Multiservice Switch 7400.

### When to use this procedure

Use this procedure when it is necessary to power down a Media Gateway/Multiservice Switch 7400.

### Prerequisites

Ensure recent provisioning changes are committed.

### Action

#### Powering down a Media Gateway/Multiservice Switch 7400

##### *At the chassis*

1



#### **WARNING**

If primary power to the shelf assembly is on, never set the individual power supply switches to the standby position. This can cause an overload to the on-line power supply.

Turn off the circuit breakers for the outlets that supply power to your switch.

**Note:** The front panel LED of each power supply will remain lit for approximately two minutes after the power supply loses power.

- 2 After a couple of minutes, verify the LEDs for the power supplies, cooling unit, and each processor card faceplate are off.
- 3 You have completed this procedure.





---

## Powering down a Media Gateway/Multiservice Switch 15000

---

### Purpose of this procedure

Use the following procedure to power down a Media Gateway/Multiservice Switch 15000.

### When to use this procedure

Use this procedure when it is necessary to power down a Media Gateway/Multiservice Switch 15000.

### Prerequisites

Recent provisioning changes need to be committed.

### Action

#### Powering up a Media Gateway/Multiservice Switch 15000

##### *At the chassis*

- 1 Breaker interface panels (BIPs) are located at the top of the chassis. Power down all five breakers simultaneously on each BIP, starting at the left.
- 2 Shut off the BIPs in the following order:
  - BIP B2
  - BIP A2
  - Note:** This will shut down the upper shelf.
  - BIP B1
  - BIP A1
  - Note:** This will shut down the lower shelf.
- 3 You have completed this procedure.



---

## Performing a partial power down of the Media Gateway/Multiservice Switch 15000

---

### Purpose

This procedure is used to perform a partial power down of a Media Gateway/Multiservice Switch 15000. This procedure moves the services from a select set of cards to another set of cards. Then it powers down the select set of cards as well as any cards that host the standby ports.

The following slots on each of the two shelves will remain powered up:

- 0
- 3
- 4
- 7
- 8
- 11
- 12
- 15

The high level steps of this procedure include the following activities:

- ensuring that the LAPS ports are active on the powered-up cards and inactive on powered-down cards
- ensuring the active PBG port is on a powered-up card
- ensuring the PBG port that connects to the SAM21 shelf controller is active
- ensuring the correct DS3 card remains active
- switching off selected power breakers

### Prerequisites

None

### Action

#### Performing a partial power down of the Media

## Gateway/Multiservice Switch 15000

### *At the frame*

- 1 Ensure that the active lines are on the cards to remain powered up by typing

```
> d laps/* nearEndRxActiveLine, workingLine,
protectionLine
```

and pressing the Enter key.

- 2 If there are any LAPS ports on a card that will be powered down, a protection switch needs to be performed.

To switch from the protection line to the working line, type

```
> switch -protectionworking laps/x
```

To switch from the working line to the protection line, type

```
> switch -workingtoprotection laps/y
```

- 3 One of the HIOPs on the XA-Core may be powered down for power conservation reasons. Determine which PBG port the HIOP corresponds to by typing

```
> d pbg/* working line
```

Example response

```
Pbg/ *
```

```
+=====+-----+-----+-----+
-----
| Pbg |      working      | Response
+=====+-----+-----+-----+
-----
| 1003 | Lp/10 Sonet/3      |
| 1100 | Lp/11 Sonet/0      |
```

- 4 Determine which PBGs are connected to the XA-Core by typing

```
>d atmif/* remoteatmif
```

and pressing the Enter key.

- 5 Match the PBG port number with the Atmif number.

- 6 Display the Sonet ports to determine whether the remote-end HIOP cards are still in service by typing

```
>d lp/10 sonet/3 operational
```

and pressing the Enter key, followed by typing

```
>d lp/11 sonet/0 operational
```

and pressing the Enter key.

- 7 Determine the states of the losAlarm and rxAisAlarm.  
If the losAlarm is On, then the corresponding HIOP card is likely powered down. If the rxAisAlarm is On, the HIOP card is probably locked.
- 8 Verify that this HIOP card is selected to be powered down for power conservation. The other Sonet port should have no alarms raised under the operational group.
- 9 Select AtmIFs with matching instance numbers. For example, if pbg/1100 and 1003 are provisioned, type  

```
>d atmif/1100 vcc/* vcd tm atmService Category  
>d atmif/1003 vcc/* vcd tm atmService Category
```
- 10 Determine which PBG port is active by displaying the corresponding AtmIf vcc traffic counts. Type  

```
>d atmif/X vcc/Y txcell, rxcell
```
- 11 The active PBG port will have incrementing txcell and rxcell counts. Ensure that the active PGB port's workingLine is on one of the cards that will remain in-service (0, 3, 4, 7, 8, 11, 12, or 15).
- 12 If the Media Gateway 15000 port's workingLine is not on one of the cards that will remain in-service, perform a Swact of the SAM21 Shelf Controller.
- 13 Verify that the other PBG port to this SAM21 shelf now has incrementing txcell and rxcell counts.
- 14 For a 4pDS3Ch or 12pDS3 card pair in slots 14 and 15, type  

```
>d -p lp/14 activeCard, mainCard, spareCard  
Lp/14
```

and press the Enter key.  
where  

```
activeCard  
is Shelf Card/14  
mainCard  
is Shelf Card/14  
spareCard  
Shelf Card/15
```
- 15 Ensure that the active card is in the set of cards that will remain in-service. If not, switch Lp activity by typing  

```
>switch lp/14
```

and press the Enter key.

- 16** Ensure that the activeCard from [step 14](#) matches the MG 9000 equipment that will remain in-service during the power conservation activity. If not, the MG 9000 equipment that is powered down will need to be switched.
- 17** Manually switch off the following breakers on the upper shelf:
  - B2.2
  - B2.5
  - A2.2
  - A2.5
- 18** Manually switch off the following breakers on the lower shelf:
  - B1.2
  - B1.5
  - A1.2
  - A1.5
- 19** You have completed this procedure.

---

## Powering down a USP

---

### Purpose of this procedure

Use the following procedure to power down a Universal Signaling Processor (USP).

### When to use this procedure

Use this procedure when it is necessary to power down the USP.

### Prerequisites

The USP backup data should be up to date. No datafill changes should be made between the final data snapshot and the powering down of the USP.

All users need to be logged out of the USP GUI and CLI.

## Action

### Powering down a USP

#### *At the USP Manager*

1



#### **CAUTION**

The following steps will take the USP out of service. In a redundant network configuration, the USP's mated STP will handle traffic once the USP is powered down.

End office isolation will occur if the USP is configured as a Signaling Gateway.

Inhibit and deactivate all links. Refer to [Configuring Links on page 347](#).

**Note:** The USP bulk-input feature and the CLI can be used to automate these tasks in the event there are a large number of links in question (refer to the "Bulk Data Input of System-db Tables" section of the USP CLI Interface Specification Manual)

- 2 Ensure that the LEDs on slot 13 and slot 16 front panel cards are not lit, and immediately turn off the A/B Power buttons on the control shelf.

- 3** Turn off the A/B Power buttons located on the backside of each extension shelf.
- 4** In the event that access to the USP is not available, it will be necessary to disconnect the power source that feeds the USP.
- 5** You have completed this procedure.



---

## Performing a partial power down of the USP

---

### Purpose

This procedure is used to perform a partial power down of a USP.

### Prerequisites

None

### Action

#### Performing a partial power down of the USP

##### *At the USP frame*

- 1 Unseat the front panel and back panel CC cards in Slot 18, beginning with the CC Slot 18 card on each of the extension shelves.
- 2 Unseat the front panel and back panel CC card in Slot 18 on the Control shelf.
- 3 Open the RTC system node provisioning and maintenance window.
- 4 Click on the System Mgmt item on the main menu to open the System Configuration window.
- 5 Click on the icon for the control CAM shelf to open the shelf\_name window.
- 6 Click on the icon for an RTC system node.

An operational-state of enabled indicates that the card is in-service. An activity state of inactive indicates that the associated card is the inactive RTC.

##### *At the USP frame*

- 7 Ensure the LEDs on the slot 13 and 16 front panel cards are not lit.
- 8 Unseat the inactive RTC card identified in [step 6](#), its associated SCSI (front panel), and the associated cards on the back panel.
- 9 You have completed this procedure.



---

## Configuring Links

---

Links provide the physical connection between two adjacent signaling points in a network. You can add new links and change or delete existing ones.

### Adding Links

To add new links, perform the following steps:

#### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Select the **link-type** for this link from the drop down box. Supported link types include:
  - **ss7iplink**: IP High Speed Link using M2PA, M2UA-SAAL, M2UA-MTP2, or M3UA
  - **atmhslink**: ATM High Speed Link over T1 or E1 interfaces
  - **chanlslink**: Channelized links supporting up to 8 channel over E1 or T1.
  - **lslink**: Low speed link, V.35 or DS0A.
  - **Virtuallink**: used to connect 2 System Identities on the same USP.
  - **mtp2hslink**: MTP L2 High Speed Link.
- 3 Click the **system-id** list and select the system identity to be associated with this link.
- 4 Select a linkset from the **linkset-name** list.
- 5 Assign an unused SLC for this link by entering one in the **SLC** box. This code is a logical representation (0 to 15) of a physical link and is agreed upon with the far end node.

An SLC can only be used once per linkset.
- 6 Select a shelf, slot, and port for the link. Click the... button to display a list of available nodes.
- 7 Indicate whether the system should periodically perform signal link testing (SLT). Click the **periodic-slt-option** check box to change the test status (defaults to unchecked, no test).

Click the check box to toggle between checked and unchecked.

- 8 Use the table below to determine the next step, based on the type of link that you are adding.

If you are provisioning:	Do:
an SS7iplink	complete step <a href="#">9</a> .
an atmhslink	proceed to step <a href="#">10</a> .
a chanlslink	proceed to step <a href="#">11</a> .
an lslink	proceed to step <a href="#">12</a> .
an mtp2hslink	proceed to step <a href="#">13</a> .

- 9 For SS7iplink, complete the following steps:
- a Click the **protocol** list and select a protocol for this link.
  - b Enter the far end destination IP address in the **dest-ipaddress** box.
 

**Note:** The provisioned IP address becomes the primary IP address if the peer is multi-homed. In addition to the primary address, each association on the USP accepts up to four multi-homed IP addresses from the far end.
  - c If the protocol for this link is M2UA-SAAL or M2UA-MTP2, enter an interface identifier in the **IID** box.
 

**Note:** The interface identifier needs to match the peer interface identifier for the link.
  - d In the **local-port** box, enter the number of the local port. For M3UA links, the port is 2905.
  - e In the **remote-port** box, enter the number of the remote port.
  - f Click the **sctp-operation-mode** list and select an operation for the link. If you select **server**, the connection starts. If you select **client**, the client establishes the connection.
 

**Note 1:** If client mode is selected, then **sctp-checksum** must be set (the choices are adler and crc32).

**Note 2:** If the transport protocol is m2ua or m3ua, then you must set the checksum to crc32.
  - g Click the **sctp-parms-index** list and select an SCTP parameter index number to associate with this link.
  - h Proceed to step [14](#).
- 10 For ATM High-speed Links, complete the following steps:

- a Enter a **port** value of 0 for atmhslinks.
  - b To enable MTP3b, select the **MTPb-option** checkbox.  
*Note:* MTP3b support is introduced in USP10.0 to enable the full ATM HSL functionality. Users must select a high-speed link that is capable of transporting MTP3b messages because not all ATM HSL or terminating nodes support MTP3b.
  - c Enter a VCC value in the **vcc** box. The value must be between 0 and 15 for atmhslinks.
  - d Enter a VPI in the **vpi** box. The default is 0.
  - e Enter a VCI in the **vci** box. The default is 5.
  - f Select a SAAL parameter index from the **saal-param-index** list.  
*Note:* There is no default SAAL parameter index.
  - g Select a SAAL timer index from the **saal-timer-index** list.  
*Note:* There is no default SAAL timer index.
  - h Proceed to step [14](#).
- 11 For channelized links, complete the following steps:
  - a Enter a **port** value of 0 for chanlslinks.
  - b Enter a channel in the channel box.
  - c Select a provisioned MTP link timer index from the **I2-timer-index** list.  
The default index is the first available index.  
*Note:* A system-id must be selected prior to selecting the I2-timer-index or a multiple timer list with the same index is displayed.
  - d Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.  
The default index is the first available index.
  - e Indicate whether the system should perform preventive cyclic retransmission (PCR) on the link using the **pcr-option** check box. PCR is recommended for all satellite links, and intercontinental links where the one-way propagation delay is greater than 15 ms. Both the transmitting and receiving

terminal units of the link must use the same error correction method.

**Note:** The default value is unchecked. If PCR is not enabled, the link uses basic error correction at MTP level 2.

- i Select a value between 5 and 20 (representing tenths of a second) in the **l2-t7-timer** box. This value represents the excessive delay of acknowledgement timer. PCR continually re-transmits unacknowledged MSUs until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.

**Note 1:** The default value for the T7 timer is 600 ms.

**Note 2:** Changing the T7 timer value on this screen will not change the T7 timer value for the provisioned timer index. If PCR is selected, the value in the T7 timer box is used for the excessive delay of acknowledgement. If PCR is not selected, the value for T7 in the timer index is used for the excessive delay of acknowledgement.

- ii Select a value between 1 and 50 (representing tenths of a second) in the **pcr-delay** box. This value represents the round trip propagation delay for the link in milliseconds.

The default value is 10, or 1000 ms.

- f Proceed to step [14](#).

**12** For low-speed link, complete the following steps:

- a Enter a **port** value of 0-3 for Islinks.
- b Select a provisioned MTP link timer index from the **l2-timer-index** list.

The default index is the first available index.

**Note:** A system-id must be selected prior to selecting the l2-timer-index or a multiple timer list with the same index will be displayed.

- c Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.

The default index is the first available index.

- d Indicate whether the system should perform preventive cyclic retransmission (PCR) on the link using the **pcr-option** check box. PCR is recommended for all satellite links, and intercontinental links where the one-way propagation delay is greater than 15 ms. Both the transmitting and receiving

terminal units of the link must use the same error correction method.

**Note:** The default value is unchecked. If PCR is not enabled, the link will use basic error correction at MTP level 2.

- i Select a value between 5 and 20 (representing tenths of a second) in the **l2-t7-timer** box. This value represents the excessive delay of acknowledgement timer. PCR continually re-transmits unacknowledged MSUs until an acknowledgement is received or the T7 timer expires, at which point the link is taken down.

**Note 1:** The default value for the T7 timer is 600 ms.

**Note 2:** Changing the T7 timer value on this screen will not change the T7 timer value for the provisioned timer index. If PCR is selected, the value in the T7 timer box is used for the excessive delay of acknowledgement. If PCR is not selected, the value for T7 in the timer index is used for the excessive delay of acknowledgement.

- ii Select a value between 1 and 50 (representing tenths of a second) in the **pcr-delay** box. This value represents the round trip propagation delay for the link in milliseconds.

The default value is 10, or 1000 ms.

- e Proceed to step [14](#).

**13** For MTP2 High Speed links, complete the following steps:

- a Enter a **port** value of 1 for mtp2hslinks.
- b Select a provisioned MTP link timer index from the **l2-timer-index** list.

The default index is the first available index.

**Note:** A system-id must be selected prior to selecting the l2-timer-index or a multiple timer list with the same index is displayed.

- c Select a provisioned MTP link SLT timer index from the **slt-timer-index** list.

The default index is the first available index.

- d Proceed to step [14](#).

**14** Click **Add**. A confirmation dialog box appears.

**15** Click **Yes** to confirm the change.

## Modifying Links

To edit links, perform the following steps:

### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to modify. Double click the link to open it in the administration panel and edit active fields as required.
- 3 Click **Modify** to save these link changes. A confirmation dialog box appears.
- 4 Click **Yes** to confirm the change.

## Deleting Links

To delete existing links, perform the following steps:

### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to delete. Double click the link to open it in the administration panel.
- 3 Click **Delete**. A confirmation dialog box appears.
- 4 Click **Yes** to confirm the change.

## Inhibiting and Uninhibited Links

Inhibit differs from deactivate because an inhibit command does not disrupt traffic. The system finds another link within the linkset before taking the inhibited link down.

To inhibit or uninhibited links, perform the following steps.

### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to Inhibit. Double click the link to open it in the administration panel.
- 3 Click **Uninhibit** to uninhibit the displayed link, or click **Inhibit** to inhibit the displayed link. A confirmation dialog box appears.



When you uninhibited or inhibit a link, several boxes are updated in the Link Status.

When you successfully uninhibit a link, the **local-inhibit-state** box changes to Uninhibited.

When you successfully inhibit a link, the **local-inhibit-state** box changes to Local Inhibit.

- 4 Click **Yes** to confirm the change.

## Activating and Deactivating Links

You can stop traffic on a link by changing its status to inactive. You can allow traffic on a link by changing its status to active.

To activate or deactivate links, perform the following steps

### *At the OAMP workstation*

- 1 Click **Configuration>mtp>link**.
- 2 Click the **Search** panel tab, click the Retrieve button (located in the command bar to the immediate left of the Help button) and locate the record you want to activate or deactivate. Double click the link to open it in the administration panel.
- 3 Click **Activate** to activate the displayed link, or click **Deactivate** to deactivate the displayed link. A confirmation dialog box appears

When you activate or deactivate a link, several boxes are updated in the Operational Data section of this window.

- 4 Click **Yes** to confirm the change.

## Understanding Link States

The information displayed in the l3-link-status, activation-state, remote-block-status, local-inhibit-state, remote-inhibit-state, congestion-level, discard-level and level-2-status report information on your links. The system updates all SS7 states once per second.

### **l3-link-status**

The l3-link-status box shows the availability of the link: available or unavailable

### **activation-state**

The activation-state box shows you if the link is active. Possible states are inactive, act-restoring, active, failed, suspended-t17, suspended-card-out-of-service, and initializing.

**remote-inhibit-status**

The remote-inhibit-status refers to links that are inhibited by the far-end node of this link. The remote-inhibit-status box displays the remote inhibit status: remote-inhibit or uninhibited.

**remote-block-state**

The local-block-state refers to links that are inhibited locally. The local-block-state box displays the local inhibit state: remote-blocked or unblocked.

**local-inhibit-state**

The local-inhibit-state refers to links that are inhibited by the near-end node of this link. The local-inhibit-state box displays the local inhibit state: local-inhibit or uninhibited.

**discard-level**

The discard-level ranges from 0 (lowest) through 3 (highest). All messages are assigned a discard priority level. Any messages with a priority level less than the currently displayed discard level are discarded.

**congestion-level**

Measurement of link congestion differs, depending on the protocol used by your system. If your system identity is ANSI-based, link congestion is measured in four levels: 0 (lowest) through 3 (highest). If your system identity is ITU 14-bit based, link congestion is measured in two levels: 0 (lowest) and 1 (highest).

The congestion levels provide a way for the USP to manage messages during times of elevated congestion. Each SS7 message is assigned a congestion priority level. Messages with high priority levels are more likely to be sent, even when congestion is high.

Any messages with a priority level lower than the currently displayed congestion level result in the following actions:

- The system generates a signaling network management (SNM) transfer control message (TFC) to notify the senders of the messages in the network of the congestion status.
- The system checks the discard level.

If the congestion level continues to remain above 0 for an extended period of time, you may need to add a link.

**level-2-status**

The level 2 status for a link appears in the level-2-status box. Possible states are idle, in-service, out-of-service, initial-alignment, aligned-not-ready, aligned-ready, processor-outage, not-aligned, proving, aligned, monitoring, local-processor-outage, remote-processor-outage, both-processor-outage, l2-congestion and unknown.



---

## Powering down the SAMF frame

---

### Purpose of this procedure

Use the following procedure to power down the SAMF frame. This involves locking all cards and the SAM21 shelf and powering down the Session Server unit and Policy Controller unit.

### When to use this procedure

Use this procedure when it is necessary to power down the SAMF frame.

### Prerequisites

None

### Action

#### Powering down the SAMF frame

##### *At the Session Server unit*

- 1 Perform procedure [Lock the SIP Gateway application on page 359](#) on the active Session Server unit.
- 2 Perform procedure [Suspend the SIP Gateway application on page 363](#) on the active Session Server unit.
- 3 Perform procedure [Halt \(shutdown\) a Session Server - Trunks unit on page 393](#) on the inactive Session Server unit.

**Note:** The state of the SIP Gateway application is saved when the unit is powered off. When the unit is powered up, the SIP Gateway application initializes in the same state in which it was powered down.

- 4 Perform procedure [Power-Off a Session Server - Trunks unit on page 399](#) on the inactive Session Server unit.
- 5 Perform procedure [Halt \(shutdown\) a Session Server - Trunks unit on page 393](#) on the active Session Server unit.

**Note:** The state of the SIP Gateway application is saved when the unit is powered off. When the unit is powered up, the SIP Gateway application initializes in the same state in which it was powered down.

- 6 Perform procedure [Power-Off a Session Server - Trunks unit on page 399](#) on the active Session Server unit.

**At the Policy Controller Unit**

- 7 Perform procedure [Halt \(shutdown\) a Policy Controller unit on page 579](#) on the inactive Policy Controller unit.
- 8 Perform procedure [Power-Off a Policy Controller unit on page 585](#) on the inactive Policy Controller unit.
- 9 Perform procedure [Halt \(shutdown\) a Policy Controller unit on page 579](#) on the active Policy Controller unit.
- 10 Perform procedure [Power-Off a Policy Controller unit on page 585](#) on the active Policy Controller unit.

**At the CS 2000 GWC Manager**

- 11 Lock all inactive GWC cards.  
Refer to [Lock a GWC card on page 407](#).
- 12 Lock all active GWC cards.  
Refer to [Lock a GWC card on page 407](#).

**At the CS 2000 SAM21 Manager**

- 13 Lock any inactive cards other than the SC cards.
- 14 Lock any active cards other than the SC cards.
- 15 Lock the inactive SC card.  
Refer to [Locking a SAM21 Shelf Controller on page 406](#).
- 16 Lock the active SC card.  
Refer to [Locking a SAM21 Shelf Controller on page 406](#).

**At the SAMF frame**

- 17 Power down the SAMF frame BIP breakers. At the top of the cabinet, turn off the breakers that supply power to the two SAM21 shelves and the Session Server (if equipped).
- 18 You have completed this procedure.

## Lock the SIP Gateway application

### Purpose of this procedure

Use the following procedure to change the administrative status of the SIP Gateway application to Locked.

### Limitations and restrictions

This procedure provides instructions for changing the service status of the SIP Gateway application software only. The NCGL operating status is not affected.



#### **CAUTION**

##### **Service interruption**

This is a service affecting procedure. Locking the SIP Gateway application releases all SIP calls in progress, regardless of call state, and causes an outage of all SIP media communications.

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

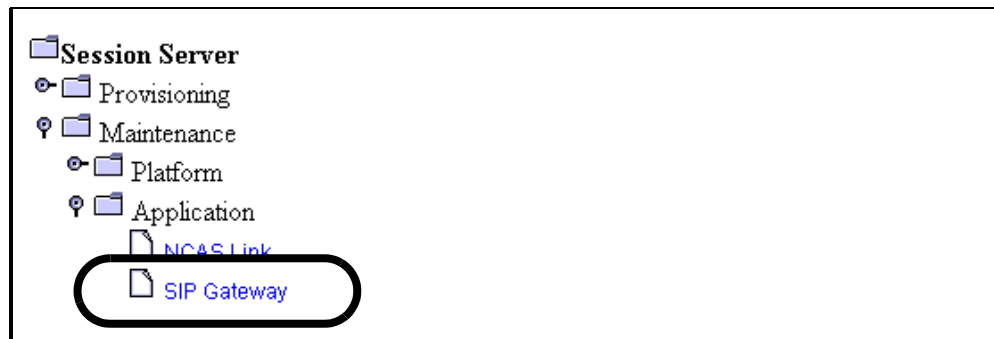
- 1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway.



3 In the SIP Gateway panel click the Lock button.

Unit Number	Activity State	Operational State
0	Active	Enabled
1	Inactive	Enabled

SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
UnLocked	Enabled	-	-

SIP Gateway Maintenance	
Administrative	Control
<div style="border: 2px solid red; border-radius: 15px; padding: 5px; display: inline-block;">Lock</div> UnLock Shut Down	Suspend UnSuspend

*The system responds:*

This action will release all existing SIP calls and will cause a SERVICE OUTAGE on this Session Server. There are x active calls. Do you wish to continue?

4 Click OK to confirm locking the SIP Gateway application.



- 5 Monitor the status of the SIP Gateway application and ensure the Administrative State changes to Locked.

SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Enabled	-	-

SIP Gateway Maintenance	
Administrative	Control
<input type="button" value="Lock"/> <input type="button" value="UnLock"/> <input type="button" value="Shut Down"/>	<input type="button" value="Suspend"/> <input type="button" value="UnSuspend"/>

**Note:** The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button. Otherwise, manually refresh the page by clicking on the Refresh button.

- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Suspend the SIP Gateway application

### Purpose of this procedure

Use the following procedure to temporarily take the SIP Gateway application out of service. This activity must be performed whenever selected SIP Gateway application provisioning changes are made and the application must be restarted for the changes to take effect.

**Note:** For more detailed information about SIP Gateway application services states and administrative functions, refer to “Interpreting SIP Gateway application states” in the *Session Server - Trunks Security and Administration*, NN10346-611.

### Limitations and restrictions

This procedure can only be performed when the SIP Gateway application is in the following service states:

- the Operational State is Enabled
- the Administrative State is Locked

### Prerequisites

The SIP Gateway application must previously have been locked. If it is not locked or you are uncertain of the state of the application, refer to procedure [Lock the SIP Gateway application on page 359](#).

### Action

#### **At the CS 2000 Session Server Manager or IEMS client**

- 1** Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2** Select Session Server > Maintenance > Application > SIP Gateway from the left side menu:



3 In the SIP Gateway panel click Suspend.

Session Server Status - Connected to Unit #0		
Unit Number	Activity State	Operational State
0	Active	Enabled
1	Inactive	Enabled

SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Enabled	-	-

SIP Gateway Maintenance	
Administrative	Control
<p>Lock</p> <p>UnLock</p> <p>Shut Down</p>	<p>Suspend</p> <p>UnSuspend</p>

- 4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box:
- the Operational State changes to Disabled
  - the Control Status changes to Suspended

SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Disabled	-	Suspended

SIP Gateway Maintenance	
Administrative	Control
<input type="button" value="Lock"/>	<input type="button" value="Suspend"/>
<input type="button" value="UnLock"/>	<input type="button" value="UnSuspend"/>
<input type="button" value="Shut Down"/>	

- 5 If applicable, restart the SIP Gateway application by executing procedures [Unsuspend the SIP Gateway application on page 367](#) and [Unlock the SIP Gateway application on page 371](#), in the order shown.
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Unsuspend the SIP Gateway application

### Purpose of this procedure

Use the following procedure to bring the SIP Gateway application back into service without restarting callP activity.

**Note:** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section “Interpreting SIP Gateway application states” in *Session Server - Trunks Security and Administration*, NN10346-611.

### Limitations and restrictions

This procedure can only be performed when the SIP Gateway application is in the following service states:

- the Operational State is Disabled
- the Administrative State is Locked
- the Control Status is Suspended

### Prerequisites

The SIP Gateway application must previously have been suspended. If it is not suspended or you are uncertain of the state of the application, refer to procedure [Suspend the SIP Gateway application on page 363](#).

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

- 1** Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

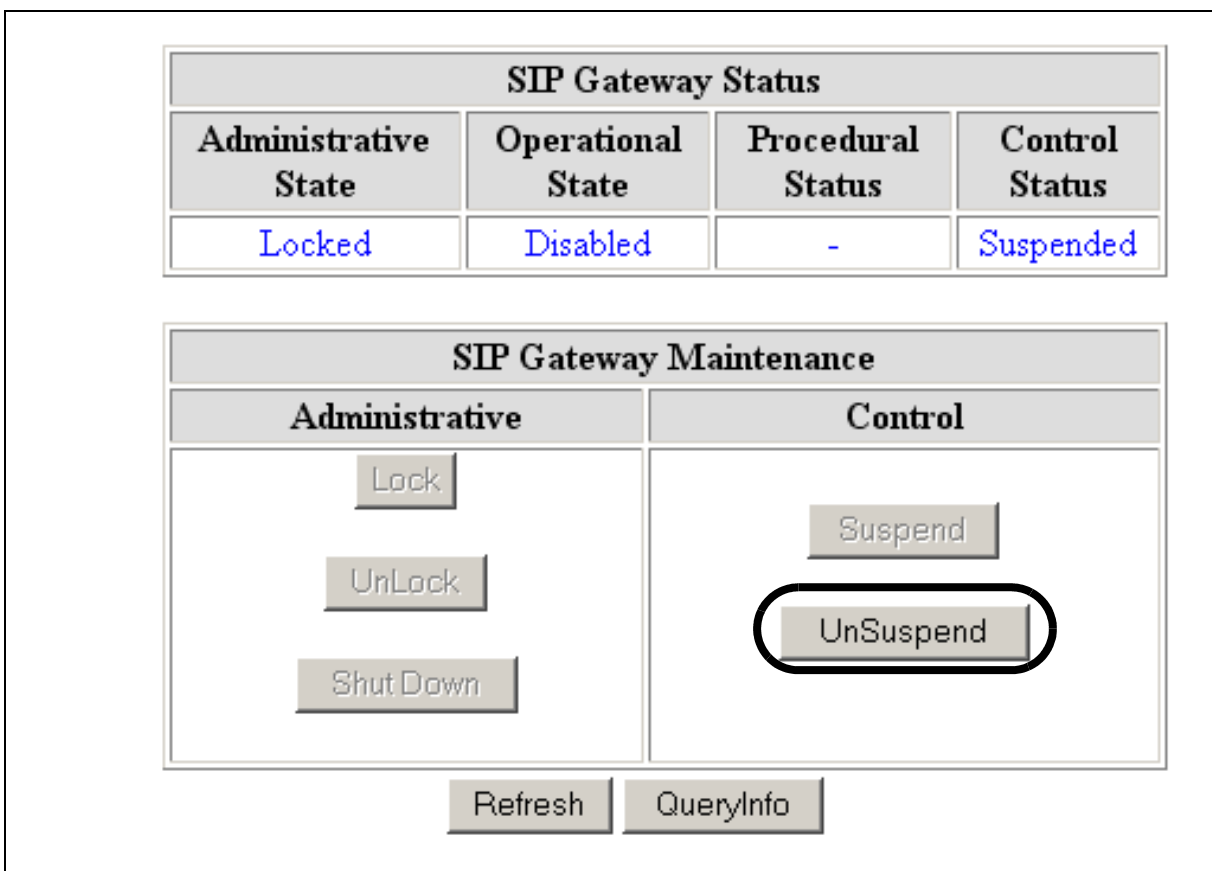
Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2** Select **Session Server > Maintenance > Application > SIP Gateway** from the left side menu:



3 In the SIP Gateway panel click Unsuspend.



4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box:

- the Operational State changes to Enabled
- the Control status changes to -



Session Server Status - Connected to Unit #0			
Unit Number	Activity State	Operational State	
0	Active	Enabled	
1	Inactive	Enabled	
SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Enabled	-	-
SIP Gateway Maintenance			
Administrative		Control	
<input type="button" value="Lock"/>  <input type="button" value="UnLock"/>  <input type="button" value="Shut Down"/>		<input type="button" value="Suspend"/>  <input type="button" value="UnSuspend"/>	

- 5 If necessary, bring the SIP Gateway application back into service by executing procedure [Unlock the SIP Gateway application on page 371](#).
- 6 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Unlock the SIP Gateway application

### Purpose of this procedure

Use the following procedure to change the administrative status of the SIP Gateway application to Unlocked, bringing the application into service and enabling call processing to begin.

**Note:** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section of *Session Server - Trunks Security and Administration*, NN10346-611.

### Limitations and restrictions

This procedure provides instructions for changing the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure [View the operational status of the NCGL platform on page 375](#).

### Prerequisites

The active unit must be in a locked Administrative state. If it is not locked or you are uncertain of the state of the application, refer to procedure [Lock the SIP Gateway application on page 359](#).

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select **Session Server > Maintenance > Application > SIP Gateway** from the left side menu:



3 In the SIP Gateway panel click Unlock.

Session Server Status - Connected to Unit #0		
Unit Number	Activity State	Operational State
0	Active	Enabled
1	Inactive	Enabled

SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
Locked	Enabled	-	-

SIP Gateway Maintenance	
Administrative	Control
<div style="text-align: center;"> <input type="button" value="Lock"/>  <input type="button" value="UnLock"/>  <input type="button" value="Shut Down"/> </div>	<div style="text-align: center;"> <input type="button" value="Suspend"/>  <input type="button" value="UnSuspend"/> </div>

- 4 Monitor the status of the SIP Gateway application in the SIP Gateway Status box and ensure the Administrative State changes to Unlocked.

Unit Number	Activity State	Operational State	
0	Active	Enabled	
1	Inactive	Enabled	

SIP Gateway Status			
Administrative State	Operational State	Procedural Status	Control Status
UnLocked	Enabled	-	-

SIP Gateway Maintenance	
Administrative	Control
<input type="button" value="Lock"/>  <input type="button" value="UnLock"/>  <input type="button" value="Shut Down"/>	<input type="button" value="Suspend"/>  <input type="button" value="UnSuspend"/>

**Note:** The status panel is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button. Otherwise, manually refresh the page by clicking on the Refresh button.

- 5 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



---

## View the operational status of the NCGL platform

---

### Purpose of this procedure

Use the following procedure to view the service status of the hardware and NCGL operating system using the CS 2000 NCGL Platform Manager. This procedure can be used as a standalone task or as part of a high-level activity.

### Limitations and restrictions

This procedure provides instructions for determining the service status of the Session Server - Trunks NCGL platform only. For instructions on determining the status of the SIP Gateway application, refer to procedure "View the operational status of the SIP Gateway application" in *Session Server - Trunks Configuration Management*, NN10338-511.

Although some activities described in this procedure can be accomplished using the CS 2000 Session Server Manager, they are described instead using the more complete CS 2000 NCGL Platform Manager.

This procedure does not describe how to view customer logs or alarms. For detailed instructions on viewing customer logs or alarms, refer to procedures in *Session Server - Trunks Fault Management*, NN10332-911.

### Prerequisites

There are no prerequisites for using this procedure.

### Action

#### ***At the CS 2000 NCGL Platform Manager or IEMS client***

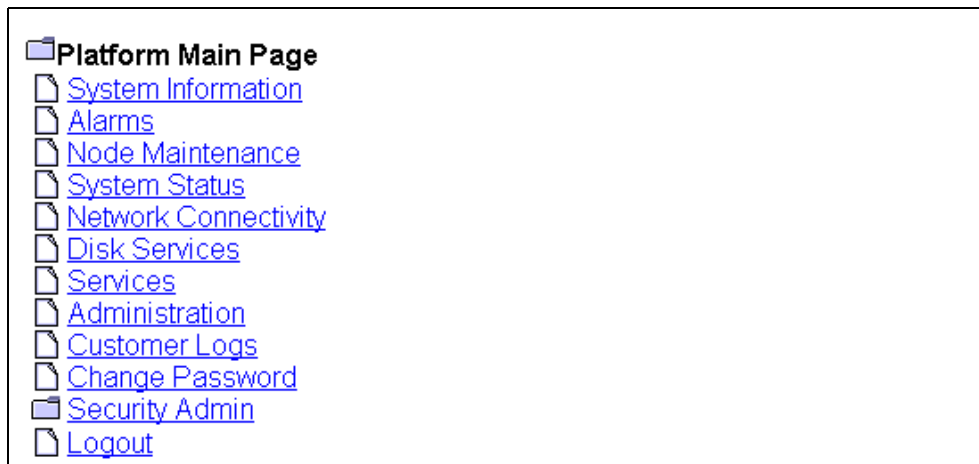
- 1 Select Succession Communication Server 2000 NCGL Platform Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

*The Platform Main Page menu is displayed.*



**2** Use the following table to determine your next step:

If	Do
you want to review the version of the platform software load, boot statistics and platform IP address	Click the System Information link and go to <a href="#">step 3</a> .
you want to review existing platform alarms	Go to <a href="#">step 17</a> and go to procedure "View Session Server - Trunks alarms" in Session Server - Trunks Fault Management, NN10332-911.
you want to review node maintenance status	Click the Node Maintenance link and go to <a href="#">step 5</a> .
you want to review the status of system processes, CPU load and memory or related alarm thresholds	Click the System Status link and go to <a href="#">step 7</a> .
you want to review the connectivity status of the network links. To perform link management activities, refer to <i>Session Server - Trunks Security and Administration</i> , NN10346-611.	Click the Network Connectivity link and go to <a href="#">step 9</a> .
you want to review storage related information including array status, disk capacity and disk alarm thresholds	Click the Disk Services link and go to <a href="#">step 10</a> .
you want to review details about platform services including the network time protocol servers	Click the Services link and go to <a href="#">step 12</a> .
you want to review platform version information only	Click the Administration link and go to <a href="#">step 14</a> .
you want to review customer logs	Go to <a href="#">step 17</a> and refer to <i>Session Server - Trunks Fault Management</i> , NN10332-911.
you want to change root passwords	Go to <a href="#">step 17</a> and refer to <i>Session Server - Trunks Security and Administration</i> , NN10346-611.



---

If	Do
you want to view TLS security information or manage security certificates	Go to <a href="#">step 17</a> and refer to <i>Session Server - Trunks Configuration Management</i> , NN10338-511 to review TLS security settings.
you are finished reviewing information and want to log out from the GUI	<a href="#">step 16</a> .

---

- 3 Review the system information page and use the following table to review the description of the various fields of the Platform (System) Information page:

**Note:** The Platform (System) Information panel does not update automatically. Click the System Information link again to update it.

Unit	Activity	Jam	State	Connectivity	Host Name	Last Update Time
1	Active	no	.	.	rtpsngss1unit1	08:55:05

The Platform Information panel does not update automatically!  
Datestamp of last update: Wednesday April 06th 2005 08:55:08 AM EDT

Platform Information	
Date:	Wednesday April 06th 2005 08:55:08 AM EDT
Time since last reboot:	12 days, 20 hours, 23 minutes, 43 seconds
System Power-On Time:	1 years 29 days 6 hours
System booted from:	Hard disk drive
Last restart cause:	Last restart due to soft reset
Last power event cause:	Last power down caused by loss of power feed.
Current version:	7.09.1.0.0502281015
Platform IP Address:	172.17.40.216
Platform EM Client IP Address:	47.142.89.70
Server Location:	lab5
Host Name:	rtpsngss1unit1

Field	Description
Unit	unit number in the node that you are logged into
Activity	activity of the unit (either active or standby)
Jam	indicates if the inactive unit is Jammed. The value is YES only if logged in to the inactive unit. From the active unit, the status is NO, but a JInact alarm indicates the inactive is Jammed.
State	indicates if the node is operating in a duplex (fault-tolerant) mode or a simplex mode (the standby unit is off-line)
Connectivity	state of the network links on the node
Host Name	name of the unit (not node)

Field	Description
Date	system date as maintained by the network time protocol (NTP) server
Time since last reboot:	amount of time that has elapsed since the unit was last rebooted for any reason
System Power-On Time:	recorded system time that the unit has been powered up
System booted from:	indicates whether the unit is currently booted from the hard drive or DVD-ROM drive
Last restart cause:	indicates any event that forced a platform reboot (manual or system generated)
Last power event cause:	indicates any event that affected the power supply subsystem of the unit chassis
Current version:	installed version of the NCGL platform software
Platform IP Address:	unit IP address
Platform EM Client IP Address:	IP address of the client web browser. When a web proxy is used, the IP address of the machine performing the proxy is displayed
Server Location:	physical location of the unit
Host Name:	name of the unit

- 4 When you have completed reviewing System Information page, return to [step 2](#).

- 5 Review the Node Maintenance page and use the following table to review the description of the various fields of the Node Maintenance page:

The Node Maintenance panel updates every 45 seconds  
Datestamp of last update: Wednesday April 06th 2005 09:19:40 AM EDT

Unit 0		
Operation State	Activity	Jam State
Enabled	Inactive	no

Unit 1		
Operation State	Activity	Jam State
Enabled	Active	no

Maintenance Actions	
<input type="button" value="SWACT"/> <input type="checkbox"/> Force	<input type="button" value="Jam"/> <input type="checkbox"/> Force

**Note:** The Node Maintenance panel is refreshed every 45 seconds.

Field	Description
Operation State	indicates the operational state of the NCGL software
Activity	indicates the activity state of the platform software
Jam State	indicates if the inactive unit is Jammed
Maintenance Actions (active unit only)	maintenance panel for performing SwAct and to Jam. Refer to <i>Session Server - Trunks Security and Administration</i> , NN10346-611, for procedures on performing a SwAct or Jam.

- 6 When you have completed reviewing the Node Maintenance page, return to [step 2](#).

- 7 Review the System Status page and use the following table to review the descriptions of the various fields of the System Status page.

Chassis Information					
Self Test			Chassis Subsystems		
Self tests passed.			Chassis subsystems OK.		

CPU Load					
1 min. load average	5 mins. load average	15 mins. load average	Minor alarm threshold 1 min.	Major alarm threshold 1 min.	Critical alarm threshold 1 min.
0.10	0.05	0.01	10.00	20.00	40.00

CPU Utilization					
5 mins. Utilization average	20 mins. Utilization average	30 mins. Utilization average	Minor alarm threshold 5 min.	Major alarm threshold 20 min.	Critical alarm threshold 30 min.
2.20	1.99	1.86	95.00%	99.00%	99.00%

Process Information				
Number of processes	Number of zombie process(es)	Zombie		
		Minor alarm threshold value	Major alarm threshold value	Critical alarm threshold value
192	1	5	10	15

Memory Information					
Total memory (MB)	Free memory (MB)	Available memory (MB)	Minor alarm threshold value (MB)	Major alarm threshold value (MB)	Critical alarm threshold value (MB)
3,790.29	2,945.21	3,294.78	500.00	250.00	100.00

**Note:** The Chassis Information panel is not automatically refreshed.

Field	Description
Chassis information: Self Test	status of the self test performed on the platform at boot up
Chassis information: Chassis Subsystems	status of the platform hardware subsystems including the memory, CPU, all drives, network connection, power supplies, cooling and other I/O connections
CPU Information: load average	indicates the 1, 5 and 15 minute load averages for the CPU utilization
CPU information: load average threshold values	indicates the 1 minute CPU load average utilization threshold value. When the set threshold value is exceeded, the appropriate minor, major or critical alarm is raised.
Chassis Utilization: Utilization average	indicates the 5, 20 and 30 minute CPU utilization average. When the threshold value is exceeded, an alarm is raised.
Chassis Utilization: alarm threshold values	indicates the 5, 20 and 30 minute CPU utilization average threshold value. When the set threshold value is exceeded, an alarm is raised.
Process Information: Number of Processes	total number of processes (non-threaded) that are running on the Session Server - Trunks Platform
Process Information: Number of zombie processes	number of defunct or terminated NCGL zombie processes  <b>Note:</b> A zombie process is a process that has terminated either because it has been killed by a signal or because it has called an exit() and whose parent process has not yet received notification of its termination. A zombie process exists solely as a process table entry and consumes no other resources.
Process Information-zombie: minor alarm threshold value	maximum number of zombie processes allowed to be run by the CPU before a minor alarm is raised indicating that the set threshold has been exceeded

Field	Description
Process Information-zombie: major alarm threshold value	maximum number of zombie processes allowed to be run by the CPU before a major alarm is raised indicating that the set threshold has been exceeded
Process Information-zombie: critical alarm threshold value	maximum number of zombie processes allowed to be run by the CPU before a critical alarm is raised indicating that the set threshold has been exceeded
Memory Information: Total Memory (MB)	total amount of RAM installed on the motherboard of each Session Server - Trunks unit. Both units must have the same amount.
Memory Information: Free Memory (MB)	amount of memory available unallocated for use
Memory Information: Available memory (MB)	amount of memory available for programs
Memory Information: minor alarm threshold value	indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a minor alarm is raised
Memory Information: major alarm threshold value	indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a major alarm is raised
Memory Information: critical alarm threshold value	indicates the threshold amount of available memory (in Mbytes) that the system must drop below before a critical alarm is raised

- 8 When you have completed reviewing the System Status, return to [step 2](#).
- 9 Review the Network Connectivity page and use the following table to review the description of the various fields of the Network Connectivity page:
 

**Note:** The Network Connectivity panel is refreshed every 45 seconds.

Unit 0 Links				
Unit IP	Inactive IP	Port 0 IP	Port 1 IP	PTP IP
172.17.40.211	172.17.40.215	172.17.40.209	172.17.40.210	192.168.1.1
Links	Status	Activity		
Link 0	.	Active		
Link 1	.	Inactive		
PTP Links	.			

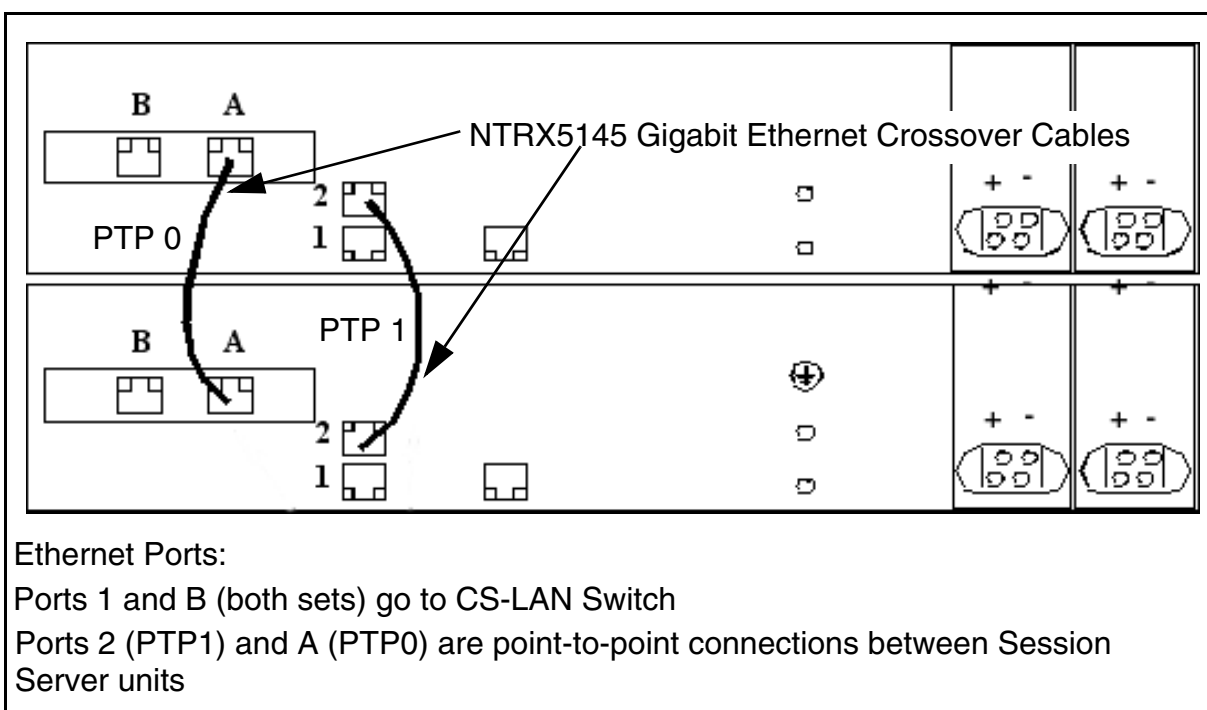
Unit 1 Links				
Unit IP	Active IP	Port 0 IP	Port 1 IP	PTP IP
172.17.40.214	172.17.40.216	172.17.40.212	172.17.40.213	192.168.1.2
Links	Status	Activity	Maintenance	
Link 0	.	Active	Lock 0	Swlink
Link 1	.	Inactive	Lock 1	
PTP Links	.			

Field	Description
Unit 0,1 Links	indicates which Ethernet IP links are installed on the units (each unit has two links)
Unit 0,1 Status	status of the Ethernet links
Unit 0,1 Activity	activity status of the Ethernet links, either active or inactive
Unit 0,1 Maintenance	indicates the maintenance actions that can be performed on the Ethernet links, either Lock, Unlock or Swlink
Unit 0,1 PTP Links status	status of the PTP links between both units in the node
Unit IP	network IP address of the Session Server - Trunks unit
Active IP	IP address of the local (active) Session Server - Trunks unit



Field	Description
Inactive IP	IP address of the mate (inactive) Session Server - Trunks unit
Port 0 IP	IP address of the active or inactive Ethernet port 0
Port 1 IP	IP address of the active or inactive Ethernet port 1
PTP IP	IP address of the active or inactive PTP link

### Crossover and LAN Ethernet cable connections for Session Server - Trunks units



- Review the Disk Services page and use the following table to review the description of the various fields of the Disk Storage page:

**Note 1:** The Disk Services panel does not update automatically. Click the Disk Services link again to update it.

**Note 2:** To create and remove file systems, refer to applicable procedures in *Session Server - Trunks Configuration Management*, NN10338-511.

RAID Array Status										
Name	Size (GB)	State	Disk 0	Disk 1	Status					
/boot	0.10	.	.	.	Array is operating normally					
ntvg	68.26	.	.	.	Array is operating normally					
Disk Maintenance										
Disk Number	Disk Size (GB)	Disk State	Disk Action							
0	68.37	.	Remove							
1	68.37	.	Remove							
Filesystem Information										
Monitored	Filesystem Name	Test Results	Total Space (MB)	Total Space Used (MB)	Total Space Used (%)	Total Space Available (MB)	Total Space Available (%)	Minor Alarm Threshold (%)	Major Alarm Threshold (%)	Critical Alarm Threshold (%)
	/	.	61.47	58.29	100.00	0.00	0.00	85.00	90.00	95.00
No	/boot	.	98.65	19.08	21.00	74.48	79.00	-	-	-
Yes	/opt/base	.	699.31	0.46	1.00	698.85	99.00	85.00	90.00	95.00
No	/opt/apps	.	507.31	314.31	62.00	193.00	38.00	-	-	-
Yes	/tmp	.	123.31	0.31	1.00	123.00	99.00	85.00	90.00	95.00
Yes	/var/log	.	507.31	9.61	2.00	497.71	98.00	85.00	90.00	95.00
No	/opt/swd	.	507.31	0.25	1.00	507.06	99.00	-	-	-
No	/opt/apps/webint	.	1,494.00	209.78	15.00	1,284.22	85.00	-	-	-
No	/opt/apps/database	.	10,006.00	48.19	1.00	9,957.81	99.00	-	-	-
No	/opt/apps/logs	.	507.31	206.34	41.00	300.98	59.00	-	-	-
No	/opt/apps/ngssbilling	.	10,006.00	2.50	1.00	10,003.50	99.00	-	-	-
Create/Remove Filesystem										
Create New Filesystem					Remove Filesystem					
Volume Group Information										
Volume Group Name	Volume Group Size (GB)	Total Space Allocated (GB)	Total Space Allocated (%)	Total Space Available (GB)	Total Space Available (%)					
ntvg	68.22	23.84	34.95	44.38	65.05					

Field	Description
RAID Array Status: Name	indicates the name of each RAID-1 array in the system
RAID Array Status: Size (GB)	indicates the size of the partition in gigabytes

Field	Description
RAID Array Status: State	Indicates a high level state for the array: <ul style="list-style-type: none"> <li>- “.”: indicates the array is functioning normally.</li> <li>- Missing: a disk was removed from the array.</li> <li>- Failed: a disk in the array has failed and needs to be replaced.</li> <li>- Rebuilding: the array is in the process of rebuilding to a fault-tolerant mode.</li> </ul>
RAID Array Status: Disk 0	service status of disk 0
RAID Array Status: Disk 1	service status of disk 1
RAID Array Status: Status	Indicates the status of the array. Values are: <ul style="list-style-type: none"> <li>- The array is operating normally</li> <li>- Missing</li> <li>- Failed</li> <li>- Rebuild</li> </ul>
Disk Maintenance: Disk Number	indicates the disk number in the array, 0 or 1
Disk Maintenance: Disk Size (GB)	total capacity of the disk drive in gigabytes
Disk Maintenance: Disk State	installation state of the disk
Disk Maintenance: Disk Action	indicates whether a hard disk can be inserted into the RAID array
Filesystem Information: Monitor	indicates the status of individual filesystems on the disk array
Filesystem Information: Filesystem Name	indicates the name of the filesystem on the disk array. Some filesystem names are reserved.
Filesystem Information: Test Results	indicates the results of any tests run on the filesystems. Tests are run approximately every 10 minutes to verify that all of the basic filesystem operations are working on each of the filesystems.
Filesystem Information: Total Space (MB)	total amount of disk space (in MB) allocated for this filesystem
Filesystem Information: Total Space Used (MB)	total amount of disk space (in MB) in use on this file system
Filesystem Information: Total Space Used (%)	total amount of disk space (in %) in use on this file system

Field	Description
Filesystem Information: Total Space Available (MB)	percentage of total disk space (in MB) free for use on this filesystem
Filesystem Information: Total Space Available (%)	amount of disk space (in %) available for use by platform processes and applications
Filesystem Information: Minor Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a minor alarm is raised indicating that the set threshold has been exceeded
Filesystem Information: Major Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a major alarm is raised indicating that the set threshold has been exceeded
Filesystem Information: Critical Alarm Threshold (%)	maximum amount of disk space (in %) that can be used before a critical alarm is raised indicating that the set threshold has been exceeded
Volume Group Information: Volume Group Name	name of the volume group in the array
Volume Group Information: Volume Group Size (GB)	total size of the volume group in the array
Volume Group Information: Total Space Allocated (GB)	amount of volume group space, in gigabytes, currently allocated to filesystems
Volume Group Information: Total Space Allocated (%)	amount of volume group space (in %) currently allocated to filesystems
Volume Group Information: Total Space Available (GB)	amount of unallocated volume group space, in gigabytes, available for filesystems
Volume Group Information: Total Space Available (%)	amount of unallocated volume group space (in %) available for filesystems

- 11 When you have completed reviewing the Disk Services page, return to [step 2](#).
- 12 Review the Services page and use the following table to review the description of the various fields of the Platform Services page:

**Note:** The Services panel does not update automatically. Click the Services link again to update it.

Network Services					
Number of Active Command Line Sessions			Number of Clients with Active Web Sessions		
1			1		

NTP Information					
Server 1	Server 2	Server 3	Total Number of Servers	Accessible Servers	Synchronized Servers
47.140.207.50 in sync	47.140.206.50 in sync	undefined	2	2	2

Field	Description
Network Services: Number of Active Command Line Sessions	number of command line interface (CLI) sessions (both remote and local) on the unit
Network Services: Number of Clients with Active Web Sessions	number of clients running one or more web GUI sessions
NTP Information: Server1 - Server 3	IP address of up to 3 Network Time Protocol (NTP) servers in the network, along with the status of the connection
NTP Information: Total Number of Servers	number of NTP servers registered with the CS-LAN network
NTP Information: Accessible Servers	number of NTP servers accessible to the Session Server - Trunks
NTP Information: Synchronized Servers	number of NTP servers to which the unit is synchronized

- 13 When you have completed reviewing Platform Services status, return to [step 2](#).
- 14 Review the Administration page and use the following table to review the description of the various fields of the Administration page:
 

**Note:** The Administration panel does not update automatically. Click the link again to update it.

Bootload Management	
Bootload	Maintenance
8.08.1.0.0502231439	Default Bootload
7.09.1.0.0502281015	<input type="button" value="Set default"/> <input type="button" value="Delete"/>
5.36.2.1.0411021023	<input type="button" value="Set default"/> <input type="button" value="Delete"/>

Software Upgrade				
Protocol	Login ID	Password	IP address	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Server Maintenance	
<b>Unit 0 - Inactive</b>	
<input type="button" value="RebootMate"/> <input type="checkbox"/> Force	<input type="button" value="HaltMate"/> <input type="checkbox"/> Force
<b>Unit 1 - Active</b>	
<input type="button" value="Reboot"/> <input type="checkbox"/> Force	<input type="button" value="Halt"/> <input type="checkbox"/> Force

Field	Description
Bootload Management: Bootload	load ID for the NCGL platform software load
Bootload Management: Maintenance	indicates whether the Bootload is the default. Can also allow choosing a new default bootload if there is more than one load available. Additional loads can come from maintenance releases.
Software Upgrade: Protocol	file transfer protocol or source location for the platform software upgrade: FTP, Anonymous FTP, HTTP, HTTPS, Local File, Local CDROM
Software Upgrade: Login ID	If a login ID is required to access the upgrade platform load from another server in the network, a login ID can be entered here.

Field	Description
Software Upgrade: Password	If a password is required to access the upgrade platform load from another server in the network, a password can be entered here.
Software Upgrade: IP Address	If it is required to access the upgrade platform load from another server in the network, an IP address can be entered here.
Software Upgrade: File	The target upgrade load path and filename is entered here.
Software Upgrade: Action Upgrade button	The Upgrade button initiates a platform NCGL upgrade.
Server Maintenance (active and inactive units)	used to execute the Reboot, Halt, Rebootmate, and Haltmate functions. These are service affecting commands.

**15** When you have completed reviewing the Administration page, return to [step 2](#), or continue with [step 16](#).

**16** If you want to logout from CS 2000 NCGL Platform Manager, click the Logout button.

*You are returned to the login page*



**17** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.





---

## Halt (shutdown) a Session Server - Trunks unit

---

### Purpose of this procedure

This procedure is used to perform a graceful shutdown a Session Server - Trunks platform NCGL operating system. Use this procedure only as part of a high-level activity such as part of a controlled shutdown activity or part of a software upgrade activity. Included at the end of this procedure is an alternate CLI method for halting a unit.

### Limitations and Restrictions

This procedure can only be performed from the active Session Server - Trunks unit.

This procedure does not cause the Session Server - Trunks unit to power-off.



#### CAUTION

This procedure halts all call processing activity and billing record generation on the affected unit, and prevents the Session Server - Trunks node from operating in a fault-tolerant mode. Ensure that the unit you are shutting down is not performing call processing activities.

### Prerequisites

Use procedure [View the operational status of the NCGL platform on page 375](#) to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

### Action

#### *At the Session Server GUI or IEMS client*

- 1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

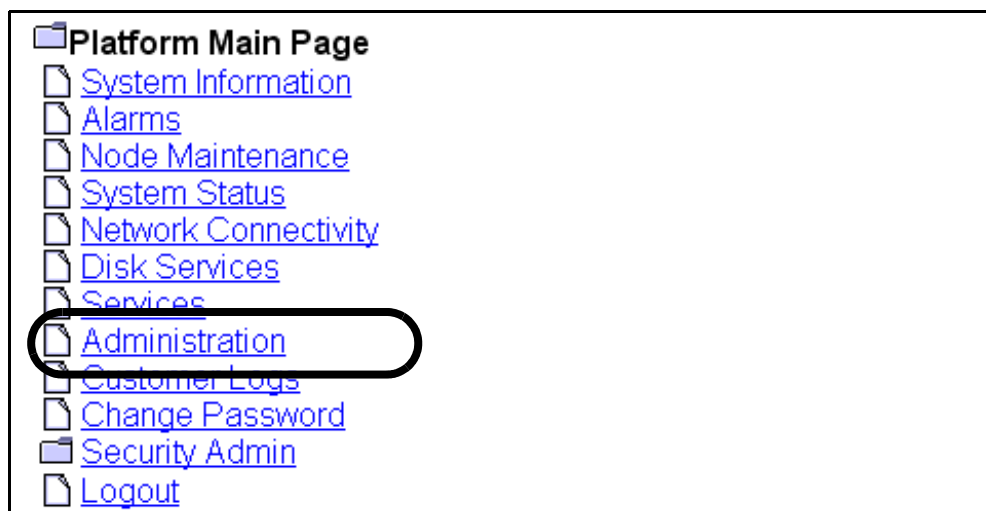
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

[Succession Communication Server 2000 NCGL Platform Manager](#)

[Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the **Administration** link.  
*The Administration page is displayed.*



- 3 Review the status of the unit you want to halt. If it is unavailable, the **Halt** or **HaltMate** buttons are not accessible.

Bootload Management				
Bootload		Maintenance		
5.20.1.0.0405122209		Default Bootload		

Software Upgrade				
Protocol	Login ID	Password	IP address	File
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Server Maintenance	
Unit 0 - Active	
<input type="button" value="Reboot"/> <input type="checkbox"/> Force	<input type="button" value="Halt"/> <input type="checkbox"/> Force
Unit 1 - Inactive	
<input type="button" value="RebootMate"/> <input type="checkbox"/> Force	<input type="button" value="HaltMate"/> <input type="checkbox"/> Force

- 4 Click the **Halt** or **HaltMate** button for the Session Server - Trunks unit you want to halt the NCGI operating system for.

**Note 1:** To override any pre-halt (shutdown) queries, click the **Force** check box before clicking the **Halt** or **HaltMate** button.

**Note 2:** In a system operating in fault-tolerant (duplex) mode, only the inactive unit can be shut down using **HaltMate** or a Forced **HaltMate**. A **Halt** or Forced **Halt** can only be performed if the system is operating in simplex mode.

5.20.1.0.0405122209			Default Bootload	
<b>Software Upgrade</b>				
<b>Protocol</b>	<b>Login ID</b>	<b>Password</b>	<b>IP address</b>	<b>File</b>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<b>Server Maintenance</b>				
<b>Unit 0 - Active</b>				
<input type="button" value="Reboot"/> <input type="checkbox"/> Force		<input type="button" value="Halt"/> <input type="checkbox"/> Force		
<b>Unit 1 - Inactive</b>				
<input type="button" value="RebootMate"/> <input type="checkbox"/> Force		<input type="button" value="HaltMate"/> <input type="checkbox"/> Force		

*The system responds:*

Are you sure you wish to halt?  
This may cause an extended service outage to any clients currently using this server. Click OK to confirm server halt or cancel to abort.

- 5 Click **OK** to confirm the halt operation.  
The NGCL and all call activity on the affected Session Server - Trunks begin the process of halting. This can take several minutes.
- 6 If you receive the following message, you must halt the unit using the Force option in step 4.  
Error: Command failed. Reason: Mate not available.
- 7 If applicable, complete procedure [Power-Off a Session Server - Trunks unit on page 399](#) to disconnect power from the unit.
- 8 This procedure is complete.

### To Haltmate or Force Haltmate?

The Haltmate action does not work if the SIP Gateway application database on the active unit is out of sync with the database on the inactive unit. Using the Haltmate command with the Force option overrides any pre-checks for this condition and forces a Halt of the inactive unit regardless of the sync state of the active unit database.

## Alternate command line interface (CLI) method

### ATTENTION

All prerequisites and restrictions shown on page [393](#) apply to using this procedure.

#### *At Session Server CLI or IEMS client*

- 1 Log onto the active Session Server unit CLI and change to the root user.
- 2 Shutdown the selected Session Server - Trunks unit by typing  
**# mtccli haltmate (to shutdown the inactive unit)**  
or  
**# mtccli halt (to shutdown the active unit operating in simplex mode)**  
and pressing the **Enter** key.
- 3 If applicable, complete procedure [Power-Off a Session Server - Trunks unit on page 399](#) to disconnect power from the unit.
- 4 You have completed this procedure.



---

## Power-Off a Session Server - Trunks unit

---

### Purpose of this procedure

This is used to power off a Session Server - Trunks unit.

This procedure may be used as a standalone task or as part of a higher level activity such as a part of a controlled shutdown activity or part of a software upgrade activity.

### Limitations and restrictions



#### CAUTION

This is a service affecting procedure. Powering off a Session Server - Trunks unit prevents the node from operating in a fault-tolerant manner. Ensure that the unit you are powering off is not the active unit. Failure to do so may result in loss of call processing.

### Prerequisites

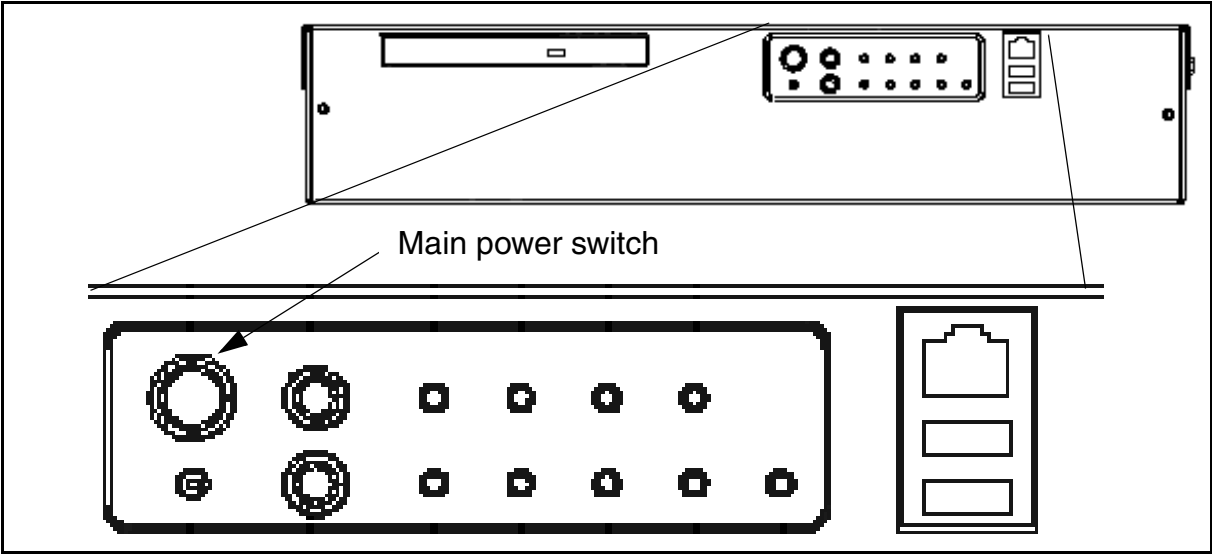
Refer to procedure [View the operational status of the NCGL platform on page 375](#) to verify that the unit to be shut down is not active.

Refer to the Session Server - Trunks Fault Management NTP, NN10332-911, for information about the high-level activity *Perform a controlled shutdown of a Session Server - Trunks node*.

### Action

#### ***At the front panel of the Session Server - Trunks unit.***

- 1 Complete procedure [Halt \(shutdown\) a Session Server - Trunks unit](#) before powering off the unit.
- 2 Once the operating system has been halted, disconnect the power to the unit using the main power switch located on the front panel.



3 The procedure is complete.



---

## Powering down the Call Control Frame

---

### Purpose of this procedure

Use the following procedure to power down the Call Control Frame (CCF).

Powering down the CCF powers down the Session Server, the SAM21 hardware cards and the STORM disk array or SAM-XTS units, in turn.

### When to use this procedure

Use this procedure when it is necessary to power down the CCF.

### Prerequisites

None

### Action

#### Powering down the Call Control Frame

##### *At the Session Server unit*

- 1 Perform procedure [Lock the SIP Gateway application on page 359](#) on the active Session Server unit.
- 2 Perform procedure [Suspend the SIP Gateway application on page 363](#) on the active Session Server unit.
- 3 Perform procedure [Halt \(shutdown\) a Session Server - Trunks unit on page 393](#) on the inactive Session Server unit.  
**Note:** The state of the SIP Gateway application is saved when the unit is powered off. When the unit is powered up, the SIP Gateway application initializes in the same state in which it was powered down.
- 4 Perform procedure [Power-Off a Session Server - Trunks unit on page 399](#) on the inactive Session Server unit.
- 5 Perform procedure [Halt \(shutdown\) a Session Server - Trunks unit on page 393](#) on the active Session Server unit.  
**Note:** The state of the SIP Gateway application is saved when the unit is powered off. When the unit is powered up, the SIP Gateway application initializes in the same state in which it was powered down.
- 6 Perform procedure [Power-Off a Session Server - Trunks unit on page 399](#) on the active Session Server unit.

**At the CS 2000 GWC Manager**

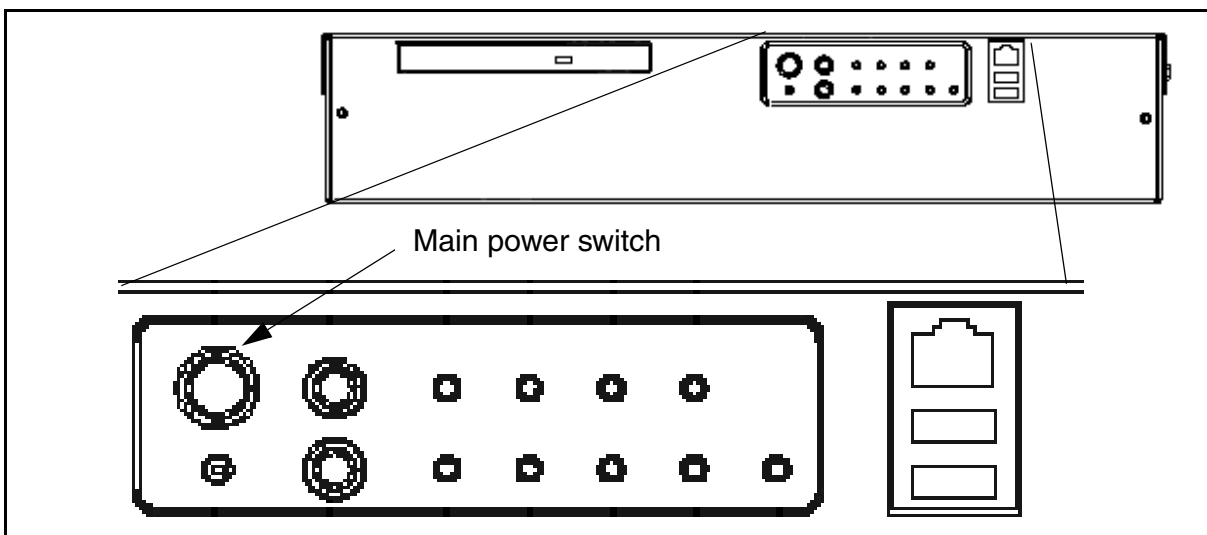
- 7 Lock all inactive GWC cards.  
Refer to [Lock a GWC card on page 407](#).
- 8 Lock all active GWC cards.  
Refer to [Lock a GWC card on page 407](#).

**At the CS 2000 SAM21 Manager**

- 9 Lock the inactive USP-lite card.
- 10 Lock the active USP-lite card.
- 11 Lock the inactive Compact Call Agent (CCA) card.  
Refer to [Locking the Call Agent on page 411](#).
- 12 Lock the active CCA card.  
Refer to [Locking the Call Agent on page 411](#).

**At the front panel of the STORM SAM-XTS units**

- 13 If your CCF is equipped with SAM-XTS units, disconnect the power to each unit using the main power switch located on the front panel.

**At the CCF**

- 14 Power down the CCF BIP breakers. At the top of the cabinet, turn off the breakers that supply power to the Session Server, the two SAM21 shelves, and the Storm SAM-XTS units or Storm Disk Array.

**15** You have completed this procedure.





## SAM21 Shelf Controller Security and Administration

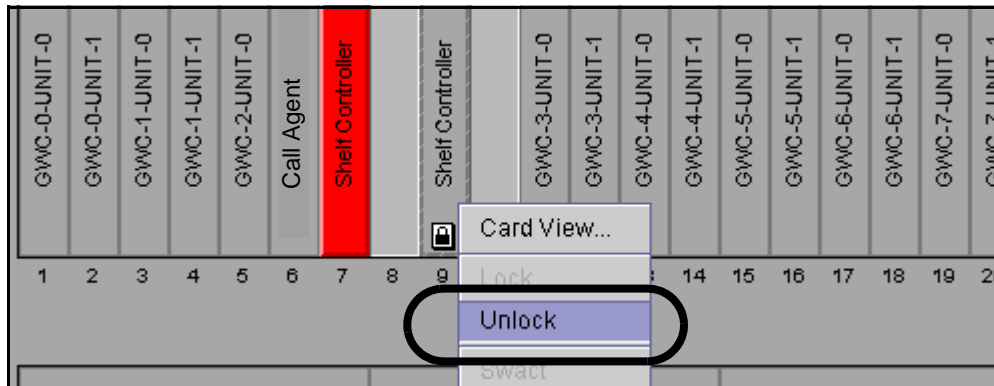
### Device administration

Administration of the SAM21 Shelf Controllers is done through the CS 2000 SAM21 Manager client.

#### Unlocking a SAM21 Shelf Controller

##### *At the CS 2000 SAM21 Manager client workstation*

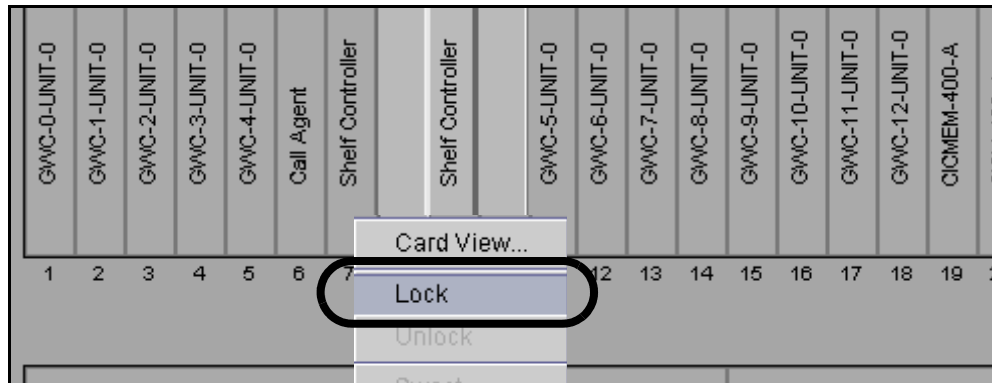
- 1 From the Shelf View, right click on the SAM21 Shelf Controller and select Unlock from the context menu.



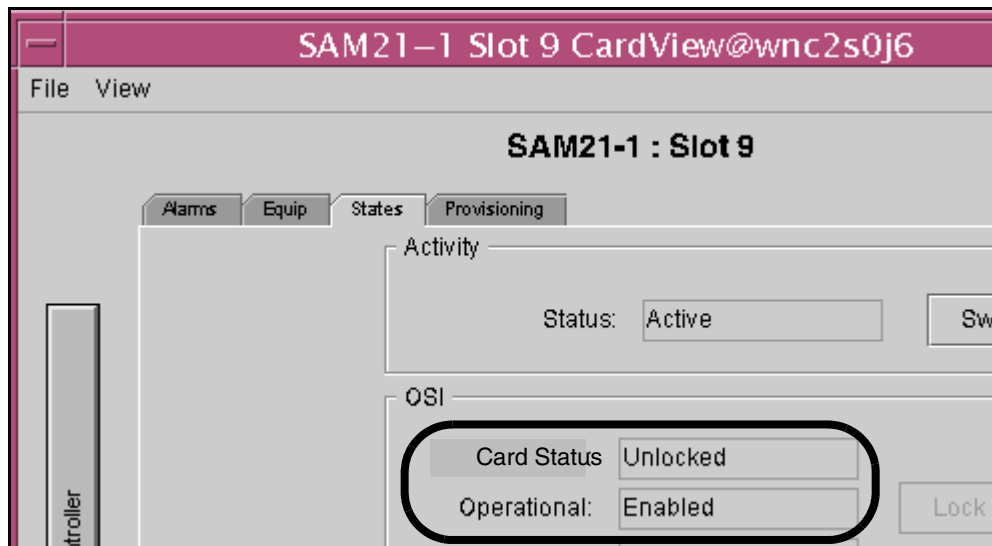
## Locking a SAM21 Shelf Controller

### *At the CS 2000 SAM21 Manager client workstation*

- 1 From the Shelf View, right click on the SAM21 Shelf Controller and select Lock from the context menu.



**Note:** Only lock a circuit pack that is in service. If a SAM21 Shelf Controller is unlocked and then relocked before the SAM21 Shelf Controller boots, flash memory can be corrupted and require a replacement SAM21 Shelf Controller. Check that a SAM21 Shelf Controller is Unlocked and Enabled from the Status tab of the Card View window.



---

## Lock a GWC card

---

### Purpose of this procedure

This procedure locks a single GWC card, stopping the services, applications, and platform software running on the GWC card.

### When to use this procedure

Use this procedure:

- when you are removing the card from service
- along with procedure [Unlock a GWC card on page 551](#) to reboot a GWC and force a software download
- as part of fault clearing activity to determine if a problem is temporary or persistent
- when you have applied or removed a patch to the GWC software using the Network Patch Manager (NPM) and have created a new GWC software image on the CS 2000 Core Manager.
- when you are removing a GWC node from the CS 2000 GWC Manager database

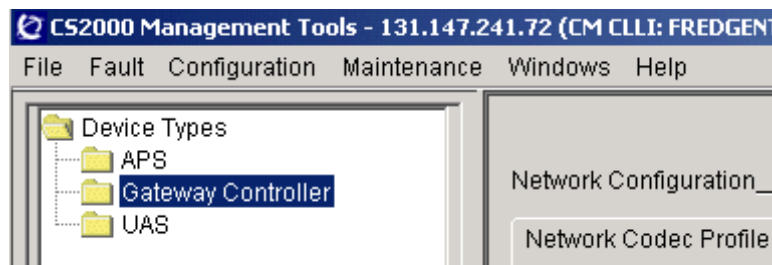
### Prerequisites

Once services on a standby card have been disabled, you can proceed with locking the card.

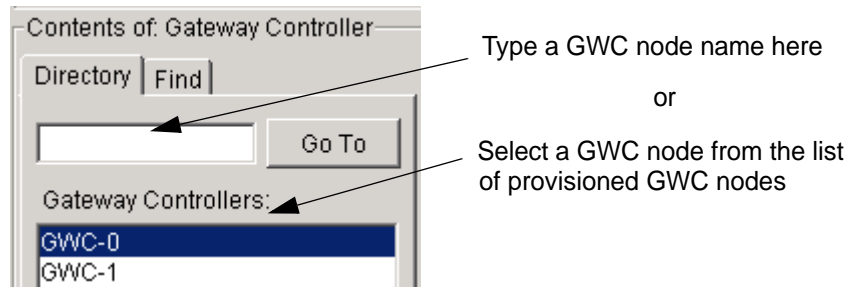
### Action

#### ***At the CS 2000 GWC Manager client***

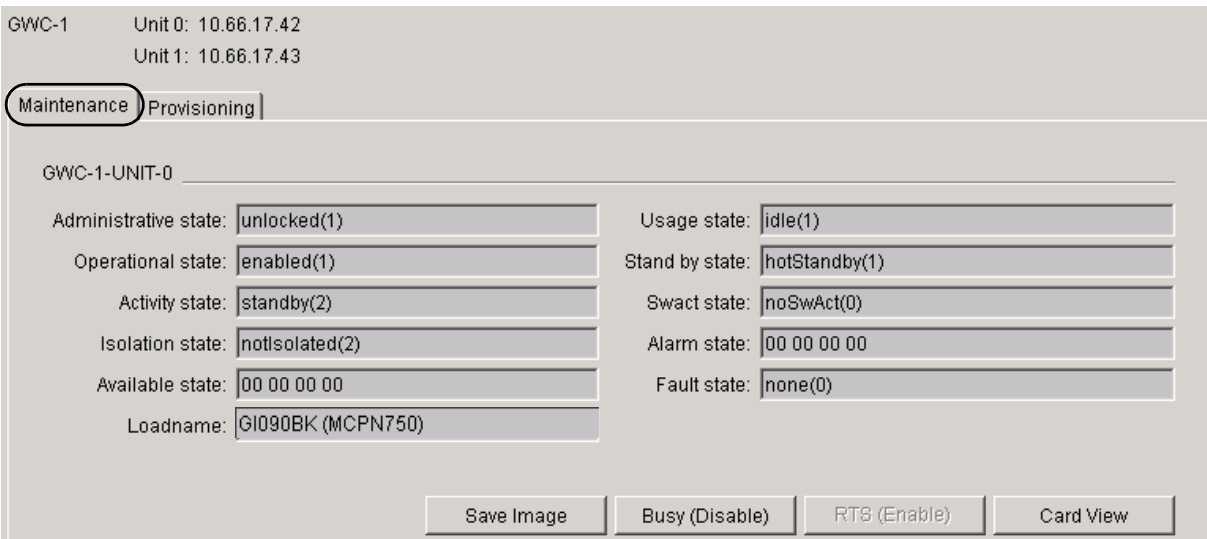
- 1 At the CS 2000 Management Tools window, click the Gateway Controller folder from the Device Types directory tree in the far left frame.



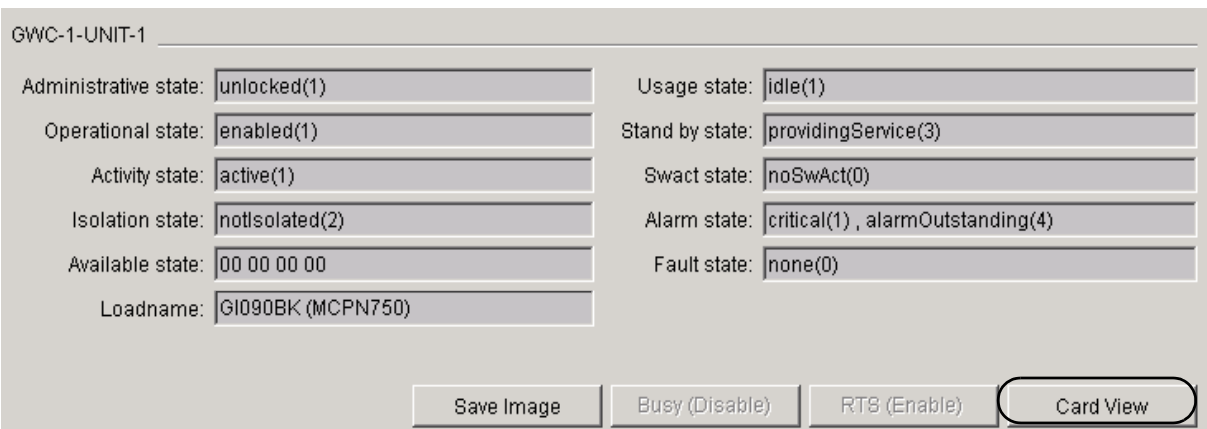
- 2 From the *Contents of: GatewayController* frame, select the GWC node that contains the card you want to lock.



- 3 Select the **Maintenance** tab to display maintenance information about the node.



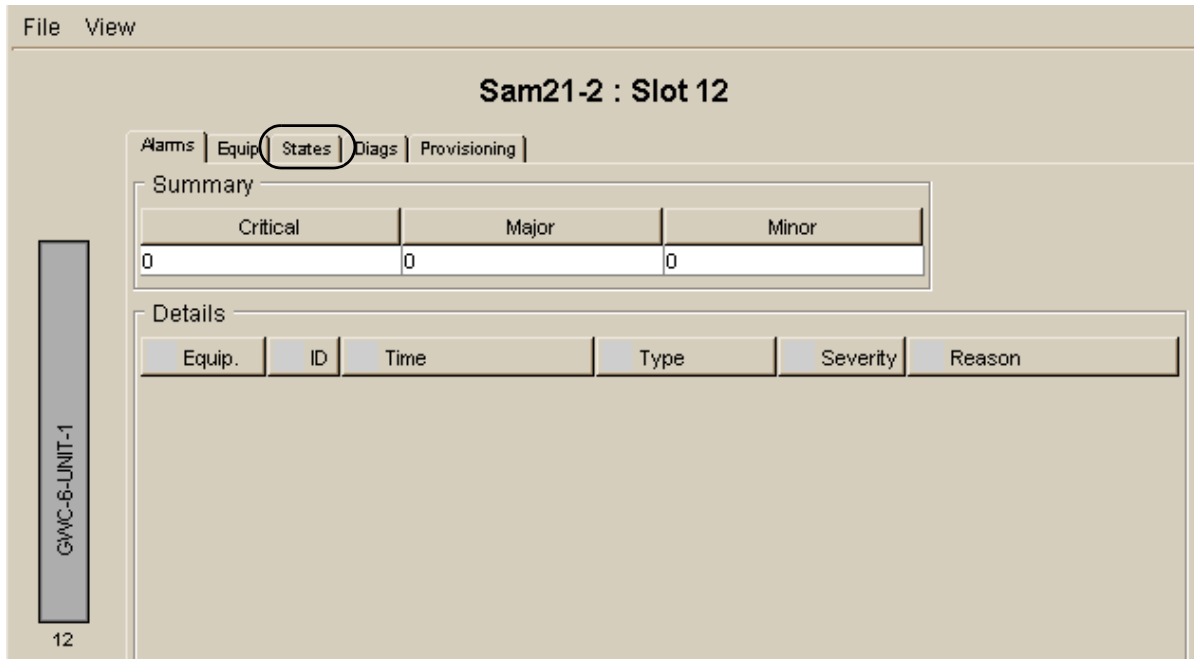
- 4 Click the **Card View** button for the card you want to lock.



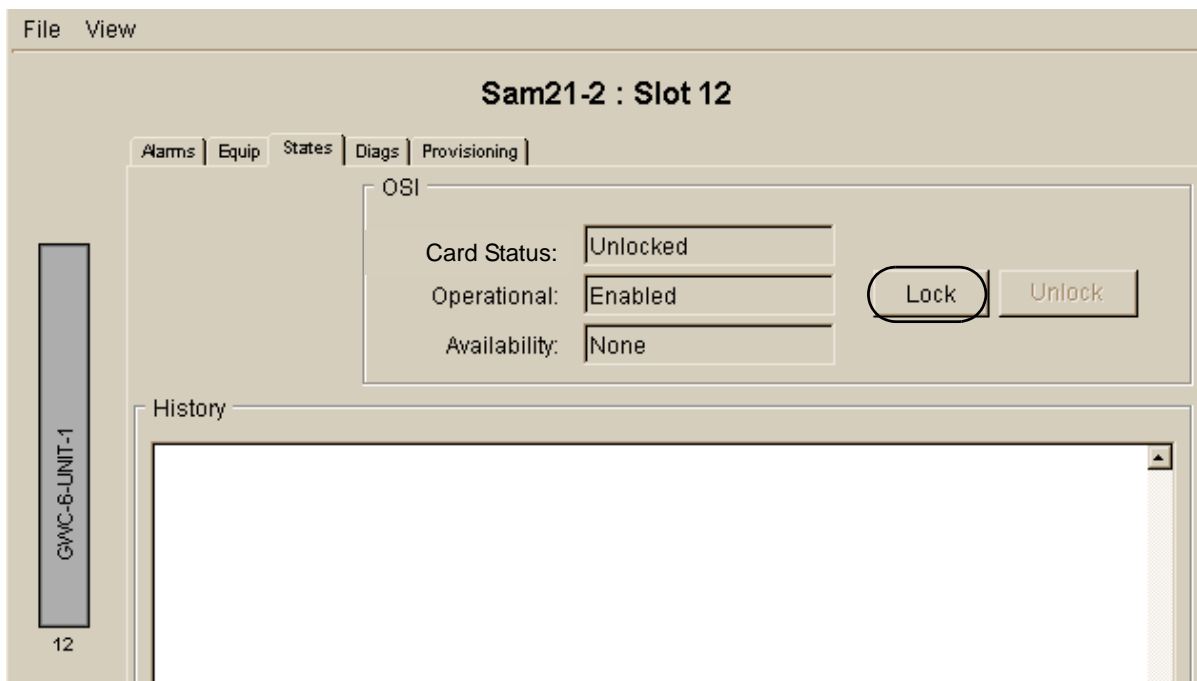


**At the CS 2000 SAM21 Manager client**

- 5 In the card view, select the **States** tab.



- 6 In the States display, click the **Lock** button to lock the card.



- 7 Observe the system response in the History window.

The card is locked when you see the text “Application locked successfully” in the History display. The lock icon (circled in the screen shot below) should also be present on the card graphic at the left of the screen:



- 8 If necessary, return to [step 2](#) and repeat this procedure for the next GWC card in the node.
- 9 The procedure is complete.

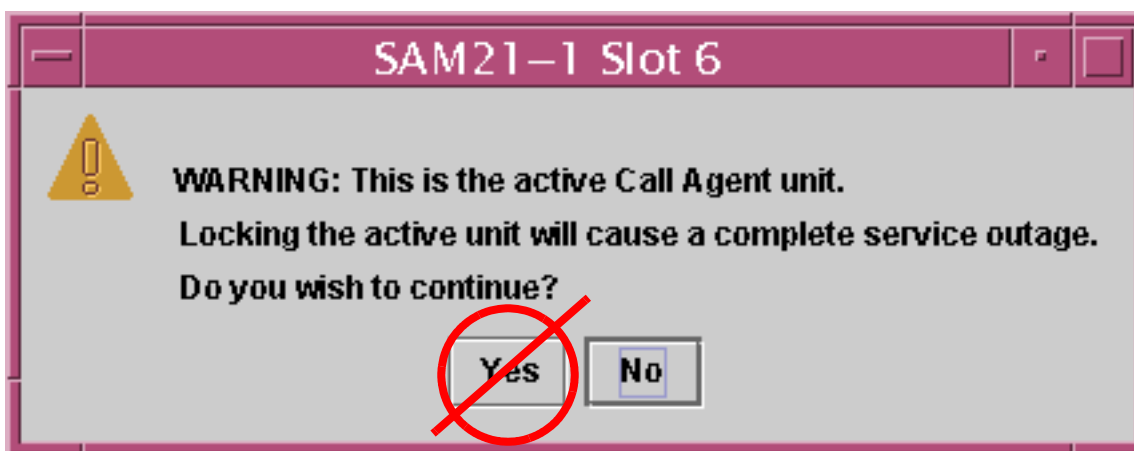
## Locking the Call Agent



**CAUTION**  
**Possible service interruption**  
Do not lock the active Call Agent.

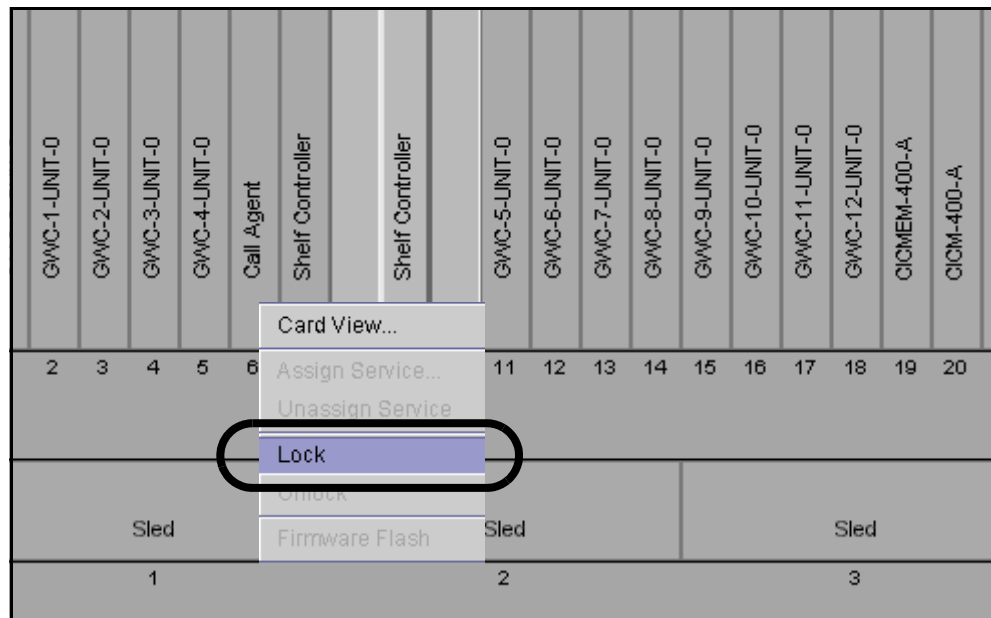
The CS 2000 SAM21 Manager client responds to an active Call Agent lock with the prompt shown in figure [Call Agent lock warning](#). Do not click Yes. The inactive Call Agent is located in the other CS 2000 SAM21 Manager shelf and a lock request does not provide a prompt when the Call Agent is inactive.

### Call Agent lock warning



#### *At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right click on the card and select Lock from the context menu.



**Note:** Lock is also available from the States tab of the Card View window.

- 2 Do not confirm a lock warning. The warning is only available for the active Call Agent. Wait for the lock icon to appear on the selected card.
- 3 This procedure is complete.

---

## Powering down the Border Control Point Manager

---

### Purpose of this procedure

Use the following procedure to power down the Border Control Point Manager. The Border Control Point Manager is installed on a Sun Netra 240 (N240).

### When to use this procedure

Use this procedure when it is necessary to power up the Sun N240 server that houses the Border Control Point Manager.

### Prerequisites

You must have the root user password for the N240.

You need two IP addresses for N240.

### Action

#### Powering down the Border Control Point Manager

##### *At the N240 server*

- 1 Telnet or SSH into the server and login as the root user.
- 2 Type  
`#init 0`  
and press the Enter key.  
At this point the server will shutdown gracefully and the Telnet or SSH connection will be closed.
- 3 At this point, the server can be turned off at the circuit breakers.
- 4 You have completed this procedure.



---

## Powering down an T1400 or N240 server

---

### Purpose of this procedure

Use the following procedure to power down a NetraTM T1400 or N240 server.

### When to use this procedure

Use this procedure when it is necessary to power down the NetraTM T1400 or duplex N240 servers.

### Prerequisites

You must have the root user password for the T1400 and N240.

If you are shutting down the N240s, you need to IP addresses for both the active and inactive units.

### Action

#### Powering down a NetraTM T1400 or N240 server

1

If you are powering down a	Do
T1400	step <a href="#">2</a>
N240	step <a href="#">6</a>

---

#### *At the T1400 server*

2 Telnet or SSH into the T1400 and login as the root user.

3 Type

```
#init 0
```

and press the Enter key.

At this point, the server will shutdown gracefully, and the telnet or SSH connection will be closed.

4 Turn off the power to the server at the circuit breaker panel of the frame.

5 Go to step [11](#).

#### *At the N240 server*

6 Telnet or SSH into the inactive server and login as the root user.

- 7 Type  
**#init 0**  
and press the Enter key.  
At this point the server will shutdown gracefully and the Telnet or SSH connection will be closed.
- 8 Telnet or SSH into the active server and login as the root user.
- 9 Type  
**#init 0**  
and press the Enter key.  
At this point the server will shutdown gracefully and the Telnet or SSH connection will be closed.
- 10 At this point, both servers can be turned off at the circuit breakers.
- 11 You have completed this procedure.



---

## Performing a partial power down of the N240 server

---

### Purpose

This procedure is used to perform a partial power down of the N240 servers. The N240 servers are commissioned with one active and one inactive unit. This procedure shuts down the inactive unit.

### Prerequisites

You must have the root user password for the N240.

You need to IP address for the inactive unit.

### Action

#### Performing a partial power down of the N240 servers

##### *At the N240 server*

- 1 Telnet or SSH into the inactive server and login as the root user.
- 2 Type  
`#init 0`  
and press the Enter key.  
At this point the server will shutdown gracefully and the Telnet or SSH connection will be closed.
- 3 At this point, the inactive server can be turned off at the circuit breaker.
- 4 You have completed this procedure.



---

## Powering down the SDM

---

### Purpose of this procedure

Use the following procedure to power down the SuperNode Data Manager (SDM) that houses the CS 2000 Core Manager.

### When to use this procedure

Use this procedure when it is necessary to power down the SDM hardware.

### Prerequisites

None

### Action

#### Powering down the SDM

##### *At the VT100 terminal*

- 1 Login as the root user.
- 2 Shutdown the SDM by typing  
**# shutdown -f**  
and pressing the Enter key.
- 3 Wait for the system to display the following:  
Halt Completed

##### *At the SDM frame*

- 4 Turn off the two breakers at the top of the SDM frame.
- 5 You have completed this procedure.



## Powering down a Ethernet Routing Switch 8600

### Purpose of this procedure

Use the following procedure to power down a Ethernet Routing Switch 8600.

### When to use this procedure

Use this procedure when it is necessary to power down a Ethernet Routing Switch 8600.

### Prerequisites

None

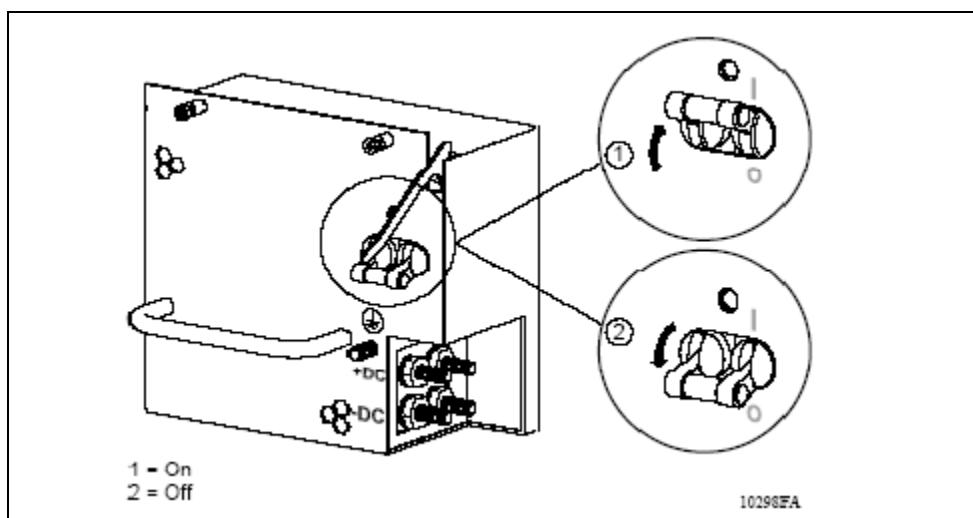
### Action

#### Powering down a Ethernet Routing Switch 8600

##### *At the Ethernet Routing Switch 8600 frame*

- 1 If you have an 8010co Chassis unit and an optional breaker interface panel (BIP) installed, set the BIP circuit breakers to the off position.  
  
Refer to Installing the Breaker Interface Panel for the 8010co Chassis, 312755-E.
- 2 Turn the power supply switch to the off position. Refer to the following figure.

##### Turning the power supply switch to the off position



- 3** Disable the incoming power from the DC input power source. You may need to switch a circuit breaker or turn off the DC input power source.
- 4** You have completed this procedure.

---

## Performing a partial power down of the Ethernet Routing Switch 8600

---

### Purpose

This procedure is used to perform a partial power down of an Ethernet Routing Switch 8600.

### Prerequisites

None

### Action

#### **Performing a partial power down of the Ethernet Routing Switch 8600**

##### ***At the chassis***

- 1** Each chassis has its own BIP circuit breaker. Set the BIP circuit breaker to the off position to work in simplex mode.
- 2** Turn one of the three DC power supplies off. This will leave 2 DC power supplies to support the remaining chassis.
- 3** You have completed this procedure.





## Powering down the XA-Core

### Application

Use this procedure to power down a DMS switch as follows:

- in the event of an emergency, for example, flooding or fire
- to protect equipment if the available functioning voltage at the power distribution center (PDC) falls below -43.75 V dc
- when instructed by the next level of support

### Prerequisites

None

### Action

#### Emergency shutdown of the switch



#### CAUTION

**This procedure results in a complete loss of subscriber service.**

Nortel Networks recommends that before you perform this procedure, you should contact emergency Technical Assistance Services (ETAS) of Nortel Networks or contact your next level of support.

#### *At your current location*

- 1 Notify network management personnel of the impending service interruption.
- 2 Notify emergency services (police, fire, ambulance) of the impending service interruption.

#### *At the switch*

- 3 Select the next step as follows:

If	Do
the switch must be shut down immediately due to dangerous environmental conditions	<a href="#">step 4</a>
there is time (one half hour or more) to shut down the switch in an orderly fashion	<a href="#">step 6</a>

- 4 Turn off the power to the power distribution centers (PDCs) by disconnecting the power feeds at the power room.  
**Note:** Turning off the switch in this manner should be done only if absolutely necessary, as current arcing may occur.
- 5 Go to [step 19](#).
- 6 Using office records, identify the peripheral modules that host emergency services (such as fire, police, and ambulance), so that these peripherals can be shut off last.
- 7 Turn off the power converter for each maintenance trunk module shelf, except those identified in [step 6](#) as essential for emergency service lines.  
**Note:** Older peripheral modules, such as line modules and digital carrier modules, use universal tone receivers resident in maintenance trunk modules.
- 8 Turn off the inverters for all MAPs and printers, except the operator MAP and one printer.
- 9 Turn off the power converters on all digital trunk controllers and trunk modules, except those identified in [step 6](#) as essential for emergency service communications.
- 10 Turn off the power converters on each line module shelf, except those identified in [step 6](#) as hosting emergency service lines.
- 11 Turn off the power converters on all line concentrating modules, except those identified in [step 6](#) as hosting emergency service lines.
- 12 Turn off the power converters on all line group controllers and line trunk controllers, except those identified in [step 6](#) as essential for emergency service communications.
- 13 Turn off the power on all remaining peripheral modules, leaving essential service peripheral modules until last.
- 14 Turn off the power for the network modules, link peripheral processor, and input/output controllers (IOCs).  
**Note:** To power down the ENET and the LPP, unseat and then reseat the power converters.
- 15 Turn off the power for all remaining devices, including the inverter that supplies the operator MAP, and any external printers, tape drives, or disk drives.
- 16 Turn off the power for the XA-Core. Power down both SIM cards in the XA-Core. In each SIM card you must turn off three breakers.

- 17** Turn off the power for the message switch. Power down one plane by turning off the power converters. Power down the second plane by unseating and then reseating the power converters.
- 18** Turn off the power to the power distribution centers (PDCs) by discontinuing the A and B feeds at the power room.
- 19** You have completed this procedure.



---

## Performing a partial power down of the XA-Core

---

### Application

Use this procedure to maintain emergency backup power for a DMS SuperNode or a DMS SuperNode SE switch. Use this procedure when the switch has an eXtended Architecture Core (XA-Core) configuration.

This procedure reduces the loss from emergency batteries to a minimum by closure of power to equipment in stages. The equipment shutdown is not necessary to maintain subscriber service. Equipment shutdown is in moving up order based on its effect on switch reliability. The equipment shutdown begins with less required equipment, such as spare printers, and ends with more required equipment.

When you perform this procedure, take into consideration the configuration and condition of your switch. Also take into consideration the expected period of the power outage, and the quantity of reserve power available. Continue as follows:

**Note:** If you receive a warning message for a loss of service if you busy a plane or unit, do not continue. Clear the problem that can cause a loss of service before you busy the plane or unit. Also you can leave both planes or units of that subsystem in service.

- Complete the number of steps of this procedure as your set of conditions needs. For example, if you expect power to restore, you can decide to leave important systems to operate in a duplex mode. The message switch (MS) is an example of a system that can have a duplex mode. Equally for reliability, you can decide to leave both units in service on peripheral modules required for emergency service lines.
- This procedure requires a condition when this procedure instructs you to busy down one plane or unit of a system. The condition is that the mate plane or unit you leave in service, is fault free and can operate normally.
- When possible, take the same plane or unit out of service on each subsystem (for example, ENET plane 0, LIM unit 0, MS 0). This action decreases the possible result of error and reduces recovery time.

### Prerequisites

None

## Action

### Emergency power conservation shutdown

**CAUTION****Potential service interruption or extended outage**

Nortel Networks recommends that you call Emergency Technical Assistance Services (ETAS) of Nortel Networks. Also call your next level of support before you perform this procedure.

**CAUTION****Potential loss of service or extended outage**

This procedure is only for conservation of emergency backup power. Do not use this procedure or sections for equipment maintenance purposes.

#### *At your current location*

- 1 Use office records to identify and record the power converters that supply the MAPs and printers for the switch.
- 2 Turn the power off on all power converters identified in step 1. Do not turn the power off for the power converters which supplies the operator's MAP and one printer connected to IOC 0.

#### *At the MAP terminal*

- 3 To confirm that an office image is available to reload the switch if a total turn off of power becomes necessary, type:

```
>AUTODUMP STATUS
```

and press the enter key.

*Example of a MAP response*

```
Successful Image: 990215_CM  
Taken: 1999/03/17 21:47:32:04.138 WED.  
On Volume: F17LIMAGE
```

```
Successful Image: 990215_MS  
Taken: 1999/03/17 21:47:32:04:138 WED.  
On Volume: F17LIMAGE
```

```
SCHEDULED-Image Dump is ON.
```

Next scheduled dump is MONDAY at 22:30 hours.  
Next image to be dumped on F02LIMAGE.

If an office image is	Do
available	step <a href="#">5</a>
not available	step <a href="#">4</a>

- 4 Record the office image. Perform the procedure, 'How to record an XA-Core office image on a disk' in this document. Return to this step when you complete the procedure to record the office image.
- 5 Turn off power for all maintenance trunk modules (MTM) in the office. Do not turn power off if the MTM contains cards that have an effect on service. To turn off power perform the procedure, 'Emergency shutdown of maintenance trunk modules' in *Recovery Procedures*, 297-8021-545.  
**Note:** Cards that have an effect on service include digitone receiver cards (NT2X48), centralized automatic message accounting (CAMA) cards (NT2X66), and digital recorded announcement machine (DRAM) cards.
- 6 Turn off power for one of the line module controllers (LMC) (NT2X14 shelf) in each double-bay line module (LM) pair in the office. To turn off the power, perform the procedure, 'Emergency shutdown of one half of a line module pair' in *Recovery Procedures*, 297-8021-545.
- 7 Turn off power for one unit of all line concentrating modules (LCM) in the office. To turn off the power, perform the procedure, 'Emergency shutdown of one unit of LCMs' in *Recovery Procedures*, 297-8021-545.
- 8 Turn off power for one unit of all line group controllers (LGC), line trunk controllers (LTC), and digital trunk controllers (DTC) in the office. To turn off the power, perform the procedure, 'Emergency shutdown of one LGC, LTC, and DTC unit' in *Recovery Procedures*, 297-8021-545.
- 9 Turn off power for one plane of all network shelves in the office, as follows:
  - for ENET, perform the procedure, 'Emergency shutdown of one enhanced network plane' in *Recovery Procedures*, 297-8021-545.
  - for JNET, perform the procedure, 'Emergency shutdown of one junctored network plane' in *Recovery Procedures*, 297-8021-545.

- 10** If you removed power from a complete network frame in step [9](#), turn off power for the cooling fans for the frame. To turn off power, remove the correct power fuses from the PDC.
- 11** Busy and power down one local message switch in the link peripheral processor (LPP). Perform the procedure, 'Emergency shutdown of one LIM unit on each LPP' in *Recovery Procedures*, 297-8021-545.
- 12** Turn off power for one unit of all CCS7 message switch and buffers (MSB7) in the office. To turn off power, perform the procedure, "Emergency shutdown of one unit of MSB7s" in *Recovery Procedures*, 297-8021-545.
- 13** Turn off power for one message switch (MS) plane. To turn off power, perform the procedure, 'Emergency shutdown of one DMS SuperNode MS plane' in *Recovery Procedures*, 297-8021-545.
- 14** If your office has a remote oscillator shelf (NT3X9507), busy the clock related to the MS number. The MS number is for the MS that you turned off power in step [13](#). To busy the clock, perform the procedure, 'Emergency shutdown of one remote oscillator shelf plane' in *Recovery Procedures*, 297-8021-545.
- 15** You have completed this procedure.







# Powering up the network

---

## Purpose of this procedure

**ATTENTION**

If your network uses a Geographically Survivable configuration, refer to [Geographic survivability on page 599](#).

This procedure details the sequence of steps necessary to power up all of the network elements in the office. Not all network elements covered in this procedure will apply to your office. The following network elements are covered by this procedure:

- XA-Core
- 3rd Party Core
- Message Switch
- ENET
- Ethernet Routing Switch 8600
- LPP
- SDM, CS 2000 Core Manager, or Core and Billing Manager
- IEMS
- CS 2000 Management Tools
- MG 9000 Manager
- Border Control Point Manager
- SAM21 shelf and cards
- CICM
- USP
- Media Gateway 15000/7400 or Multiservice Switch 15000/7400
- MDM workstation
- SPM, MG 4000, IW-SPM, DPT-SPM
- MCS servers
- Border Control Point
- MS 2000 Series or UAS

- Packet Media Anchor
- MG 9000

### **When to use this procedure**

Use this procedure in the event of a power outage. This outage may have been planned or unplanned.

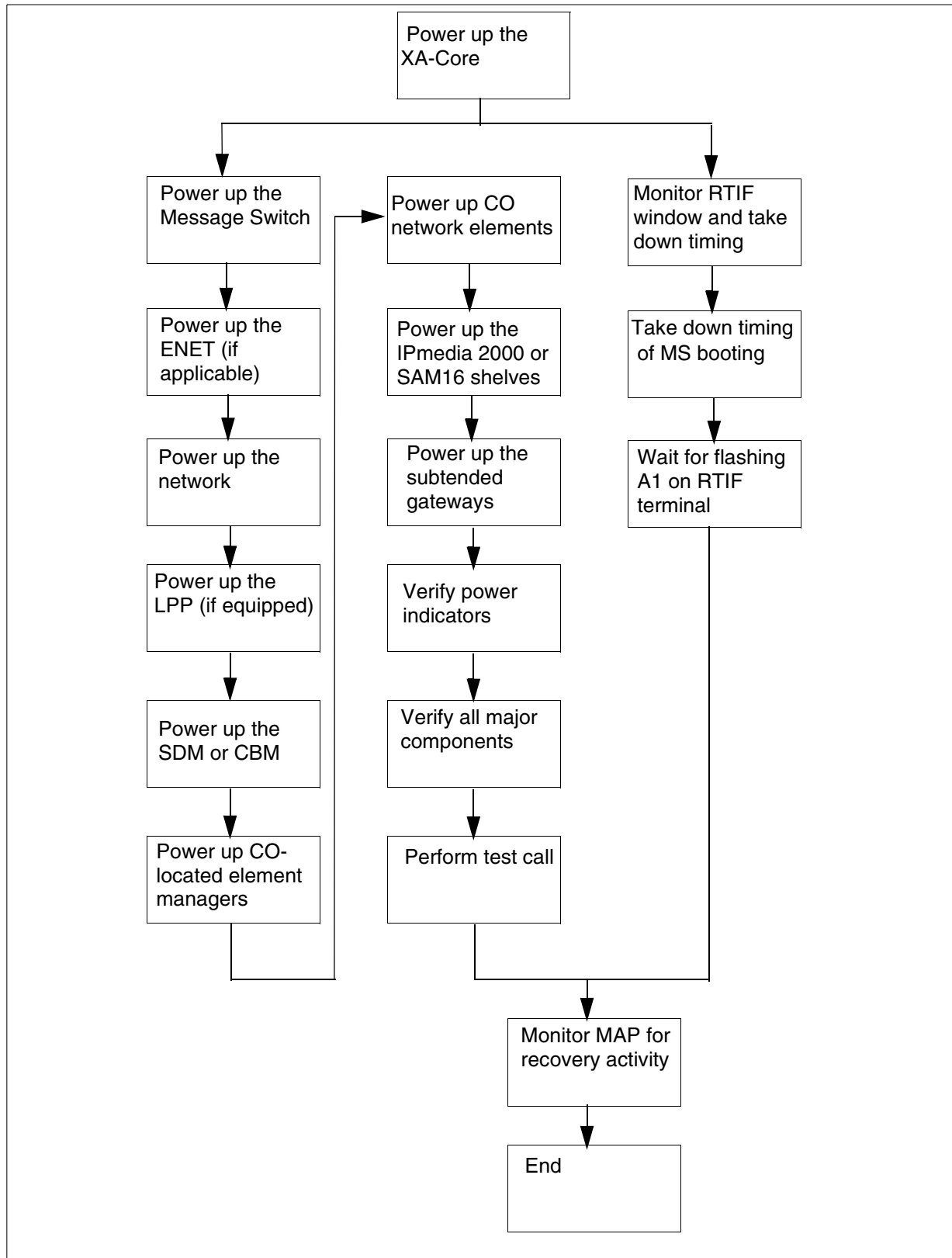
### **Prerequisites**

This procedure has the following prerequisites:

- This task requires more than one person to perform, as some steps are performed in parallel.
- The power recovery sequence can only be started when the AMP reading on SPDC-0 reaches 0.

### **Action**

This procedure contains a summary flowchart and a list of steps. Use the flowchart to review the procedure. Follow the steps to perform the recovery task.

**Figure 1 Summary of procedure for an XA-Core-based office**

**Figure 2 Summary of procedure for a CS 2000-Compact-based office*****In the network office***

- 1 Determine if you are powering up a CS 2000 or CS 2000-Compact-based office.

If you are powering up a	Do
CS 2000-based office	step <a href="#">2</a>
CS 2000-Compact-based office	step <a href="#">9</a>

- 2 Power up the XA-Core. Refer to [Powering up the XA-Core on page 445](#).
- 3 Perform steps 4 and 5 in parallel.
- 4 Power up the network elements and element managers.
  - a Power up the Message Switch and ENET (if equipped).  
Refer to [Powering up the Message Switch on page 479](#) and [Powering up the Enhanced Network on page 485](#).
  - b Power up the IP network, including the Ethernet Routing Switch 8600 and the IP Switches.  
Refer to [Powering up a Ethernet Routing Switch 8600 on page 499](#).
  - c Power up the LPP (if equipped).  
Refer to [Powering up the Link Peripheral Processors on page 503](#).
  - d Power up the SDM or CBM.  
For the SDM, refer to [Powering up the SDM on page 523](#). For the CBM, refer to [Powering up a T1400 or N240 server on page 525](#).
  - e If equipped, power up the DNS server. Refer to the hardware documentation for your server for detailed instructions.
  - f

**ATTENTION**

Wait at least 5 minutes between each step from [f](#) to [k](#).

Power up the CO located element managers, such as the IEMS, CS 2000 Management Tools, and MG 9000 Manager.

Refer to [Powering up a T1400 or N240 server on page 525](#)

- g If equipped, power up the Border Control Point Manager.  
Refer to [Powering up the Border Control Point Manager on page 529](#).
- h Power up the CO network elements, including the SAM21 SCs, GWCs, Session Server, Policy Controller, CICM, USP, Multiservice Switch 15000/7400, Media Gateway 15000/7400, and SPMs.

Refer to the following procedures:

- [Powering up the SAMF frame on page 531](#)
- [Powering up a USP on page 557](#)
- [Powering up a Media Gateway/Multiservice Switch 15000 on page 563](#)
- [Powering up a Media Gateway/Multiservice Switch 7400 on page 567](#)
- [Powering up the MDM workstation on page 569](#)
- [Powering up an SPM device on page 571](#)

- i If equipped, power up the MCS servers and/or Border Control Point.

Refer to [Powering up the MCS servers on page 575](#) and [Powering up a Border Control Point on page 587](#).

- j Power up the shelves that house the MS 2000 Series/UAS devices and Packet Media Anchor.

If your system uses an MS 2000 Series device or Packet Media Anchor, refer to [Powering up the IPmedia 2000 shelves on page 589](#). If your system uses a UAS, refer to [Powering up the SAM16 shelves on page 591](#).

- k Power up the subtended gateways, such as the MG 9000 and MTA.

For the MG 9000, refer to [Powering up an MG 9000 device on page 593](#).

For other third party devices, refer to the documentation for your hardware.

- l Proceed to step [6](#) after completing this step and step [5](#).

- 5** Collect XA-Core dead office recovery data.

- a During the power up sequence, monitor the RTIF window until Core booting is complete. Take down the timing.
- b MS booting should start next. Allow the booting to complete before proceeding to the next step. Take down the timing.
- c Restart reload should start. Wait until you see the flashing A1 on the RTIF terminal before proceeding.
- d Proceed to step [6](#) after completing this step and step [4](#).

- 6** From the operator terminal, type

```
>priority on; mapci;mtc;srstatus
```

and press the Enter key.



Check the MAP banner and monitor recovery activity. They should have critical alarms that indicate the autonomous Network Elements recovery.

- 7 Reverify all the power indicators on the Network Elements.
- 8 Go to step [15](#).
- 9 Power up the IP network, including the Ethernet Routing Switch 8600 and the IP switches.  
Refer to [Powering up a Ethernet Routing Switch 8600 on page 499](#).
- 10 Power up the SDM or CBM.  
For the SDM, refer to [Powering up the SDM on page 523](#). For the CBM, refer to [Powering up a T1400 or N240 server on page 525](#).
- 11 If equipped, power up the DNS server. Refer to the hardware documentation for your server for detailed instructions.
- 12 Perform steps [13](#) and [14](#) in parallel.
- 13 Power up the remaining network elements by performing the following steps.

**a**

**ATTENTION**

Wait at least 5 minutes between each step from [a](#) to [f](#).

Power up the CO located element managers, such as the IEMS, CS 2000 Management Tools, and MG 9000 Manager.

Refer to [Powering up a T1400 or N240 server on page 525](#)

- b** If equipped, power up the Border Control Point Manager.  
Refer to [Powering up the Border Control Point Manager on page 529](#).
- c** Power up the CO network elements, including the SAM21 SC, 3PC cards, GWCs, Session Server, CICM, USP, IW-SPM, Multiservice Switch 15000/7400, Media Gateway 15000/7400, and SPMs.  
Refer to the following procedures:
  - [Powering up the Call Control Frame on page 545](#)
  - [Powering up a USP on page 557](#)
  - [Powering up a Media Gateway/Multiservice Switch 15000 on page 563](#)

- [Powering up a Media Gateway/Multiservice Switch 7400 on page 567](#)
  - [Powering up the MDM workstation on page 569](#)
  - [Powering up an SPM device on page 571](#)
- d** If equipped, power up the MCS servers and/or Border Control Point.
- Refer to [Powering up the MCS servers on page 575](#) and [Powering up a Border Control Point on page 587](#).
- e** Power up the shelves that house the MS 2000 Series/UAS devices and Packet Media Anchor.
- If your system uses an MS 2000 Series device or Packet Media Anchor, refer to [Powering up the IPmedia 2000 shelves on page 589](#). If your system uses a UAS, refer to [Powering up the SAM16 shelves on page 591](#).
- f** Power up the subtended gateways, such as the MG 9000 and MTA.
- For the MG 9000, refer to [Powering up an MG 9000 device on page 593](#).
- For other third party devices, refer to the documentation for your device.
- g** Verify all the power indicators after the outage once all the above steps are completed.
- h** Verify all the major components after power up via IEMS (or other managers if not equipped with IEMS).
- i** Proceed to step [15](#) after completing this step and step [14](#).
- 14** Collect dead office recovery data by performing the following steps.
- a** Record the start time of the 3PC blades powering up.
  - b** While the 3PC is rebooting, attempt to login to the Call Agent Application level through the SDM, CBM, or CS 2000 Management Tools server. As soon as available, type  
**# priority on;mapci;mtc;srstatus**  
and press the Enter key.
  - c** Check the MAP banner. There should be critical alarms indicating the autonomous Network Elements recovery.
  - d** Take down the timings for the Trks, Lns, CCS, and PM alarms when they are cleared.

- e Start logutil and monitor core logs for recovery activities.  
Take down the timing of the INIT log by typing

```
# logutil;open INIT
```

- 15 You have completed this procedure.



## Powering up the XA-Core

### Application

Use this procedure to power up a dead switch that has an eXtended Architecture Core (XA-Core). The switch can be a DMS SuperNode or SuperNode SE switch. The switch is dead if the complete switch is without power. The power loss results from a loss or interruption of A and B dc power feeds to the power distribution center (PDC).

### Action

#### How to recover a dead XA-Core DMS switch

**CAUTION****Call ETAS or your next level of support**

In the event of a dead system, call the Emergency Technical Assistance Services (ETAS) of Nortel Networks. Also call your next level of support before you perform this procedure.

**DANGER****Risk of electrocution**

Do not touch the cabinet wiring. Connections with unshielded cabinet wiring can result in electric shock. Only qualified power maintenance personnel can perform the voltage measurements in step [3](#).

#### At the PDC

- 1 When possible after detection of the power outage, remove all the fuse holders for the following:
  - line concentrating equipment (LCE) talk batteries
  - trunk module equipment (TME) talk batteries
  - PDC filter fuses from the correct PDCs

**Note:** The location of the fuse holders in the fuse panel can vary, depending on your office configuration. For help in locating the fuse holders, refer to the fuse assignment diagram for your office. Also call your next level of support to help you locate the fuses.

- 2 The next step depends on if the switch power is a -48 V dc feed or by a -60 V dc feed.

If the switch power is	Do
-48 V dc	<a href="#">step 3</a>
-60 V dc	<a href="#">step 4</a>

- 3 Continue when you know of restored power at the power plant for your office. Power maintenance personnel must check for restored power at each PDC. At the rear of each PDC, measure the dc voltage across the A feed bus and the battery return plate. Repeat the dc voltage measurement for the B feed bus. Power is correct when the voltage on each feed is -48 V dc.

**Note:** Power can be at a nominal potential of -48 V dc. Under conditions that are not normal, the operating voltage can range from -43.75 V dc to -55.8 V dc. A not normal condition is a commercial power failure

If the switch has	Do
power retrieval	<a href="#">step 6</a>
no power retrieval	<a href="#">step 5</a>

- 4 Continue when you know of restored power at the power plant for your office. Request power maintenance personnel to check for restored power at each PDC. At the rear of each PDC, measure the dc voltage across the A feed bus and the battery return plate. Repeat the dc voltage measurement for the B feed bus. Power is correct when the voltage on each feed is -60 V dc.

**Note:** Power can be at a nominal potential of -60 V dc. Under conditions that are not normal, the operating voltage can range from -57.4 V dc to -67.7 V dc. A not normal condition is a commercial power failure.

If power has	Do
power retrieval	<a href="#">step 6</a>
no power retrieval	<a href="#">step 5</a>

### **At the power room**

- 5 For help in restoring power to the PDC, call the personnel responsible for maintenance of power at your site.
- When power restores to the PDC, return to this point.

**At the PDC**

**6** Inspect the alarm indication fuses for the XA-Core and the network cabinets.

If uses that blew are	Do
present	<a href="#">step 7</a>
not present	<a href="#">step 14</a>

**7** Replace the blown cartridge fuse in the rear of the fuse holder. Make sure that the amperage of the replacement cartridge fuse matches the amperage marked on the PDC.

**8** Remove the blown alarm-indication fuse from the front of the fuse holder.

**9** Re-insert the fuse holder, with the alarm-indication fuse removed, into the PDC.

**10** Get an alarm-indication fuse for replacement.

**11** Insert the alarm-indication fuse that is for replacement into the fuse holder.

**12** Continue as follows:

If the replacement fuse is	Do
not successful and blows repeatedly	<a href="#">step 13</a>
successful	<a href="#">step 14</a>

**13** Call your next level of support for help.  
Continue when you complete replacement of all blown fuses and restored power to the XA-Core and network cabinets. Continue this procedure at [step 14](#).

**14** If a second person is available to help in the recovery, continue this procedure with two sets of tasks. Request the second person to restore power from the pdc to the peripheral module frames. The second person restores power by use of steps [56](#) through [71](#) of this procedure. While the second person restores power, you recover the core and network by completion of steps [15](#) through [43](#). If one person is available, recover the core and network first.

**15** Determine if the switch has a remote oscillator shelf.

If the switch has	Do
a remote oscillator shelf	<a href="#">step 16</a>

If the switch has	Do
no remote oscillator shelf	<a href="#">step 17</a>

### ***At the remote oscillator shelf***

- 16** Turn on the power converters for the shelf.

### ***At the XA-Core cabinet***

- 17** Determine if the switch is a SuperNode switch or a SuperNode SE switch.

If the switch is	Do
a SuperNode switch	<a href="#">step 18</a>
a SuperNode SE switch	<a href="#">step 21</a>

- 18** Turn on circuit breakers for shelf interface module (SIM) A. Turn on the three switches for circuit breakers A1, A2, and A3. The SIM A card is in slot 3R of the XA-Core shelf.
- 19** Turn on circuit breakers for shelf interface module (SIM) B. Turn on the three switches for circuit breakers B1, B2, and B3. The SIM B card is in slot 16R of the XA-Core shelf.
- 20** Go to [step 23](#)
- 21** Turn on circuit breakers for shelf interface module (SIM) A. Turn on the two switches for circuit breakers A1 and A2. The SIM A card is in slot 3R of the XA-Core shelf.
- 22** Turn on circuit breakers for shelf interface module (SIM) B. Turn on the two switches for circuit breakers B1 and B2. The SIM B card is in slot 16R of the XA-Core shelf.
- 23** Determine if all the power converters have power. You know that all the power converters have power when all the Converter Off lights go off.

If all the power converters have	Do
power	<a href="#">step 26</a>
not power	<a href="#">step 24</a>

- 24** To power up the frame perform the procedure, “Clearing an Ext FSP DPCC cabinet major alarm” in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).  
When you completed the procedure, return to this point.



25 Go to [step 17](#)

**At the XA-Core reset terminal**


26 Monitor the XA-Core reset terminal to determine if the switch has booted.

When the switch boots, the XA-Core reset terminal displays a response to indicate a boot in progress. The response also displays different diagnostic messages and alphanumeric addresses. When the switch has completely booted, an A1 appears on the RTIF display.

If the response has	Do
an A1	<a href="#">step 27</a>
no A1 after approximately 15 min	<a href="#">step 111</a>

**At the MAP terminal**

27



**CAUTION**  
**Extended service interruption**  
 The exact log in procedure can vary, depending on your office configuration. If you need additional help, call the personnel responsible for the next level of support.

Determine if you have to log in.

**Note:** The log in message indicates that you have to manually log in. An automatic log in can occur if the office parameters have automatic log in.

*Example of a MAP response*

Please Login.

If the log in is	Do
not automatic	<a href="#">step 28</a>
automatic	<a href="#">step 32</a>

28 Press the break key.

*Example of a MAP response*

?

29 To log in to the MAP terminal, type:

**>LOGIN**

and press the enter key.

*Example of a MAP response*

```
Enter User Name
```

30 To enter the user name, type:

**>user\_name**

and press the enter key.

where

user\_name is the name of the user for the account

*Example of a MAP response*

```
Enter Password
```

31 To enter the password, type:

**>password**

and press the enter key.

where

password is the name of the password for the account

*Example of a MAP response*

```
SuperNode1 Logged in on 1997/01/15 at 20:37:17
```

32



#### **CAUTION**

All customers must follow the sequence of steps set out in this procedure. Do not interrupt this procedure at this point to clear an alarm. If a TOD critical alarm appears under the APPL level in the alarm banner, and if the system uses Network Time Protocol (NTP), you must complete all steps in the sequence shown. You will clear the TOD critical alarm by completing [step 39](#). (For information on NTP, see [step 39](#).)

To turn on priority, type:

**>PRIORITY ON**

and press the enter key.

*Example of a MAP response*

```
Pref>
```

- 33** To determine if the system time is correct, type:

**>TIME**

and press the enter key.

*Example of a MAP response*

```
Time is 14:55:50
```

If the system time is	Do
correct	<a href="#">step 36</a>
not correct	<a href="#">step 34</a>

- 34** To enter the correct time (by use of the 24 hour clock), type:

**>SETTIME hh mm**

and press the enter key.

where

hh is the hour (00 to 23)

mm is the minute (00 to 59)

*Example of a MAP response*

```
Warning: There is an automated TOD clock
change
request scheduled on:
1997/10/15 at 1:00 (see table DSTTABLE).
Do you want to proceed with this request?
Please confirm ("YES", "Y", "NO", or "N")
```

- 35** To confirm the command, type:

**>YES**

and press the enter key.

*Example of a MAP response*

```
Time is 20:40:00 on WED 1997/10/15.
```

- 36** Determine if the system date is correct.

If the system date is	Do
correct	<a href="#">step 40</a>

**If the system date is****Do**

not correct

[step 37](#)

- 37** To enter the correct date, type:

**>SETDATE dd mm yyyy**

and press the enter key.

where

dd is the day (01 to 31)

mm is the month (01 to 12)

yyyyy is the year

*Example of a MAP response*

Warning: There is an automated TOD clock change request scheduled on:

1997/10/15 at 1:00 (see table DSTTABLE).

Do you want to proceed with this request?

Please confirm ("YES", "Y", "NO", or "N")

- 38** To confirm the command, type:

**>YES**

and press the enter key.

*Example of a MAP response*

Date is WED. 15/OCT/1997 00:00:00

- 39** If the system uses Network Time Protocol (NTP) as the timing reference, and if a TOD critical alarm is displayed under the APPL level in the alarm banner, perform the procedure titled 'How to check and adjust the XA-Core TOD' in the XA-Core Maintenance Manual, 297-8991-510. By performing that procedure, you will clear the TOD critical alarm. Return to this point when finished.

**Note:** In the German market only, switches can use Network Time Protocol (NTP) as the timing reference for the time-of-day clock. The system uses Network Time Protocol if the value of the SNTP\_CLIENT office parameter in table OFCENG has been set to Y. For information on the office parameter, see the chapter titled 'XA-Core data schema overview' in the *XA-Core Reference Manual*, 297-8991-810.

**At the MAP terminal**

- 40** To access the NET level of the MAP display, type:

**>NET**

and press the enter key.

*Example of a MAP response*

```
NET
                                     11111  11111  22222
22222  33
Plane  01234  56789  01234  56789  01234
56789  01
   0  0000
   1  0000
JNET
```

- 41** To manually busy the network module for return to service, type:

**>BSY plane\_no pair\_no**

and press the enter key.

where

plane\_no is the network plane number (0 or 1)

pair\_no is the network plane pair number (0 to 31)

- 42** To return the network module to service, type:

**>RTS plane\_no pair\_no**

and press the enter key.

where

plane\_no is the network plane number (0 or 1)

pair\_no is the network plane pair number (0 to 31)

- 43** Repeat steps [41](#) through [42](#) for each JNET shelf.

When all JNET shelves recover, continue this procedure at step [44](#).

- 44** Determine if there are additional input output controller (IOC) and maintenance and administration position (MAP) terminals to recover.

If recover of additional IOCs and MAP terminals is	Do
not complete	<a href="#">step 45</a>
complete	<a href="#">step 56</a>

- 45 Restore power to all remaining power inverters in the office.

**At the IOC**

- 46 Locate the IOC for recovery.

If recovery is for	Do
an IOC	<a href="#">step 47</a>
an IOM	<a href="#">step 51</a>

- 47 Turn on the power converters on the IOC.

**Note:** The version of IOC determines if the IOC has one or two power converters.

- 48 While you press the reset button on one of the IOC power converters, lift the related circuit breaker to turn on the FSP.

- 49 Release the reset button.

- 50 Repeat steps [46](#) through [49](#) for each IOC for recovery, then continue this procedure at [step 51](#).

- 51 To access the input output device (IOD) level of the MAP display, type:

**>IOD**

and press the enter key.

- 52 To access the IOC level of the MAP display for the IOC for recovery, type:

**>BSY ioc\_no**

and press the enter key.

where

ioc\_no is the number of the IOC or IOM

- 53 To return the IOC or IOM to service, type:

**>RTS ioc\_no**

and press the enter key.

where

ioc\_no is the number of the IOC or IOM

- 54 Repeat steps [52](#) through [53](#) for each IOC or IOM for recovery, then continue this procedure at [step 55](#).

- 55 Log in to additional MAP terminals as required.

**Note:** Steps [28](#) through [31](#) describe how to log in to the MAP terminal.

**At the PDC**


**56** Steps [57](#) through [71](#) describe how to restore power from the PDC to Series I and Series II peripheral module frames. Continue as follows:

If the PDC power to the PM frames restores	Do
correctly	<a href="#">step 72</a>
not correctly	<a href="#">step 57</a>

**57** Get one of the following capacitor charging tools:

- a 100-W, 120-V light bulb installed into a socket that has pigtail leads
- tool number T000655 (CPC number NTA0600512), that has a fuse holder-style connector instead of pigtail leads for easier insertion

**58**



**WARNING**  
Possible equipment damage or extended service interruption  
Use correct fuses. When replacing fuses in the PDC, make sure that the amperage of the fuses is correct. The fuse amperage must match the amperage marked on the PDC.

At the first empty fuse slot in the PDC, connect the leads of the capacitor charging tool. Connect the leads across the contacts for the fuse holder until the lamp decreases brightness. If you use a charging tool with a fuse holder-style connector, insert the connector into the slot. Insert the connector until the lamp decreases brightness.

**59** Remove the capacitor charging tool and immediately insert again the correct fuse holder into the slot.

**60** Repeat steps [58](#) and [59](#) for all the LCE talk battery, TME talk battery, and PDC filter fuse holders you removed in step 1. When all fuses restore to the PDCs, continue with this procedure.

- 61 Determine if any alarm-indicating fuses blew.

**Note:** The fuse alarm-indicator lamp lights when an alarm-indicating fuse blows.

If any alarm-indicating fuses have	Do
blown	<a href="#">step 62</a>
not blown	<a href="#">step 72</a>

- 62 Locate a fuse holder with a blown alarm-indicating fuse.

**Note:** You can replace blown fuses in any order.

- 63 The cartridge fuse in the fuse holder has blown. Remove the fuse holder from the PDC.
- 64 Replace the blown cartridge fuse in the rear of the fuse holder. Make sure that the amperage of the replacement cartridge fuse matches the amperage marked on the PDC.
- 65 Remove the blown alarm-indicating fuse from the front of the fuse holder.
- 66 Insert again the fuse holder, with the alarm-indicating fuse removed, into the PDC.
- 67 Get a replacement alarm-indicating fuse.
- 68 Insert the replacement alarm-indicating fuse into the fuse holder.
- 69 Determine if the alarm-indicating fuse blows.

**Note:** The fuse alarm indicator lamp lights when an alarm-indicating fuse blows.

If the alarm-indicating fuse is	Do
blown	<a href="#">step 111</a>
not blown	<a href="#">step 70</a>

- 70 Determine if you replaced all the blown alarm-indicating fuses.

If you have	Do
replaced all the blown alarm-indicating fuses	<a href="#">step 71</a>
not replaced all the blown alarm-indicating fuses	<a href="#">step 62</a>



- 71 Determine if the fuse alarm indicator lamp lit.

If the fuse alarm indicator lamp lit	Do
yes	<a href="#">step 111</a>
no	<a href="#">step 72</a>

**At the PM frames**

- 72 Select a peripheral module (PM) frame to power up.

**Note:** The PM frames can power up in any order.

- 73 Locate the frame supervisory panel (FSP) and the power converters on the frame.
- 74 Determine if the FSP for the frame has fuses or circuit breakers.

If the FSP has	Do
fuses	<a href="#">step 75</a>
circuit breakers	<a href="#">step 80</a>

- 75 Determine if the power converters have Power Reset buttons or Power Reset switches.

If the power converters have	Do
Power Reset buttons	<a href="#">step 76</a>
Power Reset switches	<a href="#">step 78</a>

- 76 To turn on each power converter press and hold its Power Reset button for 2 s.

**Note:** The Converter Fail light goes off when the power converter turns on.

- 77 Determine if all the power converters turn on correctly, indicated by all the Converter Fail lights going off.

If all the Converter Fail lights are	Do
off	<a href="#">step 82</a>
not off	<a href="#">step 83</a>

- 78** To turn on each power converter pull out the power switch and toggle it to the Power Reset position.

**Note:** The Converter Fail light goes off when the power converter turns on.

- 79** Determine if all the power converters turns on correctly, indicated by all the Converter Fail lights are off.

**If all the Converter Fail lights are**

**Do**

off

[step 82](#)

not off

[step 83](#)

- 80** Turn on each power converter as follows:

- Toggle the circuit breaker to the ON position.
- Press and hold the Power Reset button for 2 s.
- Release the circuit breaker and the Power Reset button.

**Note:** The Converter Fail light goes off when the power converter turns on.

- 81** Determine if all the power converters turn on correctly, indicated by all the CONVERTER FAIL lights are off.

**If all the Converter Fail lights are**

**Do**

off

[step 82](#)

not off

[step 83](#)

- 82** Determine if all PM frames turn on.

**If all the PM frames turn on**

**Do**

yes

[step 87](#)

no

[step 83](#)

- 83** Determine if a try made to power up the remaining PM frames.

**If power up has**

**Do**

not tried

[step 84](#)

tried and failed

[step 86](#)

- 84** Power up the next PM frame.

- 85** Go to [step 73](#).

- 86 To power up the remaining PM frames perform the correct procedures in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).

**At the MAP terminal**

- 87 To access the SRSTATUS level of the MAP display, type:

**>MAPCI;MTC;SRSTATUS**

and press the enter key.

*Example of a MAP response*

```

SRSTATUS
0 Quit  OVERALL STATUS  Pend: 0%  Inprg: 0%
Comp: 100%  Fail: 0%
2 View_  View: SYSTEM
14:08:30
3 List_          Pend  InPrg  Comp  Fail      Pend
InPrg Comp Fail
4          MS          0      0      2      0      IOD
5  5      30  2
5          NET          0      0      6      0      Other
21  3      13  3
6          SER1          0      41     0      0
7          SER2          0      39     0      0
8          SER3          0      0      37     0
9
10          MTC:
11          STATUS:
    
```

- 88 From the MAP display, determine the recovery status of the Series I and II PMs.

**Note:** Series I PM recovery status displays to the right of the word ‘SER1’ in the MAP display. Series II PM recovery status displays to the right of the word ‘SER2’ in the MAP display. Recovery status can be one of pending, in progress, complete, or failed.

If the recovery status is	Do
zero	<a href="#">step 91</a>
not zero	<a href="#">step 89</a>

- 89 Determine from office records or other office personnel which PMs to manually recover first.

- 90** To manually recover the PMs in the required order, perform the correct alarm clearing procedures in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).

**91**



**CAUTION**

**Loss of billing data**

Different billing systems than automatic message accounting (AMA) or additional billing system, can be in your office configuration. Call your next level of support to determine if other billing systems are in your office, and if you require recovery action.

To access the device independent recording package (DIRP) level of the MAP, type:

**>IOD;DIRP**

and press the enter key.

- 92** To determine the state of the recording volumes for the billing system, type:

**>QUERY subsystem ALL**

and press the enter key.

where

subsystem is the name of the DIRP system used for the billing system

*Example of a MAP response*

```
SSNAME  SSNO  SEQNO  ROTATES  POOLNO  PARLPOOL
EMERGENCY
AMA      0      1      6      9      62
***YES***
REGULAR
FILE(S) STATE VOLUME RECCOUNT BLOCK E V V_B VLID
FNUM FRN#
ACTIVE  NONEg
STANDBY1 NONE
PARALLEL
FILE      STATE VOLUME  BLOCK E V V_B VLID
FNUM FRN#
                NONE
REGULAR VOLUME(S)
```

```
VOL# VOLNAME STATE IOC CARD VOL FSEG ROOM
VLID FILES
REGULAR SPACE
```

If the state of the recording volumes for the billing system has	Do
no volumes allocated, as indicated by the word NONE under the state header on the MAP display	<a href="#">step 94</a>
any volume is IN ERROR, as indicated under the REGULAR VOLUME(S) header on the MAP display	<a href="#">step 93</a>
all volumes are READY, as indicated under the REGULAR VOLUME(S) header on the MAP display	<a href="#">step 95</a>

**Note:** Different billing systems than automatic message accounting (AMA) or additional billing system, can be in your office configuration. Call your next level of support to determine if other billing systems are in your office, and if you require recovery action.

- 93** To reset any volumes that are IN ERROR, type:

```
>RSETVOL vol_name
```

and press the enter key.

where

vol\_name is the name of the volume to reset

If the volumes reset has	Do
passed	<a href="#">step 95</a>
failed	<a href="#">step 111</a>

- 94** Perform the procedure, "Allocating recording volumes in the DIRP utility" in *Routine Maintenance Procedures*, 297-8001-546 (North American market) or 297-9051-546 (International market). When you complete the procedure, return to this point.
- 95** To determine the state of the DLOG recording volumes, type:

```
>QUERY DLOG ALL
```

and press the enter key.

*Example of a MAP response*

```
SSNAME SSNO SEQNO ROTATES POOLNO PARLPOOL
EMERGENCY
DLOG 2 1 102 10 NONE
***YES***
```

```

.
REGULAR
FILE(S) STATE VOLUME RECCOUNT BLOCK E V V_B VLID
FNUM FRN#
ACTIVE AVAIL S01DDLOG      6      6  0 22 NO 8447
0013 204D
STANDBY1 AVAIL S00DDLOG     0      0  0 23 NO 8408
0014 309B
.
REGULAR VOLUME(S)
VOL# VOLNAME STATE      IOC CARD VOL FSEG ROOM
VLID FILES
    22 S01DDLOG READY      N/A N/A  7   5  18
8447 A
    23 S00DDLOG READY      N/A N/A  8   4  18
8408 S1
REGULAR SPACE
VOL# VOLNAME STATE      SEGS  EXP UNEXP TOTAL
    22 S01DDLOG READY      5    13   0    18
    23 S00DDLOG READY      4    14   0    18

```

If the state of DLOG recording volumes is	Do
no allocated volumes, as indicated by the word NONE under the state header on the MAP display	<a href="#">step 97</a>
any volume is IN ERROR, as indicated under the REGULAR VOLUME(S) header on the MAP display	<a href="#">step 96</a>
all volumes are READY, as indicated under the REGULAR VOLUME(S) header on the MAP display	<a href="#">step 98</a>

**Note:** Different billing systems than automatic message accounting (AMA) or additional billing system, can be in your office configuration. Call your next level of support to determine if other billing systems are in your office, and if you require recovery action.

- 96** To reset any volumes that are IN ERROR, type:
- ```
>RSETVOL vol_name
```
- and press the enter key.
- where

vol\_name is the name of the volume to reset

| If the volumes reset has | Do                       |
|--------------------------|--------------------------|
| passed                   | <a href="#">step 98</a>  |
| failed                   | <a href="#">step 111</a> |

- 97** Perform the procedure, “Allocating recording volumes in the DIRP utility” in *Routine Maintenance Procedures*, 297-8001-546 (North American market) or 297-9051-546 (International market). When you complete the procedure, return to this point.
- 98** Determine from your next level of support if you need to recover other DIRP systems (for example, JF, OM).

| If you need to recover other DIRP systems | Do                       |
|-------------------------------------------|--------------------------|
| yes                                       | <a href="#">step 99</a>  |
| no                                        | <a href="#">step 103</a> |

- 99** Perform the correct procedures in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market). When you complete the procedures, return to this point.

- 100** To determine if DIRP logs generated, type:  
**>LOGUTIL;OPEN DIRP**  
 and press the enter key.

| If DIRP log generated | Do                       |
|-----------------------|--------------------------|
| yes                   | <a href="#">step 101</a> |
| no                    | <a href="#">step 103</a> |

- 101** Refer to the *Log Report Reference Manual*, 297-8001-840 (North American market) or 297-9051-840 (International market), and take the correct action.  
 When you complete the log report activities, return to this point.

- 102** To turn off priority, type:  
**>PRIORITY OFF**  
 and press the enter key.

- 103** To access the SRSTATUS level of the MAP display, type:  
**>MAPCI;MTC;SRSTATUS**  
 and press the enter key.

*Example of a MAP response*

```

SRSTATUS
0 Quit  OVERALL STATUS  Pend: 0%  Inprg: 0%
Comp: 100%  Fail: 0%
2 View_  View: SYSTEM
14:08:30
3 List_          Pend  InPrgr  Comp  Fail      Pend
InPrgr Comp Fail
4          MS      0      0      2      0      IOD
5  5      30      2
5          NET      0      0      6      0      Other
21  3      13      3
6          SER1     0      0      41     0
7          SER2     0      0      39     0
8          SER3     0      0      37     0
9
10         MTC :
11         STATUS:

```

**104** Determine the status of the switch recovery.**If the status of the switch recovery is****Do**

any Series III PMs that failed recovery

[step 105](#)

any Series I or II PMs that failed recovery

[step 107](#)

any IODs or other devices and services that failed recovery

[step 110](#)

that the system has completely recovered

[step 112](#)

**105** To manually recover the PMs, perform the procedure, "Recovering Link Peripheral Processors" in *Recovery Procedures*, 297-8001-545 (North American market) or 297-9051-545 (International market).

When you complete the procedure, return to this point.

**106** Go to step [103](#).

**107** Determine from office records or other office personnel which PMs you can recover first.

**108** To manually recover the PMs in the required order perform the correct alarm clearing procedures in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).



When you complete the procedure, return to this point.

- 109** Go to [step 103](#).
- 110** To manually recover IODs and other devices and services, perform the correct procedure in this document. Also you can refer to your site-related operating procedures.
- 111** For additional help, call the personnel responsible for the next level of support.
- 112** You have completed this procedure.

















---

## Performing a partial power down recovery of the XA-Core

---

### Application

Use this procedure to return to normal operation an eXtended Architecture Core (XA-Core) configuration of a switch. The switch is a DMS SuperNode or a DMS SuperNode SE switch. Use this procedure after having performed all parts of the procedure 'Emergency power conservation shutdown' to maintain emergency backup power. The procedure 'Emergency power conservation shutdown' follows an extended commercial power outage.

This procedure describes equipment recovery in decreasing order based on its effect on system reliability. The equipment restoration begins with more required equipment and ends with less required equipment such as maintenance trunk modules. The configuration of your office and the requirements of your operating company, can change the order of equipment restoration. The return of elements of the switch to service can be in a different order.

### Prerequisites

None

### Action

#### Emergency power conservation restoration

**WARNING****Potential extended equipment outage**

Nortel Networks recommends that you perform this procedure under the supervision of Emergency Technical Assistance Services (ETAS) of Nortel Networks. Also call your next level of support before you perform this procedure.

**CAUTION****Potential loss of service or extended outage**

This procedure is only to restore normal operation after the performance of measures for emergency power conservation. Do not use this procedure or parts of this procedure for equipment maintenance purposes.

**At your current location**

- 1 Use office records to identify and record the power converters which supply the MAPs and printers of the switch.
- 2 Restore power to all the power converters identified in step [1](#) that supply power to the MAPs and printers of the switch.

**At the MAP**

- 3 Restore power to one side of the remote oscillator shelf (NT3X9507), if you turned off power to save emergency backup power. To restore power, perform the procedure 'Restoring the remote oscillator shelf to duplex operation' in *Recovery Procedures*, 297-8021-545.
- 4 Restore power to one message switch (MS) shelf if you turned off power to save emergency backup power. To restore power, perform the procedure 'Restoring the MS duplex operation' in *Recovery Procedures*, 297-8021-545.
- 5 Restore power to one unit of the CCS7 message switch and buffer (MSB7) if you turned off power to save emergency backup power. To restore power, perform the procedure 'Restoring the MSB7 to duplex operation' in *Recovery Procedures*, 297-8021-545.
- 6 Restore power to one link interface module (LIM) unit on one or more link peripheral processors (LPP) if you turned off power to save emergency backup power. To restore power, perform the procedure 'Restoring LPP LIMs to duplex operation' in *Recovery Procedures*, 297-8021-545.
- 7 If you removed power from one or more network frames, restore power to the changed frames at the power distribution center (PDC).
- 8 Restore power to one or more junctored network (JNET) shelves if you turned off power to save emergency backup power. To restore power, perform the procedure 'Restoring the junctored network to duplex operation' in *Recovery Procedures*, 297-8021-545.
- 9 Restore power to one or more enhanced network (ENET) shelves if you turned off power to save emergency backup power. To restore power, perform the procedure 'Restoring the enhanced network to duplex operation' in *Recovery Procedures*, 297-8021-545.
- 10 Restore power to one or more units of a line group controller (LGC), line trunk controller (LTC), or digital trunk controller (DTC). Restore power if you turned off power to save emergency backup power. To restore power, perform the procedure

- 'Restoring LGCs, LTCs, and DTCs to duplex operation' in *Recovery Procedures, 297-8021-545*.
- 11** Restore power to one or more units of a line concentrating module (LCM) if you turned off power to save emergency backup power. To restore power, perform the procedure 'Restoring LCMs to duplex operation' in *Recovery Procedures, 297-8021-545*.
  - 12** Restore power to one or more line modules (LM) if you turned off power to save emergency backup power. To restore power, perform the procedure 'Restoring line modules to duplex operation' in *Recovery Procedures, 297-8021-545*.
  - 13** Restore power to one or more maintenance trunk modules (MTM) if you turned off power to save emergency backup power. To restore power, perform the procedure 'Returning maintenance trunk modules to service' in *Recovery Procedures, 297-8021-545*.
  - 14** To clear any alarms on the MAP display, perform the correct alarm clearing procedure. The correct alarm clearing procedure is in this document or in the *Alarm and Performance Monitoring Procedures, 297-8021-543*.
  - 15** You have completed this procedure.







---

## Powering up the Message Switch

---

### Application

Use this procedure to power up the Message Switch (MS) when recovering from a power outage.

### Action

#### Powering up the MS

##### *At the XA-Core frame*

- 1 Locate the NT9X31 and NT9X30 power converters for message switch 0 (MS 0) in slots 33F and 36F on the MS 0 shelf.
- 2 Turn on the NT9X31 and NT9X30 power converters in slots 33F and 36F of the MS 0 shelf at the same time. Lift and release the power switches located on the faceplates of the converters.
- 3 Locate the NT9X31 and NT9X30 power converters for MS 0 in slots 1F and 4F on the MS 0 shelf.
- 4 Turn on the NT9X31 and NT9X30 power converters in slots 1F and 4F of the MS 0 shelf at the same time. Lift and release the power switches located on the faceplates of the converters.
- 5 Locate the NT9X31 and NT9X30 power converters for message switch 1 (MS 1) in slots 33F and 36F on the MS 1 shelf.
- 6 Turn on the NT9X31 and NT9X30 power converters in slots 33F and 36F of the MS 1 shelf at the same time. Lift and release the power switches located on the faceplates of the converters.
- 7 Locate the NT9X31 and NT9X30 power converters for MS 1 in slots 1F and 4F on the MS 01shelf.
- 8 Turn on the NT9X31 and NT9X30 power converters in slots 1F and 4F of the MS 1 shelf at the same time. Lift and release the power switches located on the faceplates of the converters.

##### *At the MAP terminal*

- 9 To access the SRSTATUS level of the MAP, type:

```
>MAPCI;MTC;SRSTATUS
```

and press the enter key.

*Example of a MAP response*

```
SRSTATUS
0 Quit  OVERALL STATUS  Pend: 0%  Inprg: 0%
Comp: 100%  Fail: 0%
```

```

2 View_ View: SYSTEM
14:08:30
3 List_ Pend InPrg Comp Fail Pend
InPrg Comp Fail
4 MS 0 0 2 0 IOD
5 5 30 2
5 NET 0 0 6 0 Other
21 3 13 3
6 SER1 0 41 0 0
7 SER2 0 39 0 0
8 SER3 0 37 0 0
9
10 MTC:
11 STATUS:

```

**10** Determine the recovery status of the MSs.

**Note:** MS recovery status displays to the right of the word 'MS' in the MAP display. Recovery status for each MS can be one of pending, in progress, complete, or failed.

| If the recovery status is                                | Do                      |
|----------------------------------------------------------|-------------------------|
| either MS failed recovery                                | <a href="#">step 15</a> |
| either MS continues to have pending recovery             | <a href="#">step 11</a> |
| another status different from failed or pending recovery | <a href="#">step 12</a> |

**11** Wait until both MSs are either in recovery development or have completed recovery.

When neither MS continues to have pending recovery, go to step [10](#)

**12** To access the MS Clock level of the MAP display, type:

**>MAPCI;MTC;MS;CLOCK**

and press the enter key.

**13** To synchronize the clocks, type:

**>SYNC**

and press the enter key.

| If the SYNC command is | Do                      |
|------------------------|-------------------------|
| successful             | <a href="#">step 16</a> |
| failed                 | <a href="#">step 14</a> |



- 14** Record the reason for synchronization failure, as shown in the MAP response. Repeat the try to synchronize the MS clocks later, after networks and PMs are in service.
- 15** For additional help, call the personnel responsible for the next level of support.
- 16** You have completed this procedure.







## Powering up the Enhanced Network

### Application

Use this procedure to manually power up the enhanced network (ENET) in the event of a power failure.

### Action

#### Powering up the ENET

##### *At the ENET frames*

- 1 Locate the NT9X31 power converters in slots 1F and 33F on the ENET shelves.
- 2 To turn on the NT9X31 power converters lift and release the power switches located on the faceplates of the converters.
- 3 Locate the NT9X30 power converters in slots 4F and 36F on the ENET shelves.
- 4 Turn on the NT9X30 power converters lift and release the power switches located on the faceplates of the converters.
- 5 Determine if all the converters have power. Power is indicated by all the Converter Off lights going off.

| If all the power converters have | Do                     |
|----------------------------------|------------------------|
| power                            | <a href="#">step 7</a> |
| not power                        | <a href="#">step 6</a> |

- 6 To power up the ENET frame perform the procedure, '*Clearing an Ext FSP DPCC cabinet major alarm*' in the document, *Alarm and Performance Monitoring Procedures, 297-8021-543*.  
When you complete the procedure, return to this point.

##### *At the MAP terminal*

- 7 To access the SRSTATUS level of the MAP display, type:  
**>MAPCI;MTC;SRSTATUS**  
and press the enter key.

*Example of a MAP response*

```
SRSTATUS
0 Quit  OVERALL STATUS  Pend: 0%  Inprg: 0%
Comp: 100%  Fail: 0%
```

```

2 View_ View: SYSTEM
14:08:30
3 List_ Pend InPrg Comp Fail Pend
InPrg Comp Fail
4 MS 0 0 2 0 IOD
5 5 30 2
5 NET 0 0 6 0 Other
21 3 13 3
6 SER1 0 41 0 0
7 SER2 0 39 0 0
8 SER3 0 37 0 0
9
10 MTC:
11 STATUS:

```

- 8** From the MAP display, determine the recovery status of the network.

**Note:** Network recovery status displays to the right of the word 'NET' in the MAP display. Recovery status can be one of pending, in progress, complete, or failed.

| If the status of any network element is | Do                      |
|-----------------------------------------|-------------------------|
| failed                                  | <a href="#">step 11</a> |
| pending                                 | <a href="#">step 9</a>  |
| another status                          | <a href="#">step 13</a> |

- 9** Continue when there are no network elements that continue to be pending recovery.
- 10** Go to [step 8](#).
- 11** To manually recover the ENET perform the procedure, 'Recovering the Enhanced Network' in Recovery Procedures, 297-8021-545.
- 12** Go to [step 7](#).
- 13** You have completed this procedure.





























---

## Powering up a Ethernet Routing Switch 8600

---

### Purpose of this procedure

Use the following procedure to power up a Ethernet Routing Switch 8600.

### When to use this procedure

Use this procedure when it is necessary to power up a Ethernet Routing Switch 8600.

### Prerequisites

None

### Action

#### Powering up a Ethernet Routing Switch 8600

##### *At the Ethernet Routing Switch 8600 frame*

- 1 Turn the DC input power source on or reset the power source circuit breaker to provide power to the power supply.
- 2 Turn the power supply switch for all three DC power supplies to the on position.

**Note:** You must turn on two of the power supply units within 2 seconds of each other. If you wait longer to turn on the second power supply, one of the power supplies could shut down. To correct this condition, turn off both power supplies, wait at least 30 seconds, and then turn on both power supplies again within 2 seconds.

- 3 You have completed this procedure.



## Performing a partial power down recovery of the Ethernet Routing Switch 8600

---

### Purpose

This procedure is used to perform a partial power down recovery of an Ethernet Routing Switch 8600.

### Prerequisites

None

### Action

#### Performing a partial power down recovery of the Ethernet Routing Switch 8600

##### *At the chassis*

- 1 Turn the DC input power source on, or reset the power source circuit breaker to provide power to the power supply.
- 2 Turn the power supply switch to the on position.
- 3 You have completed this procedure.



## Powering up the Link Peripheral Processors

### Application

Use this procedure to power up the Link Peripheral Processors (LPP) or fiberized LPPs (FLPPs) in the event of a power failure.

**Note:** Throughout this procedure, LPP is used to refer to both the LPP and FLPP.

### Action

#### Recovering LPPs

##### At the PDC

- Determine if PDC has power restored to the LPP(s).

| If PDC has                     | Do                     |
|--------------------------------|------------------------|
| power restored to the LPPs     | <a href="#">step 5</a> |
| not power restored to the LPPs | <a href="#">step 2</a> |

- Check the PDC fuses that supply the LPP.

| If there are           | Do                     |
|------------------------|------------------------|
| blown fuses            | <a href="#">step 3</a> |
| no blown fuses visible | <a href="#">step 4</a> |

- Replace the blown fuses.

**Note:** If fuses blow repeatedly, call your next level of support for help.

When PDC power restores to the LPPs, continue this procedure at [step 5](#).

- Call the personnel responsible for maintaining power at your site, or refer to your next level of support for help.

When PDC power restores to the LPPs, continue this procedure at [step 5](#).

- Locate the LPPs for recovery.

**At the LPP cabinet**

6

**WARNING****Static electricity damage**

Wear a wrist strap connected to the wrist-strap grounding point of a frame supervisory panel (FSP). Also a wrist strap can connect to a modular supervisory panel (MSP). Wear a wrist strap when handling circuit cards. A wrist strap protects the cards against damage caused by static electricity.

Locate the NT9X74 cards in all link interface shelves (LIS).

**Note:** NT9X74 cards are in shelf position 7F and 32F on all LISs.

- 7 To unseat each NT9X74 card, release the locking levers and carefully pull the card towards you about 25 mm (1 in.).
- 8 Locate the NT9X30 power converters in slots 4F and 36F of the link interface module (LIM) unit shelf.
- 9 To turn on the power converters of the LIM unit shelf, toggle the switch each NT9X30 card.
- 10 Locate the NT9X30 or NTDX16 power converters for each LIS.
 

**Note:** NT9X30 power converters are in slots 4F and 36F for each LIS. NTDX16 power converters can be in slots 1F, 4F, 33F, and 36F for each LIS.
- 11 To turn on the LIS power converters, toggle the switch on each NT9X30 or NTDX16 card.
- 12 Determine if all the power converters turned on power correctly. All the CONVERTER OFF lights go off when power turns on correctly.

| If all the CONVERTER OFF lights are | Do                      |
|-------------------------------------|-------------------------|
| off                                 | <a href="#">step 15</a> |
| not off                             | <a href="#">step 13</a> |

- 13 To power up the frame, perform the procedure, 'Clearing an Ext FSP LPP cabinet major alarm' in *Alarm Clearing and Performance Monitoring Procedures*, 297-8001-543 (North American market) or 297-9051-543 (International market).



When you complete the procedure, return to this point.

- 14 Go to [step 8](#).
- 15 Put in position all NT9X74 cards as follows:
  - Carefully slide each NT9X74 card back into the LIS.
  - Push on the upper and lower edges of each faceplate. Make sure that the card is completely in the slot of the shelf.
  - Close the locking levers on each card.

- 16 Repeat steps [5](#) through [15](#) for each LPP in your office.

When power restores to all LPPs, continue this procedure at step [17](#).

- 17 To access the SRSTATUS level of the MAP display, type:

**>MAPCI;MTC;SRSTATUS**

and pressing the Enter key.

*Example of a MAP response*

```
SRSTATUS
0 Quit OVERALL STATUS Pend: 0% Inprg: 0%
Comp: 100% Fail: 0%
2 View_ View: SYSTEM
14:08:30
3 List_ Pend InPrg Comp Fail Pend
InPrg Comp Fail
4 MS 0 0 2 0 IOD
5 5 30 2
5 NET 0 0 6 0 Other
21 3 13 3
6 SER1 0 41 0 0
7 SER2 0 39 0 0
8 SER3 0 37 0 0
9
10 MTC:
11 STATUS:
```

- 18 From the MAP display, determine the recovery status of the Series III PMs.

**Note:** Series III PM recovery status displays to the right of the word 'SER3' in the MAP display. Recovery status can be one of pending, in progress, complete, or failed.

| If the Series 3 PMs are | Do                      |
|-------------------------|-------------------------|
| zero                    | <a href="#">step 20</a> |

| If the Series 3 PMs are | Do                      |
|-------------------------|-------------------------|
| not zero                | <a href="#">step 19</a> |

- 19** To manually recover the PMs, perform the procedure, 'Recovering Link Peripheral Processors' in *Recovery Procedures*, 297-8021-545.
- When you complete the procedure, return to this point.
- 20** You have completed this procedure.





































---

## Powering up the SDM

---

### Purpose of this procedure

Use the following procedure to power up the SuperNode Data Manager (SDM) that houses the CS 2000 Core Manager.

### When to use this procedure

Use this procedure when it is necessary to power up the SDM hardware.

### Prerequisites

None

### Action

#### Powering up the SDM

##### *At the SDM frame*

- 1 Turn on the two top breakers at the top of the SDM frame.
- 2 Wait a few moments until the green lights on each card are steady.

##### *At the VT100 terminal*

- 3 Login as root and type  
`# sdmmtc`  
and press the Enter key.
- 4 Verify that all hardware is in service.
- 5 Verify that rootvg and datavg logical volumes are mirrored at the storage level.

**Note:** There will likely be alarms at the connection and application levels. The general status of the SDM will be in-service trouble (IsTb).

- 6 You have completed this procedure.



---

## Powering up a T1400 or N240 server

---

### Purpose of this procedure

Use the following procedure to power up a Netra™ T1400 or N240 server. Powering up the N240 server will, in turn, supply power for the following applications:

- IEMS
- Core and Billing Manager
- CS 2000 Management Tools applications
- MG 9000 Manager

### When to use this procedure

Use this procedure when it is necessary to power up the Netra™ T1400 or duplex N240 servers.

### Prerequisites

None

### Action

#### Powering up a Netra™ T1400 or N240 server

- 1** To bring the T1400 server into service, turn on the circuit breakers. The T1400 should recover on its own.
- 2** To bring the duplex N240 servers into service, turn on the circuit breakers. To help with recovery, turn the power on to what was the active server first. If there is no record of this, turn on the Unit 0 server before the Unit 1 server.  
  
Once power is restored to the server they will recover on their own.
- 3** You have completed this procedure.



---

## Performing a partial power up of the N240 server

---

### Purpose

This procedure is used to perform a partial power down recovery of the N240 servers. The N240 servers are commissioned with one active and one inactive unit. In a partial power down, the inactive unit is powered down, while the active unit remains powered up. This procedure powers up the inactive unit.

### Prerequisites

You must have the root user password for the N240.

You need to IP address for the inactive unit.

### Action

#### Performing a partial power down recovery of the N240 servers

##### *At the N240 server*

- 1 To bring the inactive N240 server into service, turn on the circuit breakers. The server should recover on its own and start syncing with the active server.
- 2 You have completed this procedure.





---

## Powering up the Border Control Point Manager

---

### Purpose of this procedure

Use the following procedure to power up the Border Control Point Manager. The Border Control Point Manager is installed on a Sun Netra 240 (N240).

### When to use this procedure

Use this procedure when it is necessary to power up the Sun N240 server that houses the Border Control Point Manager.

### Prerequisites

None

### Action

#### Powering up the Border Control Point Manager

##### *At the frame housing the Border Control Point Manager*

- 1 For DC powered shelves, switch the circuit breakers at the EBIP that provide power to the servers being powered to the ON position. The breaker will have the 'I' side (top) of the breaker depressed.  
**Note:** The DC powered N240 does not have a Power ON/OFF switch and can only be powered ON/OFF from the breaker at the EBIP.
- 2 For AC powered shelves, push the rocker located on the top of the AC outlet to apply power to the servers. It should be switched to the "I" position.
- 3 Once the breakers are switched ON at the power source, power up the servers by switching the breakers on the back of the chassis to the ON position.
- 4 Verify the system is powered up correctly by observing the LEDs on the front of the N240.
- 5 You have completed this procedure.



---

## Powering up the SAMF frame

---

### Purpose of this procedure

Use the following procedure to power up the SAMF frame. Powering up the SAMF frame allows the SAM21 hardware cards, the Policy Controller unit, and the Session Server unit to return to service.

### When to use this procedure

Use this procedure when it is necessary to power up the SAMF frame.

### Prerequisites

None

### Action

#### Powering up the SAMF frame

##### *At the SAMF frame*

- 1 Power up the SAMF BIP breakers. At the top of the cabinet, turn on the breakers that supply power to the two SAM21 shelves and the Session Server (if equipped).

##### *At the CS 2000 SAM21 Manager*

- 2 If necessary, unlock the previously active Shelf Controller (SC). Refer to [Unlocking a SAM21 Shelf Controller on page 405](#).
- 3 If necessary, unlock the previously inactive SC. Refer to [Unlocking a SAM21 Shelf Controller on page 405](#).
- 4 If necessary, unlock any remaining locked cards on the SAM21 other than the GWC cards.

##### *At the CS 2000 GWC Manager*

- 5 If necessary, unlock all previously active GWC cards. Refer to [Unlock a GWC card on page 551](#).
- 6 If necessary, unlock all previously inactive GWC cards. Refer to [Unlock a GWC card on page 551](#).

##### *At the Policy Controller unit*

- 7 Determine which physical or logical unit you want to become active and power that unit up first by executing procedure [Power-On and boot a Policy Controller unit on page 533](#).

- 8 Once the active unit has begun call processing, power up the mate unit by executing procedure [Power-On and boot a Policy Controller unit on page 533](#).

***At the Session Server unit***

- 9 Determine which physical or logical unit you want to become active and power that unit up first by executing procedure [Power-On and boot a Session Server - Trunks unit on page 535](#).
- 10 Log onto the active unit to monitor the status of the SIP Gateway application using procedure [View the operational status of the SIP Gateway application on page 537](#). Verify that the Administrative state of the SIP Gateway application becomes Unlocked and the Operational state becomes Enabled.  
  
If the active unit comes up in any state other than Unlocked:Enabled, refer to Session Server Security and Administration, NN10346-611, and complete one or both of the following procedures:
  - complete procedure Unsuspend the SIP gateway application
  - complete procedure Unlock the SIP gateway application
- 11 Once the active unit has begun call processing, power up the mate unit by executing procedure [Power-On and boot a Session Server - Trunks unit on page 535](#).
- 12 From the active unit, verify that the SIP Gateway application databases on the both units have synchronized using procedure [Verify synchronization status on page 543](#)
- 13 Monitor the system for an appropriate period per your site guidelines.  
  
If you experience problems with call processing, refer to Session Server Security and Administration, NN10346-611, and perform the following tasks in order:
  - complete procedure Invoke a maintenance SwAct of the Session Server platform
  - complete procedure Inhibit a system SwAct (Jam)
  - contact your next level of support or Nortel GNPS
- 14 The procedure is complete.

## Power-On and boot a Policy Controller unit

### Purpose of this procedure

This procedure is used to power on a Policy Controller unit that has been installed as a replacement, or was shutdown for any other reason.

This procedure may be used as a standalone task or as part of a higher level activity such as part of a dead office recovery activity or software upgrade activity.

### Limitations and restrictions

There are no restrictions on using this procedure.

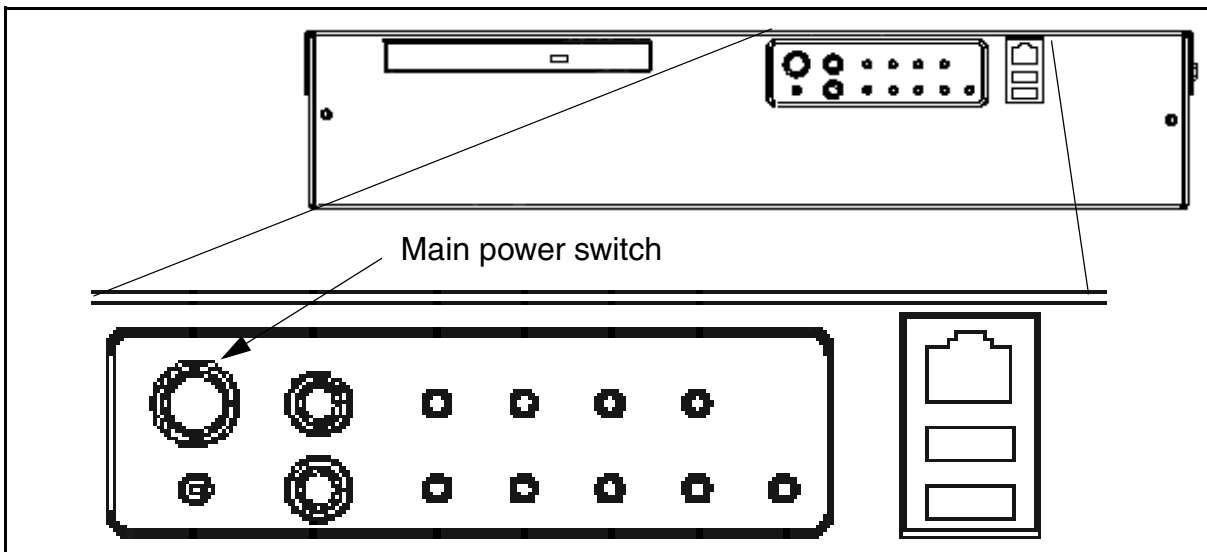
### Prerequisites

If the unit was a replacement unit recently installed, ensure that all power cabling connections have been properly installed and secured at the rear of the chassis and SAM-F frame.

### Action

#### *At the front panel of the Policy Controller unit*

- 1 If necessary, power on the Policy Controller using the main power switch located on the front panel.



- 2 If desired, at the Policy Controller console, monitor the boot progress of the unit.
- 3 The procedure is complete.



## Power-On and boot a Session Server - Trunks unit

### Purpose of this procedure

This procedure is used to power on a Session Server - Trunks unit that has been installed as a replacement, or was shutdown for any other reason.

This procedure may be used as a standalone task or as part of a higher level activity such as part of a dead office recovery activity or software upgrade activity.

### Limitations and restrictions

There are no restrictions on using this procedure.

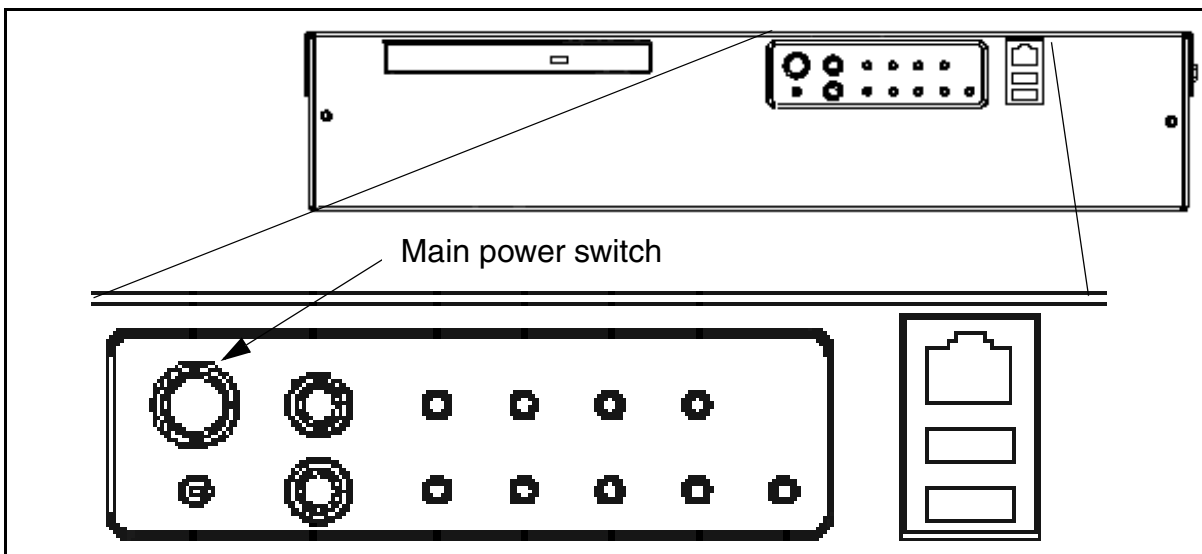
### Prerequisites

If the unit was a replacement unit recently installed, ensure that all power cabling connections have been properly installed and secured at the rear of the chassis and SAM-F frame.

### Action

#### *At the front panel of the Session Server - Trunks unit*

- 1 If necessary, power on the Session Server - Trunks using the main power switch located on the front panel.



- 2 If desired, at the Session Server - Trunks console, monitor the boot progress of the unit.
- 3 The procedure is complete.





## View the operational status of the SIP Gateway application

### Purpose of this procedure

Use the following procedure to view the service status of the SIP Gateway application.

### Limitations and restrictions

This procedure provides instructions for determining the service status of the SIP Gateway application software only. For instructions on determining the status of the platform and operating system, refer to procedure [View the operational status of the NCGL platform on page 375](#).

### Prerequisites

There are no prerequisites for this procedure.

### Action

#### ***At the CS 2000 Session Server Manager or IEMS client***

- 1 Select Succession Communication Server 2000 Session Server Manager from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- [Succession Communication Server 2000 NCGL Platform Manager](#)
- [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.



### 3 Monitor the status of the SIP Gateway application from this view:

| Session Server Status - Connected to Unit #1 |                |                   |
|----------------------------------------------|----------------|-------------------|
| Unit Number                                  | Activity State | Operational State |
| 0                                            | Inactive       | Enabled           |
| 1                                            | Active         | Enabled           |

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                                                                                                  |                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Administrative                                                                                                           | Control                                                                            |
| <input type="button" value="Lock"/><br><input type="button" value="UnLock"/><br><input type="button" value="Shut Down"/> | <input type="button" value="Suspend"/><br><input type="button" value="UnSuspend"/> |

|                                   |
|-----------------------------------|
| Last Performed Operation: Refresh |
| Result: Passed                    |

This page updates automatically every 10 seconds!  
 Last update: Thu Jun 10 13:04:20 EDT 2004

**Note:** This view is refreshed according to the value shown in the drop down box at the bottom of the status panel. To increase or decrease the refresh rate, select a different value from the drop down menu and click the Refresh Rate button or manually refresh the page by clicking the Refresh button.

- 4 Refer to section [Interpreting SIP Gateway application status and maintenance fields on page 539](#) to review the description of the various fields of this view.
 

**Note:** For more detailed information about SIP Gateway application services states and administrative functions, refer to the Overview section “Interpreting SIP Gateway application states” in *Session Server - Trunks Security and Administration*, NN10346-611.
- 5 The following service affecting actions are available:
  - Lock the SIP Gateway application
  - Unlock the SIP Gateway application
  - Suspend the SIP Gateway application
  - Unsuspend the SIP Gateway application
  - Cold SwAct the SIP Gateway application
- 6 To view the number of active calls currently being handled by the application and the synchronization status of the units, click QueryInfo.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| SIP Gateway is: In Sync                         |
| SIP Gateway Cold SwAct                          |

- 7 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Interpreting SIP Gateway application status and maintenance fields

Use the following table to assist you in interpreting information displayed in the Status area:

| Field                      | Description                                                                          |
|----------------------------|--------------------------------------------------------------------------------------|
| Unit Connection Status Bar | Indicates which unit in the node the CS 2000 Session Server Manager is connected to. |
| Unit Number                | Identifies the two units in the node, labeled 0 and 1.                               |

| Field             | Description                                                                                                                                                                                                     |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Activity State    | Indicates which unit is Active and which is Inactive (standby). Also acts as an indirect indicator of fault-tolerant status; when both units have an Operational status of Enabled, the node is fault-tolerant. |
| Operational State | Indicates the service status of each unit, Enabled or Disabled.                                                                                                                                                 |

Use the following table to assist you in interpreting information displayed in the SIP Gateway status area:

| Field                | Indication                        |
|----------------------|-----------------------------------|
| Administrative State | Locked, Unlocked, or ShuttingDown |
| Operational State    | Enabled or Disabled               |
| Procedural Status    | Terminating or -                  |
| Control Status       | Suspended or -                    |

Use the following table to assist you in interpreting the SIP Gateway area's CCITT X.731-style and related DMS-style status indicators:

| Administrative State | Operational State | Procedural Status | Control Status | DMS style Service States          |
|----------------------|-------------------|-------------------|----------------|-----------------------------------|
| Locked               | Disabled          | -                 | Suspended      | Offline (OFFL)                    |
| Locked               | Enabled           | -                 | -              | Manual Busy (MANB)                |
| Locked               | Enabled           | Terminating       | -              | Manual Busy Transitioning (MANBP) |
| Unlocked             | Enabled           | -                 | -              | In Service (INSV)                 |
| Unlocked             | Disabled          | -                 | -              | System Busy (SYSB)                |

| <b>Administrative State</b>                       | <b>Operational State</b> | <b>Procedural Status</b> | <b>Control Status</b> | <b>DMS style Service States</b> |
|---------------------------------------------------|--------------------------|--------------------------|-----------------------|---------------------------------|
| Shutting Down                                     | Enabled                  | -                        | -                     | Going out of service (INSVD)    |
| <b>Note:</b> (-) indicates a status of in-service |                          |                          |                       |                                 |



## Verify synchronization status

### Purpose of this procedure

Use this procedure to determine the synchronization status of the two units.

### Limitations and restrictions

There are no restrictions for performing this procedure.

### Prerequisites

There are no prerequisites for performing this procedure.

### Action

#### *At the CS 2000 Session Server Manager or IEMS client*

- 1 Select **Succession Communication Server 2000 Session Server Manager** from the launch point menu.

Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

- ▣ [Succession Communication Server 2000 NCGL Platform Manager](#)
- ▣ [Succession Communication Server 2000 Session Server Manager](#)

- 2 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu:



- At the bottom of the SIP Gateway Maintenance panel, locate and click the QueryInfo button.

| SIP Gateway Status   |                   |                   |                |
|----------------------|-------------------|-------------------|----------------|
| Administrative State | Operational State | Procedural Status | Control Status |
| UnLocked             | Enabled           | -                 | -              |

| SIP Gateway Maintenance                    |                                 |
|--------------------------------------------|---------------------------------|
| Administrative                             | Control                         |
| <p>Lock</p> <p>UnLock</p> <p>Shut Down</p> | <p>Suspend</p> <p>UnSuspend</p> |
| Refresh                                    | QueryInfo                       |

- The synchronization status of the units is displayed at the bottom of the query results panel.  
If the units are not in sync, check for alarm conditions.

|                                                 |
|-------------------------------------------------|
| Last Performed Operation: Query Number of Calls |
| Result: Passed                                  |
| Number Of Active Calls: 0                       |
| SIP Gateway is: In Sync                         |
| SIP Gateway Cold SwAct                          |

- This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Powering up the Call Control Frame

### Purpose of this procedure

Use the following procedure to power up the Call Control Frame (CCF).

Powering up the CCF allows the SAM21 hardware cards and the STORM disk array to return to service.

### When to use this procedure

Use this procedure when it is necessary to power up the CCF.

### Prerequisites

None

### Action

#### Powering up the Call Control Frame

##### *At the CCF*

- 1 Determine the configuration of your CCF.

| If the CCF configuration includes                              | Do                     |
|----------------------------------------------------------------|------------------------|
| a STORM disk array and two STORM cards in the Call Agent shelf | <a href="#">step 2</a> |
| two STORM SAM-XTS units                                        | <a href="#">step 3</a> |

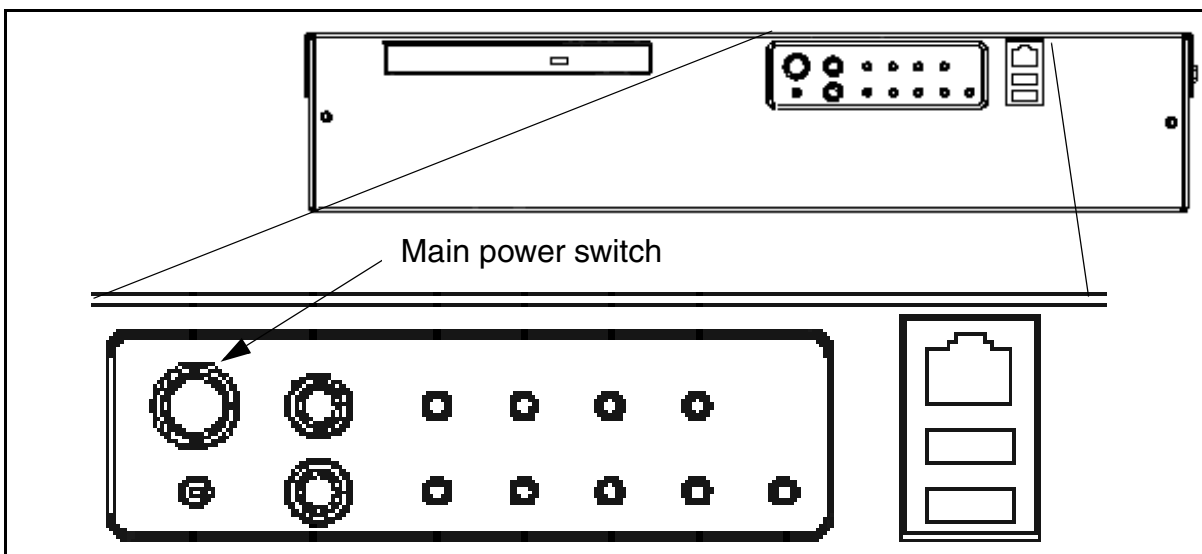
- 2 Power up the CCF BIP breakers. At the top of the cabinet, turn on the breakers that supply power to the STORM disk array and the two SAM21 shelves.

Go to [step 6](#)

- 3 Power up the CCF BIP breakers. At the top of the cabinet, turn on the breakers that supply power to the two SAM21 shelves and the STORM SAM-XTS units.

##### *At the front panel of the STORM SAM-XTS units*

- 4 If necessary, power on the STORM SAM-XTS units using the main power switch located on the front panel.



- 5 At the console, monitor the boot progress of the unit until booting is complete.

***At the CS 2000 SAM21 Manager***

- 6 If necessary, unlock the previously active Shelf Controller (SC). Refer to [Unlocking a SAM21 Shelf Controller on page 405](#).
- 7 If necessary, unlock the previously inactive SC. Refer to [Unlocking a SAM21 Shelf Controller on page 405](#).
- 8 If necessary, unlock the previously active Compact Call Agent (CCA) card. Refer to [Unlocking the Call Agent on page 549](#).
- 9 If necessary, unlock the previously inactive CCA card. Refer to [Unlocking the Call Agent on page 549](#).
- 10 If necessary, unlock the previously active USP-lite card.
- 11 If necessary, unlock the previously inactive USP-lite card.
- 12 If necessary, unlock any remaining locked cards on the SAM21 other than the GWC cards.

***At the CS 2000 GWC Manager***

- 13 If necessary, unlock all previously active GWC cards. Refer to [Unlock a GWC card on page 551](#).
- 14 If necessary, unlock all previously inactive GWC cards.

Refer to [Unlock a GWC card on page 551](#).

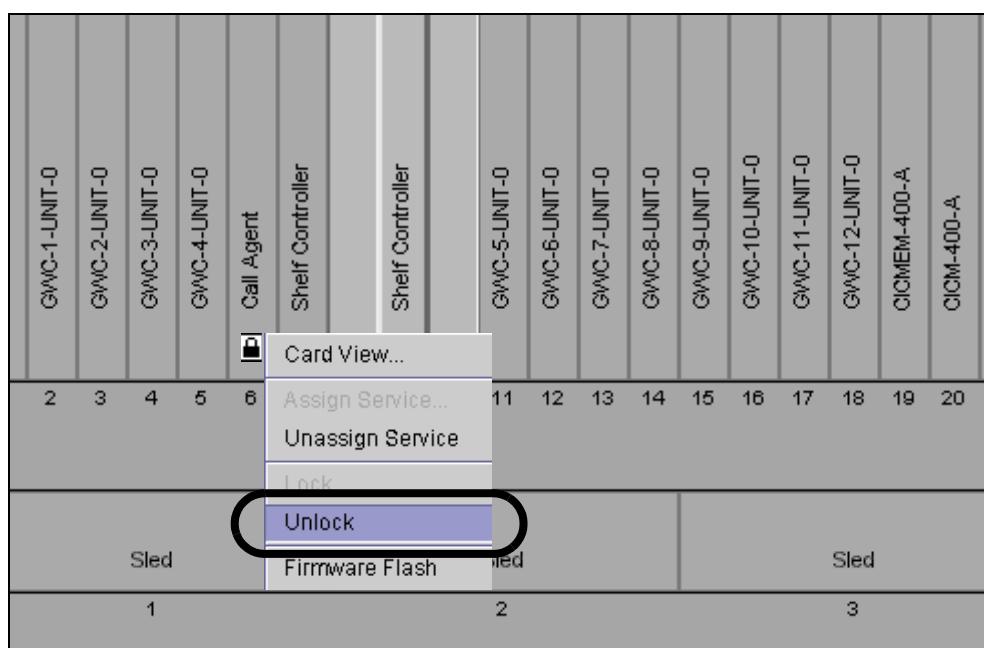
- 15** You have completed this procedure.



## Unlocking the Call Agent

### At the CS 2000 SAM21 Manager client

- 1 From the Shelf View, right click on the card and select Unlock from the context menu.



**Note:** Unlock is also available from the States tab of the Card View window.

The card resets, downloads software, and reboots.

- 2 Wait for the lock icon to disappear.  
**Note:** Do not perform any patching activities on the Call Agent until ten minutes have passed.
- 3 This procedure is complete.



---

## Unlock a GWC card

---

### Purpose of this procedure

This procedure initiates a reboot of the GWC card causing the card to download its software from the CS 2000 Core Manager and to restart its call processing services and applications software.

### When to use this procedure

Use this procedure:

- after replacing a GWC card.
- as part of a fault clearing activity.
- when a new software load is available.
- when you have completed reprovisioning a GWC card or GWC node (a node is made up of unit 0 and unit 1 GWC cards) and you would like the card or node to begin using the new provisioning values.
- when you have applied or removed a patch to the GWC software using the Network Patch Manager (NPM) and have saved a new GWC software image to the CS 2000 Core Manager.

**Note:** For more information about upgrading or patching GWC software, refer to the *Upgrading the Gateway Controller* NTP, NN10196-461.

### Prerequisites

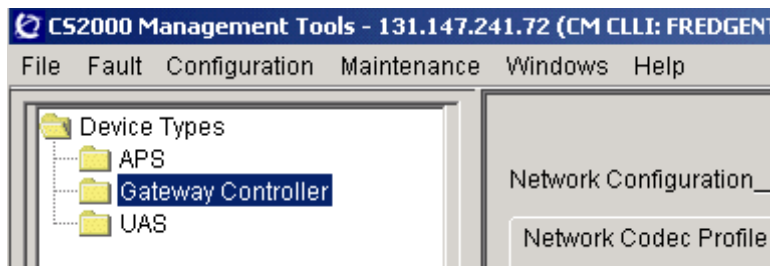
The GWC card must be locked. The procedure [Lock a GWC card on page 407](#) in this NTP provides instruction on how to lock a GWC card.

If the IP addresses for the card that you want to unlock and its mate are not contiguous, you will not be able to unlock the card. You must correct these addresses using procedure “Manually re-provision GWC cards” in the *Gateway Controller Configuration Management*, NN10205-511 before attempting to unlock the card.

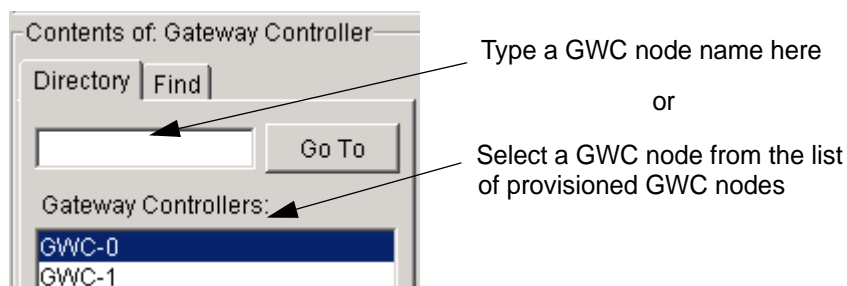
### Action

#### **At the CS 2000 GWC Manager client**

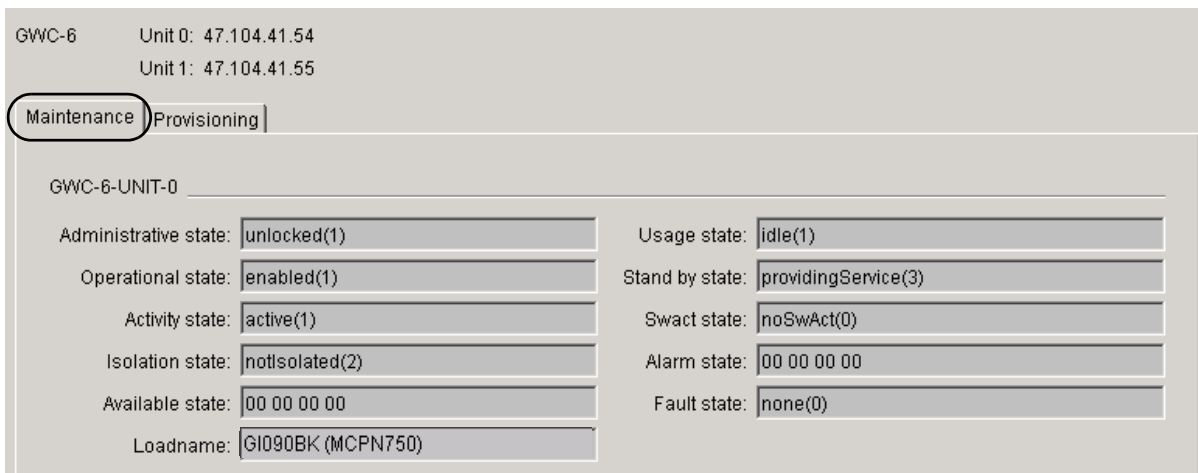
- 1 At the CS 2000 Management Tools window, click the *Gateway Controller* folder from the Device Types directory tree in the far left frame.



- 2 From the *Contents of: GatewayController* frame, select the GWC node that contains the card you want to unlock.



- 3 Select the **Maintenance** tab to display maintenance information about the node.



- 4 Click the **Card View** button for the card you want to unlock. This action opens the CS 2000 SAM21 Manager.

**Note:** If a card is currently locked, all fields display the value <unknown>.



GWC-6-UNIT-1

|                       |           |                 |           |
|-----------------------|-----------|-----------------|-----------|
| Administrative state: | <unknown> | Usage state:    | <unknown> |
| Operational state:    | <unknown> | Stand by state: | <unknown> |
| Activity state:       | <unknown> | Swact state:    | <unknown> |
| Isolation state:      | <unknown> | Alarm state:    | <unknown> |
| Available state:      | <unknown> | Fault state:    | <unknown> |
| Loadname:             |           |                 |           |

Save Image Busy (Disable) RTS (Enable) Card View

Force Warm Swact Cold Swact

### At the CS 2000 SAM21 Manager

- 5 In the card view, select the **States** tab.

**Note:** If you want to display the status of all cards in the shelf, select the **Shelf View** from the **View** menu.

File View

Sam21-2 : Slot 12

Alarms Equip **States** Diags Provisioning

Summary

| Critical | Major | Minor |
|----------|-------|-------|
| 0        | 0     | 0     |

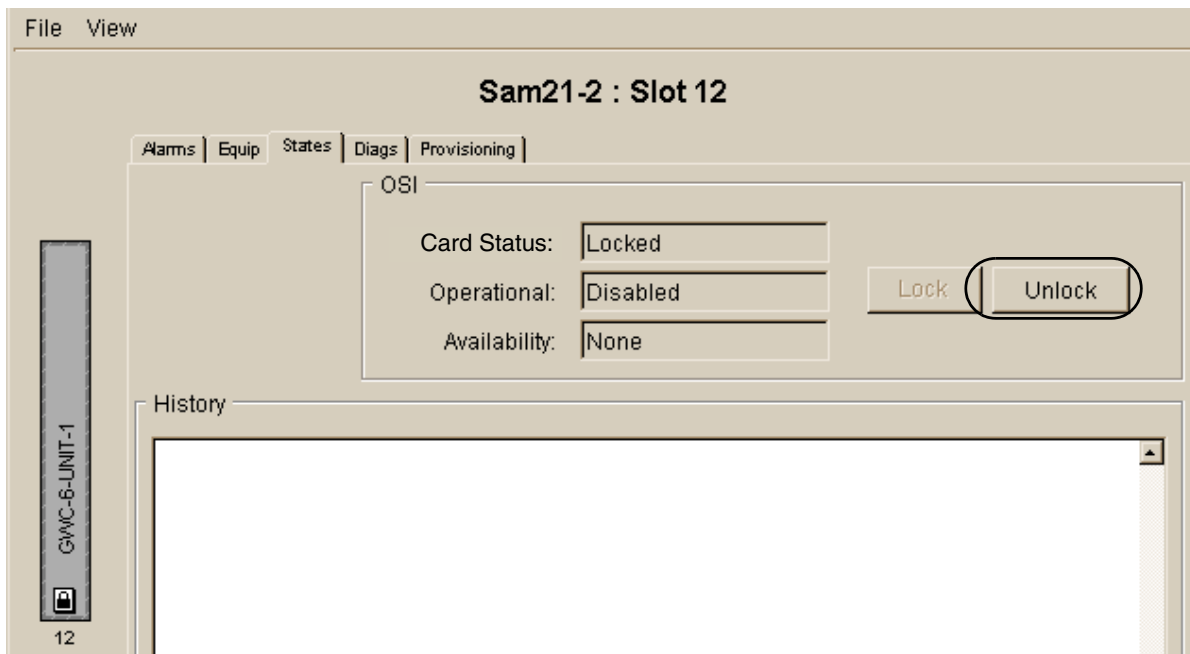
Details

| Equip. | ID | Time | Type | Severity | Reason |
|--------|----|------|------|----------|--------|
|--------|----|------|------|----------|--------|

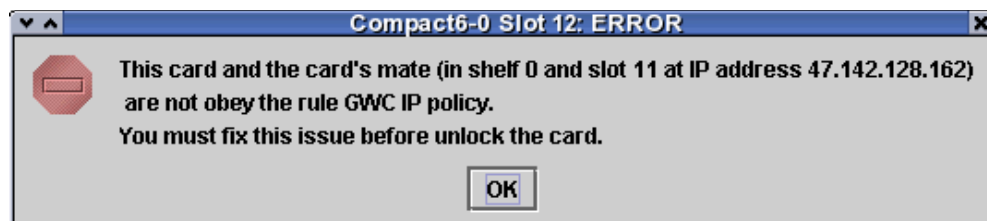
GWC-6-UNIT-1

12

- 6 In the States display, click the **Unlock** button to unlock the card.

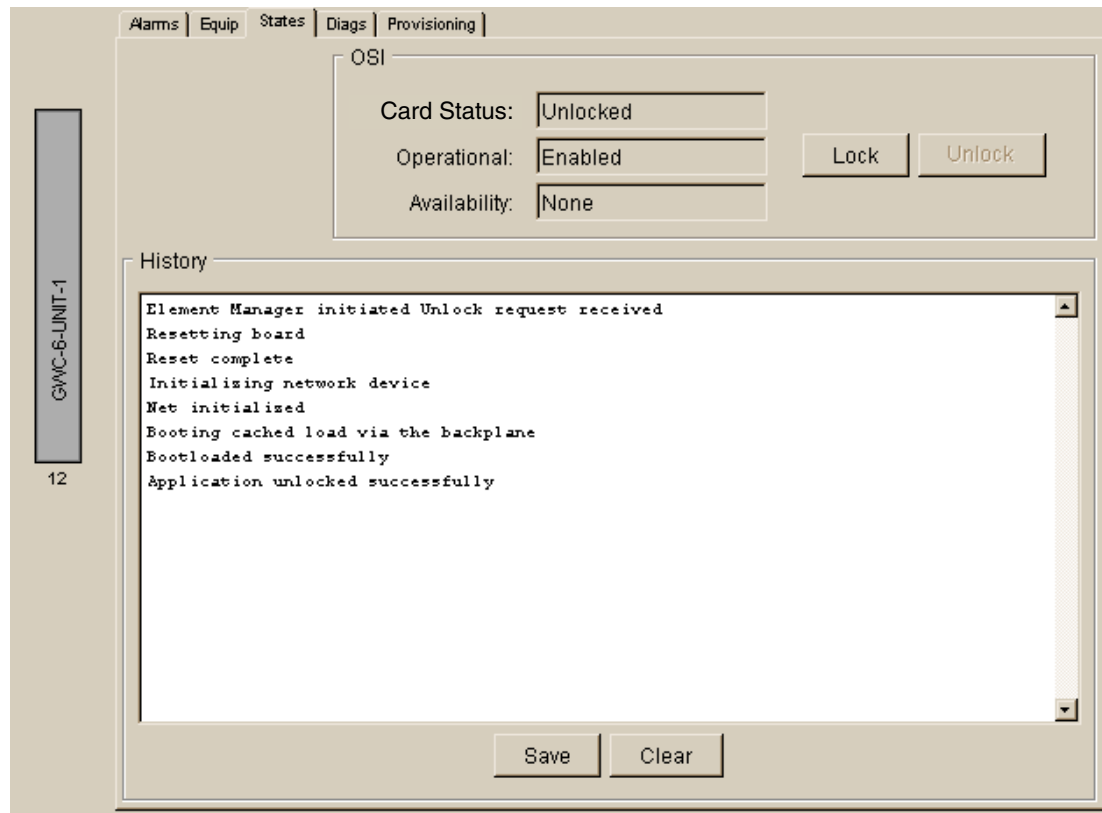


If the IP addresses for the selected card and its mate are not contiguous, the system displays the following error message:



Follow procedure “Manually re-provision GWC cards” in the *Gateway Controller Configuration Management*, NN10205-511 to correct these addresses, then repeat this procedure.

- 7 Observe the system response in the History window.  
The card is unlocked when you see the text “Application unlocked successfully”.



- 8 Return to [step 2](#) and repeat this procedure for the next GWC card until all the GWC cards have been unlocked and brought into service. Remember, each GWC node has two GWC cards.
- 9 The procedure is complete.



---

## Powering up a USP

---

### Purpose of this procedure

Use the following procedure to power up a Universal Signaling Processor (USP).

### When to use this procedure

Use this procedure when it is necessary to power up the USP. USP RTC-12 will initially be used to get the shelf back in service.

### Prerequisites

The CS 2000 Core and USP ABS server must be in-service.

### Action

#### Powering up a USP

##### *At the USP shelf*

- 1 Ensure all cards are seated in the USP shelf with the exception of the RTC-15 (slot 15) front panel card on the Control shelf.
- 2 Power up both A/B buttons on the control and extension shelves.
- 3 RTC-12 should SCSI boot and it should come into service within 1-2 minutes of being powered up.

##### *At the USP Manager*

- 4 Once RTC-12 is up, use the USP Manager to uninhibit and activate all links, where applicable. Refer to [Configuring Links on page 347](#).
- 5 Verify logs and alarms to ensure no unexpected problems and perform test calls.
- 6 Verify that all cards on all shelves are up and running with the exception of RTC-15.
- 7 Ensure that the System Date/Time is set to the current local time, if not using SNTP. Refer to [Setting the Date and Time on the USP on page 561](#).

##### *At the USP frame*

- 8 Once all cards are up and properly running, reseal RTC-15. RTC-15 should SCSI boot and perform a database synchronization with RTC-12. RTC-15 should come into service in approximately 5-7 minutes.

***At the USP Manager***

- 9 Verify that RTC-15 is in-service and inactive.
- 10 Verify logs and alarms again to ensure no unexpected or undesired events and perform test calls.
- 11 Verify that the USP can communicate with the ABS. From the USP Manager main menu, click on the Administration button and select ABS Settings.
- 12 Select the Test button to initiate a series of tests to ensure the USP can properly communicate with the ABS.
- 13 Check the USP logs for the test results. Troubleshoot ABS connectivity in the event that the tests fail.  
  
**Note:** To assist with troubleshooting, the Logs message will include the nature of the test failure.
- 14 Take a snapshot of the USP, and copy the snapshot to the ABS using the File Manager.
- 15 Using the ABS CM GUI, modify the site information to point to the new snapshot.
- 16 You have completed this procedure.

---

## Performing a partial power down recovery of the USP

---

### Purpose

This procedure is used to perform a partial power down recovery of a USP.

### Prerequisites

None

### Action

#### Performing a partial power down recovery of the USP

##### *At the USP frame*

- 1 Reseat the front panel and back panel CC card in Slot 18 on the Control shelf.
- 2 Reseat the front panel and back panel CC cards in Slot 18, beginning with the CC Slot 18 card on each of the extension shelves.
- 3 Reseat the inactive RTC.  
  
The inactive RTC should SCSI boot and perform a database synchronization with the active RTC. It will take approximately 5-7 minutes to come into service.

##### *At the USP Manager*

- 4 Verify the reseated RTC is in-service and inactive.
- 5 Verify logs and alarms to ensure there were no unexpected or undesired events.
- 6 Perform test calls.
- 7 You have completed this procedure.





## Setting the Date and Time on the USP

If your user account has administrative privileges, you can set the date and time information for a system. The date and time information includes month-day-year, hour-minute-second, and time zone data. In addition, you can configure the system to automatically adjust the clock settings when daylight savings time begins and ends.

You need to manually reset the date/time information if both of the RTC system nodes should go offline at the same time for any length of time. This usually occurs for one of the following reasons:

- if you perform a restore operation
- if you perform a complete office recovery (COR) on your system
- if your system is booted from an alternate boot data snapshot

You can set your USP to use the simple network time protocol (SNTP) to query a network time protocol server. Each time the USP queries the network time protocol server, the USP resets its time accordingly. The SNTP protocol enables the USP to obtain the accurate time of day and keep the same time as other elements in the network.

**Note:** If SNMP is not enabled for your system, verify the time settings for your system weekly to ensure that the system time is synchronized with the time on your OAMP workstation.

### Setting Date/Time information

#### *At the OAMP workstation*

- 1 Click **Administration>Date/Time** window. The current date and time settings for the system appear.
- 2 Determine if you want your USP to use the simple network time protocol (SNTP).

---

**If:**

No

Yes, user defined

---

**Do:**
Proceed to [step 3](#).

Check Enable SNTP Time Sync (User defined) in the SNTP portion of the window. Add an IP address for the SNTP server in the SNTP Server Address field. The information in the Time portion of the window is greyed out. Proceed to [step 5](#).

---

- 3 To set the date, click the calendar icon and highlight the day corresponding to today's date.
- 4 To set the time of day, click the clock icon. Use the spin boxes to set hour, minutes and seconds.
- 5 To set the local time zone, click the **Time Zone** drop-down menu. A world-wide list of time zones appears. Select the time zone listing that matches the local time zone.  
*Note:* The daylight savings time boxes are unavailable when the time zone you select does not use daylight savings time.
- 6 To enable or disable the automatic system clock adjustment for daylight savings time, click the **Adjust clock for daylight savings changes** box.  
*Note:* If you are enabling the automatic system clock adjustment for daylight savings time for the first time, make sure you perform steps [7](#) to [13](#).
- 7 Set the starting month for daylight savings time, click **dst-start-month**. Select the month in which daylight savings time starts.
- 8 Set the starting day in the **dst-start-day** spinbox.
- 9 Set the starting hour in the **dst-start-hour** spinbox.
- 10 Set the ending month for daylight savings time, click **dst-end-month**. Select the month in which daylight savings time ends.
- 11 Set the ending day in the **dst-end-day** spinbox.
- 12 Set the ending hour in the **dst-end-hour** spinbox.
- 13 Click **OK**.

---

## Powering up a Media Gateway/Multiservice Switch 15000

---

### Purpose of this procedure

Use the following procedure to power up a Media Gateway/Multiservice Switch 15000.

### When to use this procedure

Use this procedure when it is necessary to power up a Media Gateway/Multiservice Switch 15000.

### Prerequisites

None

### Action

#### Powering up a Media Gateway/Multiservice Switch 15000

##### *At the chassis*

- 1 Breaker interface panels (BIPs) are located at the top of the chassis. Switch on the breakers on each BIP. The system should come up on its own.  
  
**Note:** In the event that the CP card or its disk becomes unserviceable, the backup-up provisioning data and software will be downloaded from the MDM backup copy and SDS site, respectively.
- 2 You have completed this procedure.



---

## Performing a partial power down recovery of the Media Gateway/Multiservice Switch 15000

---

### Purpose

This procedure is used to perform a partial power down recovery of a Media Gateway/Multiservice Switch 15000.

### Prerequisites

None

### Action

#### Performing a partial power down of the Media Gateway/Multiservice Switch 15000

##### *At the frame*

- 1 Manually switch on the following breakers on the lower shelf:
  - A1.5
  - A1.2
  - B1.5
  - B1.2
- 2 Manually switch on the following breakers on the upper shelf:
  - A2.5
  - A2.2
  - B2.5
  - B2.2
- 3 The system should recover and come up on its own.
- 4 You have completed this procedure.



---

## Powering up a Media Gateway/Multiservice Switch 7400

---

### Purpose of this procedure

Use the following procedure to power up a Media Gateway/Multiservice Switch 7400.

### When to use this procedure

Use this procedure when it is necessary to power up a Media Gateway/Multiservice Switch 7400.

### Prerequisites

All power supply switches must be in the standby position.

### Action

#### Powering up a Media Gateway/Multiservice Switch 7400

##### *At the chassis*

- 1 Disengage all processor cards from the backplane of the shelf.
- 2 Engage the minimum number of processor cards required, based on the number of power supplies in the shelf.
  - If you have one power supply, engage a CP in slot 0 and at least one FP.  
Do not engage more than seven FPs. Ensure that all other processors are disengaged.
  - If you have two power supplies, engage at least one CP and two FPs. Or, engage two CPs and at least one FP.
- 3 Turn on the circuit breakers for the outlets that supply power to your switch.
- 4 Verify that the LEDs on all power supplies are red.
- 5 Apply power to one of the power supplies by setting its power switch to the on position. Verify that the power supply LED is green.  
  
Normal operation is not guaranteed if there are no processor cards in the shelf. If you have not installed any processor cards before you switch on a power supply, the system does not supply power to the shelf and the power supply LED remains red.
- 6 Verify that the cooling unit LED is green and is operational. You should be able to hear the fans start to rotate.

- 7** If necessary, apply power to a second and third power supply by setting their power switches to the on position. Verify that the LED for each power supply is green.  
  
If you install eight or more FPs, you must use a second power supply. If your system contains fewer than eight FPs, the system uses the second power supply for redundancy.
- 8** If necessary, engage the remaining processor cards.
- 9** Verify the LED color on each FP in appropriate.
- 10** Verify that the appropriate LEDs are illuminated on termination panels.
- 11** You have completed this procedure.



---

## Powering up the MDM workstation

---

### Purpose of this procedure

Use the following procedure to power up the MDM Sun Fire™ V480 workstation.

### When to use this procedure

Use this procedure when it is necessary to power up the MDM workstation.

### Prerequisites

An MDM user account is required.

### Action

#### Powering up the MDM workstation

##### *At the workstation*

- 1 Switch the workstation on.
- 2 Once the workstation has started, login with an MDM user account and ensure that the MDM toolset is available.
- 3 You have completed this procedure.



---

## Powering up an SPM device

---

### Purpose of this procedure

This procedure details the sequence of steps necessary to power up a Spectrum Peripheral Module (SPM), Media Gateway 4000 (MG 4000), Interworking Spectrum Peripheral Module (IW-SPM), or Dynamic Packet Trunking Spectrum Peripheral Module (DPT-SPM).

### When to use this procedure

Use this procedure when it is necessary to power up the SPM/MG 4000/IW-SPM/DPT-SPM.

### Prerequisites

None.

### Action

#### *At the MAP terminal*

- 1 Restore power to the frame and re-insert the fuses.
- 2 Reseat the SIM cards if they were unseated and turn them on one at a time using the switches on the front.
- 3 Reseat any unseated cards in the shelves.
- 4 Post the SPM/MG 4000/IW-SPM/DPT-SPM by typing  
**>MAPCI;MTC;PM;POST SPM <spm\_no>**  
and pressing the Enter key.  
where  
**spm\_no**  
is the number of the SPM/MG 4000/IW-SPM/DPT-SPM
- 5 Select and RTS the CEMs by typing  
**>SELECT CEM ALL;BSY ALL; LOADMOD ALL;RTS ALL**  
and pressing the Enter key.
- 6 Select and RTS the SRM, OC3 RMs, ATM RMs, and/or GEM RMs by typing  
**>QUIT;SELECT <rm\_type> ALL;BSY ALL;LOADMOD ALL;RTS ALL**  
and pressing the Enter key.  
where

**rm\_type**

is either SRM, OC3, ATM, or GEM

**Note:** To RTS the ATM, use the BSY FORCE and RTS FORCE commands.

- 7 Bring the carriers into service by typing

```
>QUIT ALL;MAPCI;MTC;TRKS;CARRIER;POST SPM  
<spm_no>;BSY ALL;RTS ALL
```

and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 8 Post and recover the trunks on the SPM at the TTP level by typing

```
>QUIT ALL;MAPCI;MTC;TRKS;TTP;PRADCH;POST AD SPM  
<spm_no>;BSY ALL;RTS ALL
```

and pressing the Enter key, followed by typing

```
>QUIT ALL;MAPCI;MTC;TRKS;TTP;POST D SPM  
<spm_no>;BSY ALL;RTS ALL
```

and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 9 Return to the PM level and post the SPM by typing

```
>QUIT ALL;MAPCI;MTC;PM;POST SPM <spm_no>
```

and pressing the Enter key.

where

**spm\_no**

is the number of the SPM/MG 4000/IW-SPM/DPT-SPM

- 10 Select and RTS the remaining RMs by typing

```
>SELECT <rm_type> ALL;BSY ALL;LOADMOD ALL;RTS  
ALL
```

and pressing the Enter key.

where

**rm\_type**

is DLC, DSP, VSP, and ALM

- 11 You have completed this procedure.

---

## Performing a partial power down recovery of the SPM

---

### Purpose

This procedure is used to perform a recovery of a partial power down of a DMS-SPM, MG 4000, IW-SPM, or DPT-SPM. In this procedure, SPM refers to the completed family of SPM devices unless otherwise noted.

### Prerequisites

None

### Action

#### Performing a partial power down recovery of the SPM

##### *At the MAP*

- 1 Post the SPM to recover by typing  
**>POST SPM <spm\_no>**  
and pressing the Enter key.  
where  
**spm\_no**  
is the number of the SPM to be powered down
- 2 Manually reseal the inactive CEM.
- 3 Post, busy, and return the inactive CEM to service by typing  
**>POST CEM <inactive\_cem>; BSY; RTS**  
and pressing the Enter key.
- 4 Manually reseal each RM.
- 5 Select, busy, and return each inactive resource module to service by typing  
**>POST <rm\_type> ALL; BSY ALL; RTS ALL**  
and pressing the Enter key.  
where  
**rm\_type**  
is SRM, OC3, ATM, GEM, DSP, VSP, ALM, or DLC
- 6 Perform [step 5](#) for each RM type.
- 7 You have completed this procedure.



---

## Powering up the MCS servers

---

### Purpose of this procedure

This procedure details the steps needed to power up the 8 MCS servers. The database server should be brought into service before any other servers. If other servers come up first, restart the management server.

### When to use this procedure

Use this procedure to power up and recover the MCS servers from a power outage.

### Prerequisites

None

### Action

#### *At the frame housing the MCS servers*

1

#### **ATTENTION**

The following shows the preferred order, which is not the way the system comes up if all servers are powered on at the same time.

Power on the database server by turning on the circuit breakers that provide power to the servers. It takes from 5 to 8 minutes for the server to boot and load Oracle.

2

After the DBSvr powers on, telnet to the box and run a spot check to make sure it is ready.

**a** Make sure Oracle is loaded. The best way is to telnet to the database. Type: **sqlplus** and fill in the username and password (in other words, log in as *user*, not *root*). If Oracle is running, you should receive the `SQL>` command prompt. Type **quit** to exit from sqlplus.

**b** Verify that the snmp service is running on the database box. Type: **ps -ef | grep snmp**. You should see three snmp processes:

```
/usr/local/sbin/snmpd -f udp:161
```

```
/bin/sh
```

```
/opt/app/oracle/product/9.2.0/bin/dbsnmpwd
```

```
/opt/app/oracle/product/9.2.0/bin/dbsnmp
```

The snmp processes are not critical to getting the system up. However, if any of the snmp processes are not running, you will not be able to see accurate reporting of this box on the System Management Console.

- c To stop or start oracle, telnet to the database as sysadmin and then su to root. Go to the following directory: `/etc/init.d`. The stop command is **./dbora stop**. The start command is **./dbora start**. These commands will severely affect service.
- 3 Verify that the SysMgr processes on the MgmtSvr/AcctMgr box are running in order to control the MCS components from the System Management Console. Telnet to the MgmtSvr/AcctMgr box as *nortel*.
    - a Make sure that the SysMgr processes are running by typing: **meinit -p**. You should see three processes running. If any of these processes are not running, you will not be able to launch the System Management Console:
 

```
Rel2.0    NTme_pids  mgmtsvr  mgmtsvr.3
Rel2.0    NTme_pids  tsscma   tsscma.5
Rel2.0    NTme_pids  tssfpma  tssfpma.6
```
    - b To stop or start the SysMgr, go to the following directory: `IMS/mgmtsvr/bin/mgmtsvr/` and type: **./MgmtSvrShutdown.pl**. This will kill any (or all) of the SysMgr processes.
    - c To start the SysMgr, stay in the same directory and type: **MgmtSvrConfigSetup.pl**. This will try to start all three processes. You will see a messages on the telnet session that say something like “starting tsscma waiting 30 seconds.” The tssfpma process will start next, followed by the mgmtsvr processes.
    - d To observe the SysMgr startup logs, after performing step b above, go to the following directory: `/var/Rel2.0/mgmtsvr`. Then type: **tail -f mgmtsvr.3.log**.
    - e Verify that the snmp process is running on the MgmtSvr/AcctMgr box by typing: **ps -ef | grep snmp**.  
You should see one process running:  
`/usr/local/sbin/snmpd -f udp:161`. If this process is not running or you get an alarm from the System Management Console that there is a problem with the



- 
- MgmtSvr/AcctMgr's snmp, then kill the process. The process will automatically restart in about 30 seconds.
- f** Restart the AcctMgr process. If any of the components send an alarm in the System Management Console indicating that the component cannot communicate with the primary or backup CAM, then again restart the AcctMgr process. Right click on the Accounting component in the System Management Console and select Restart. Confirm the request. A progress box will pop up and then disappear when the restart has begun. While the Accounting module is rebooting, the other MCS component will throw alarms to the System Management Console, but those will go away when the Acct component is fully operational.
- 4** Now verify the state of the other machines and the MCS components on them. Launch the System Management Console as you normally would. Expand the navigation tree fully so that each component is fully exposed.
- a** Restart the AppSvr. If the clients are having trouble communicating with the AppSvr, then restart the AppSvr. Right click on the AppSvr component in the System Management Console and select **Restart**. Confirm the request. You should see a progress window and it disappears after the restart has begun. To view AppSvr startup logs, telnet to the AppSvr box (we recommend that you telnet as *nortel*) and go to the following directory:  
`/var/Rel2.0/appsvr`. Type: **tail -f appsvr.0.log**.
  - b** Verify that the AppSvr's snmp process is running. This step is the same as [3e](#) above.
  - c** Restart the IPCM. If the i2004 phones are not responding to client registers, the hollow blinking icons in the i2004 display, then restart the IPCM component. Right click on the IPCM component in the System Management Console and select **Restart**. Confirm the request. You see a progress window that will disappear after the restart has begun. To view IPCM startup logs, telnet to the IPCM box (recommend as *nortel*) and go to the following directory: `/var/Rel2.0/esm`. Type: **tail -f esm.1.log**.
  - d** Verify that the IPCM's snmp process is running. This step is the same as [3e](#) above. Most likely, the Provisioning Module and the WebClient Module are deployed on the same box as the IPCM. Therefore, you only need to verify the snmp service on the box once.

- e Restart the Provisioning component. The best way to see if the Provisioning Module is behaving properly is to log in to the ProvClient. Launch a web browser to the IP address of the box where the Provisioning Module is deployed, such as <http://192.168.0.10/prov>. Log in as admin/admin and attempt any of the List options in the navigation tree, for example, List Devices or List Users. If the browser doesn't respond properly, then restart the Provisioning Module by right clicking on the Provisioning component in the System Management Console and select **Restart**. Confirm the request.
- f Restart the WebClientMgr component. Log in to the Personal Agent through your browser, such as <http://192.168.0.10/pa>. Log in as a subscriber, such as myusername@mydomain.com, and enter the subscriber's password. The Personal Agent should appear for that subscriber. If it does not, or the interface does not seem to respond correctly, restart the Provisioning Module described in [4e](#) above. (If you've already restarted it once and the ProvClient interface seems ok, but the Personal Agent interface is still not working correctly, it is probably a configuration issue.)
- g Launch the WebClient GUI from inside a subscriber's Personal Agent page. Attempt to log in to the WebClient when the System Management Console completes loading.

---

## Halt (shutdown) a Policy Controller unit

---

### Purpose of this procedure

This procedure is used to perform a graceful shut down a Policy Controller platform NCGL operating system. Use this procedure only as part of a high-level activity such as part of a controlled shutdown activity or part of a software upgrade activity. Included at the end of this procedure is an alternate CLI method for halting a unit.

### Limitations and Restrictions

This procedure does not cause the Policy Controller unit to power-off.

Ensure that the Policy Controller unit you are shutting down is not performing call processing activities.



#### CAUTION

This procedure halts all call processing activity and billing record generation on the affected unit, and prevents the Policy Controller node from operating in a fault-tolerant mode.

### Prerequisites

Use procedure "View the operational status of a Policy Controller NCGL platform" in Policy Controller Fault Management, NNxxxxx-911, to check for any disk array rebuilds in progress. Wait for the rebuild to complete before executing this procedure.

### Action

#### *At the CS 2000 Policy Controller Launch Point*

- 1 Select **Succession Communication Server NCGL Platform Manager** from the launch point menu.

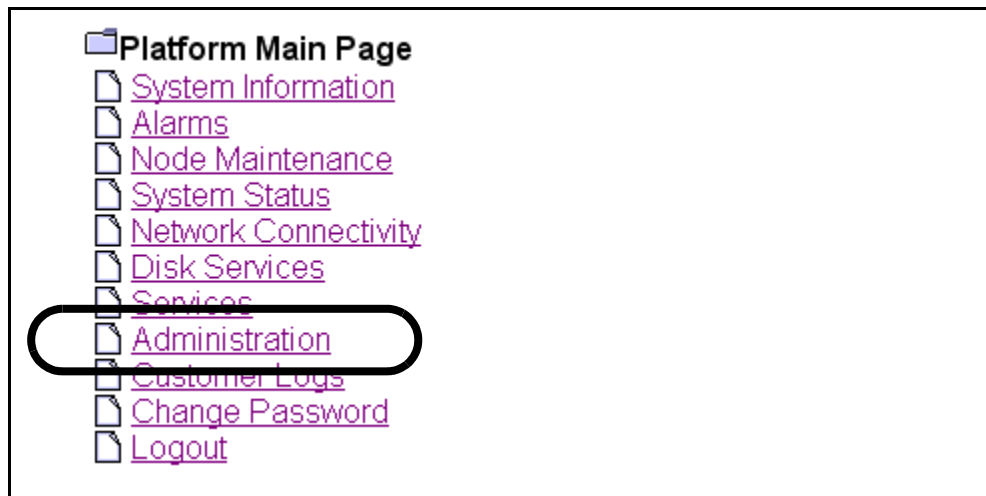
Service providers use this web interface to perform administrative tasks such as provisioning application data, performing platform or application maintenance, and monitoring logs and alarms.

Please select one of the following management interfaces:

[Succession Communication Server 2000 NCGL Platform Manager](#)

[Succession Communication Server 2000 Session Server Manager](#)

- 2 Click the **Administration** link.  
*The Administration page is displayed.*



- 3 Review the status of the unit you want to halt. If it is unavailable, the **Halt** or **HaltMate** buttons are not accessible.

| Bootload Management |  |  |                  |  |
|---------------------|--|--|------------------|--|
| Bootload            |  |  | Maintenance      |  |
| 5.20.1.0.0405122209 |  |  | Default Bootload |  |

| Software Upgrade     |                      |                      |                      |                      |
|----------------------|----------------------|----------------------|----------------------|----------------------|
| Protocol             | Login ID             | Password             | IP address           | File                 |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

| Server Maintenance                                                       |                                                                        |
|--------------------------------------------------------------------------|------------------------------------------------------------------------|
| <b>Unit 0 - Active</b>                                                   |                                                                        |
| <input type="button" value="Reboot"/> <input type="checkbox"/> Force     | <input type="button" value="Halt"/> <input type="checkbox"/> Force     |
| <b>Unit 1 - Inactive</b>                                                 |                                                                        |
| <input type="button" value="RebootMate"/> <input type="checkbox"/> Force | <input type="button" value="HaltMate"/> <input type="checkbox"/> Force |

- 4 Click the **Halt** or **HaltMate** button for the Policy Controller unit you want to halt the NCGL operating system for.

**Note:** To override any pre-halt (shutdown) queries, click the **Force** check box before clicking the **Halt** or **HaltMate** button.

| Bootload Management                       |                      |                                         |                      |                      |
|-------------------------------------------|----------------------|-----------------------------------------|----------------------|----------------------|
| Bootload                                  |                      |                                         | Maintenance          |                      |
| 5.20.1.0.0405122209                       |                      |                                         | Default Bootload     |                      |
| Software Upgrade                          |                      |                                         |                      |                      |
| Protocol                                  | Login ID             | Password                                | IP address           | File                 |
| <input type="text"/>                      | <input type="text"/> | <input type="text"/>                    | <input type="text"/> | <input type="text"/> |
| Server Maintenance                        |                      |                                         |                      |                      |
| Unit 0 - Active                           |                      |                                         |                      |                      |
| Reboot <input type="checkbox"/> Force     |                      | Halt <input type="checkbox"/> Force     |                      |                      |
| Unit 1 - Inactive                         |                      |                                         |                      |                      |
| RebootMate <input type="checkbox"/> Force |                      | HaltMate <input type="checkbox"/> Force |                      |                      |

*The system responds:*

```
Are you sure you wish to halt?
This may cause an extended service outage to any
clients currently using this server. Click OK to
confirm server halt or cancel to abort.
```

- 5 Click **OK** to confirm the halt operation.  
The NGCL and all call activity on the affected Policy Controller begins the process of halting. This can take several minutes.
- 6 If you receive the following message, you must halt the unit using the Force option in step 4.  

```
Error: Command failed. Reason: Mate not available.
```
- 7 If applicable, complete procedure [Power-Off a Policy Controller unit on page 585](#) to disconnect power from the unit.
- 8 This procedure is complete.

### To Haltmate or Force Haltmate?

The Haltmate action does not work if the SIP Gateway application database on the active unit is out of sync with the database on the inactive unit. Using the Haltmate command with the Force option overrides any pre-checks for this condition and forces a Halt of the inactive unit regardless of the sync state of the active unit database.

## Alternate command line interface (CLI) method

### ATTENTION

All prerequisites and restrictions shown on page [579](#) apply to using this procedure.

### *At the Policy Controller console interface*

- 1 Log onto a Policy Controller unit using a secure shell by typing  

```
> ssh -l <userid> <PC_IP_address>
```

and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**PC\_IP\_address**

is the IP address of the Policy Controller unit

**Example**

```
ssh -l mtc 45.128.54.12
```

- 2 When prompted, enter your password.
- 3 Change to the root user by typing  

```
$ su - root
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Shutdown the Policy Controller unit by typing  

```
# halt
```

and pressing the **Enter** key.
- 6 If applicable, complete procedure [Power-Off a Policy Controller unit on page 585](#) to disconnect power from the unit.
- 7 You have completed this procedure.





---

## Power-Off a Policy Controller unit

---

### Purpose of this procedure

This is used to power off a Policy Controller unit.

This procedure may be used as a standalone task or as part of a higher level activity such as a part of a controlled shutdown activity or part of a software upgrade activity.

### Limitations and restrictions



#### CAUTION

This is a service affecting procedure. Powering off a Policy Controller unit prevents the node from operating in a fault-tolerant manner. Ensure that the unit you are powering off is not the active unit. Failure to do so may result in loss of call processing.

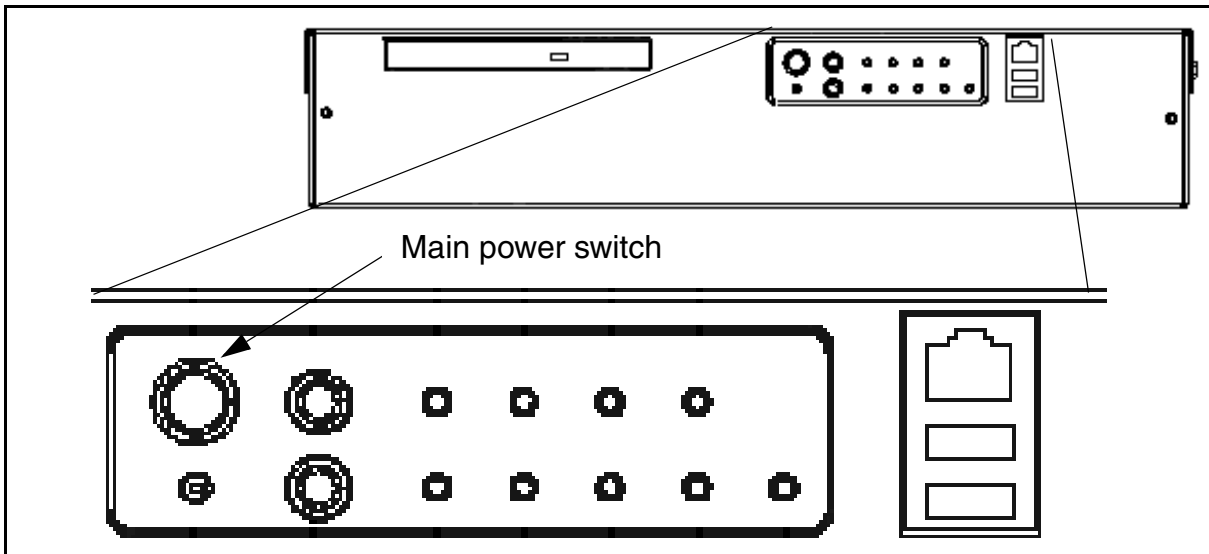
### Prerequisites

Refer to procedure “View the operational status of a Policy Controller NCGI platform” in Policy Controller Fault Management, NNxxxxx-911 to verify that the unit to be shut down is not active.

### Action

#### ***At the front panel of the Policy Controller unit.***

- 1 Complete procedure [Halt \(shutdown\) a Policy Controller unit on page 579](#) in before powering off the unit.
- 2 Once the operating system has been halted, disconnect the power to the unit using the main power switch located on the front panel.



3 The procedure is complete.

---

## Powering up a Border Control Point

---

### Purpose of this procedure

Use the following procedure to power up a Border Control Point. The Border Control Point shelves are powered from either a PDU or EBIP located at the top of the frame depending on if the frame is AC or DC powered.

### When to use this procedure

Use this procedure when it is necessary to power up the chassis that houses the Border Control Point.

### Prerequisites

None

### Action

#### Powering up the Border Control Point

##### *At the frame housing the Border Control Point*

- 1 For DC powered shelves, switch the circuit breakers at the EBIP that provide power to the shelf being powered to the ON position. The breaker will have the '1' side (top) of the breaker depressed.
- 2 For AC powered shelves, push the rocker located on the top of the AC outlet to apply power to the chassis. It should be switched to the 'I' position.
- 3 Once the breaker are switched ON at the power source, power up the shelf by switching the breaker on the back of the chassis to the ON position.
- 4 Observe the System, Power/Fan, Slot (filled) and Host Card LEDs as the unit is being powered. Once power on is complete, they should all have a steady green color.
- 5 You have completed this procedure.



---

## Powering up the IPmedia 2000 shelves

---

### Purpose of this procedure

Use the following procedure to power up the IPmedia 2000 shelves that house the MS 2000 series devices and the Packet Media Anchor. The IPmedia 2000 shelves reside in either a SAMF frame or CCF, depending on whether or not your solution uses the CS 2000 or CS 2000-Compact.

### When to use this procedure

Use this procedure when it is necessary to power up the IPmedia 2000 shelves.

### Prerequisites

None

### Action

#### Powering up the Media Server 2000 servers

##### *At the CCF or SAMF frame*

- 1 Open the front door of the CCF/SAMF frame.
- 2 At the EBIP at the top of the frame, turn the breaker associated the Media Server to the ON position.
- 3 Ensure that the Green Power LED on the front of the Nortel Media Server 2000 is on (right hand side of the card).  
After 1 to 2 minutes, the Green LED on the left hand side of the card lights.
- 4 Verify the status of the LEDs on the front of the Nortel Media Server 2000:
  - Red Fail LED is off (left hand side of the board).
  - ACT LED is on (left hand side of the board).  
**Note:** It may take up to 60 seconds for the ACT LED to light up.
  - Blue LED does not remain on (right hand side of the board).
  - PWR LED is on (right hand side of the board).
  - Both Ethernet Link LEDs are on (middle of the board).  
**Note:** The Ethernet LEDs are Green when indicating a connection, and Orange when indicating activity.

**Note:** Check the Media Server 2000 to make sure it is set to an unlocked state.

- 5 You have completed this procedure.

---

## Powering up the SAM16 shelves

---

### Purpose of this procedure

Use the following procedure to power up the SAM16 shelves that house the UAS devices. The SAM16 shelves reside in either a SAMF frame or CCF, depending on whether or not your solution uses the CS 2000 or CS 2000-Compact.

### When to use this procedure

Use this procedure when it is necessary to power up the SAM16 shelves.

### Prerequisites

None

### Action

#### Powering up the SAM16 shelves

##### *At the CCF or SAMF frame*

- 1 Open the front door of the CCF/SAMF frame.
- 2 At the EBIP at the top of the frame, turn the breakers associated the SAM16 to the ON position.
- 3 You have completed this procedure.





## Powering up an MG 9000 device

### Purpose of this procedure

Use the following procedure when power to the MG 9000 has been lost.

### When to use this procedure

Use this procedure when it is necessary to power up the MG 9000 frame.

### Prerequisites

None

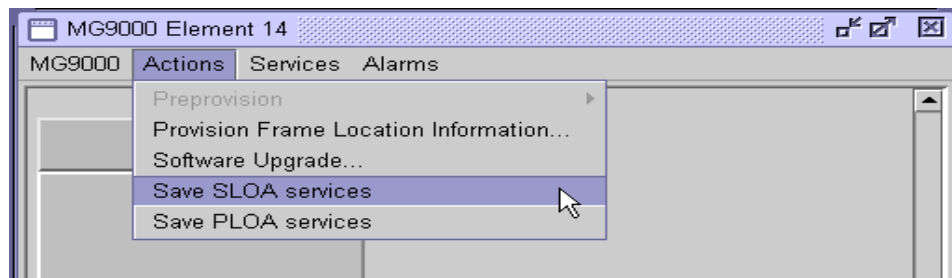
### Action

#### Recovering an MG 9000 that has lost power and cannot communicate with the MG 9000 Manager

##### *At the MG 9000 Manager*

- 1 At the Subnet View of the MG 9000 Manager, select the MG 9000 to be re-commissioned. A warning window indicating that your connection to the gateway is down may appear. This will not block the saving of services information.
- 2 Save a copy of the MG 9000 Manager SLoA provisioning data as follows (you'll be re-entering this data later):
  - a To Save the SLoA services provisioning data, at the Frame (Element) view, select the "Save SLOA services" option from the Actions menu.

##### Frame View



An acknowledgment window appears in response to this request. The acknowledgment window contains the name of the two files (with .html and .text suffixes) where your data had been stored on the MG 9000 Manager.

- b Record the file name provided in the Save acknowledgement window for later use.

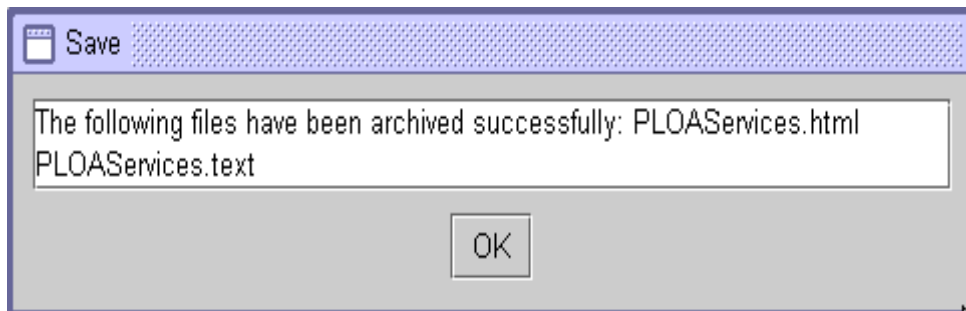
### Save acknowledgement message for SLoA



- 3 Save a copy of the MG 9000 Manager PLoA provisioning data as follows (you'll be re-entering this data later):
  - a To save the PLoA services provisioning data, at the Frame (Element) view, select the "Save PLOA services" option from the Actions menu.
 

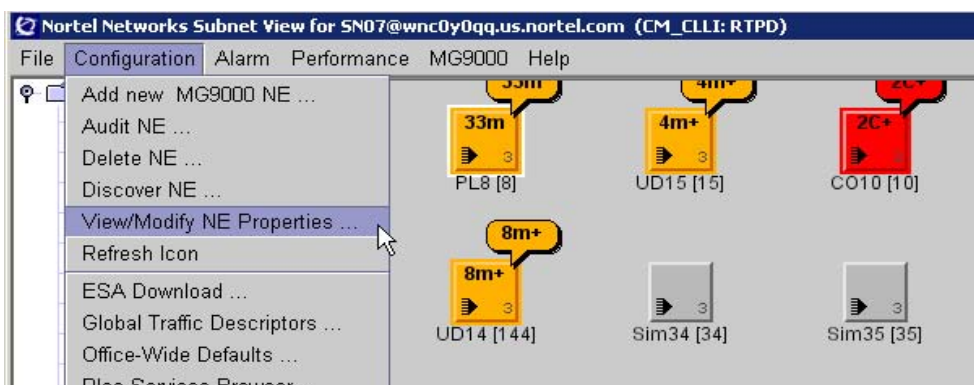
An acknowledgment window appears in response to this request. The acknowledgment window contains the name of the files where your data had been stored on the MG 9000 Manager.
  - b Record the file name provided in the Save acknowledgement window for later use.

### Save acknowledgement message for PLoA



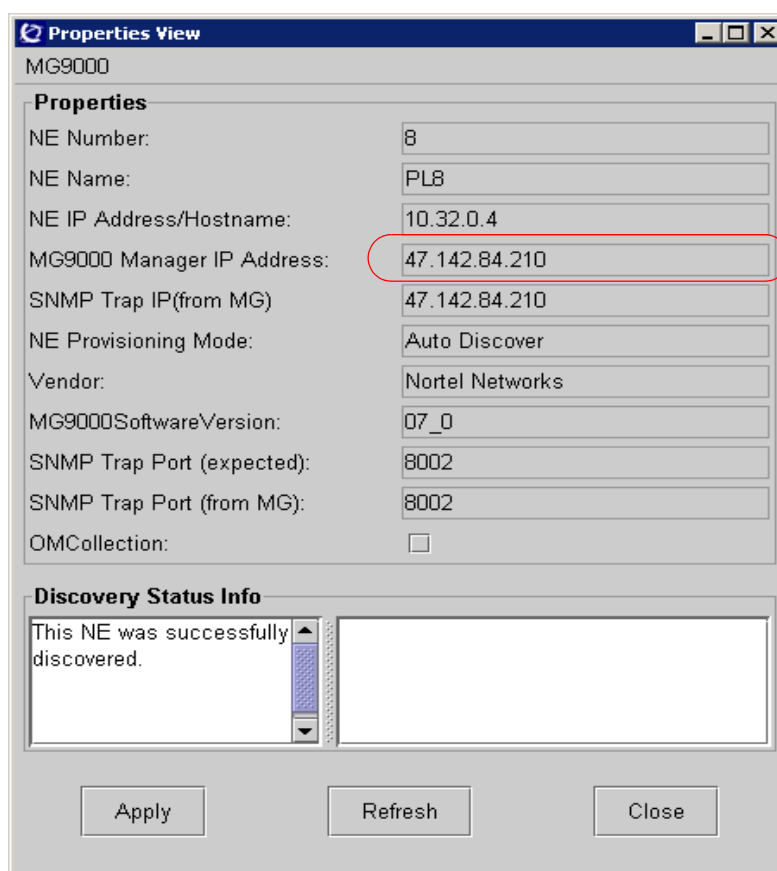
- 4 Obtain the IP address of the MG 9000 Manager server (not the mid-tier or client). At the Subnet View, select Configuration->View/Modify NE Properties from the menu bar.

## Subnet View accessing Configuration ->View/Modify NE Properties



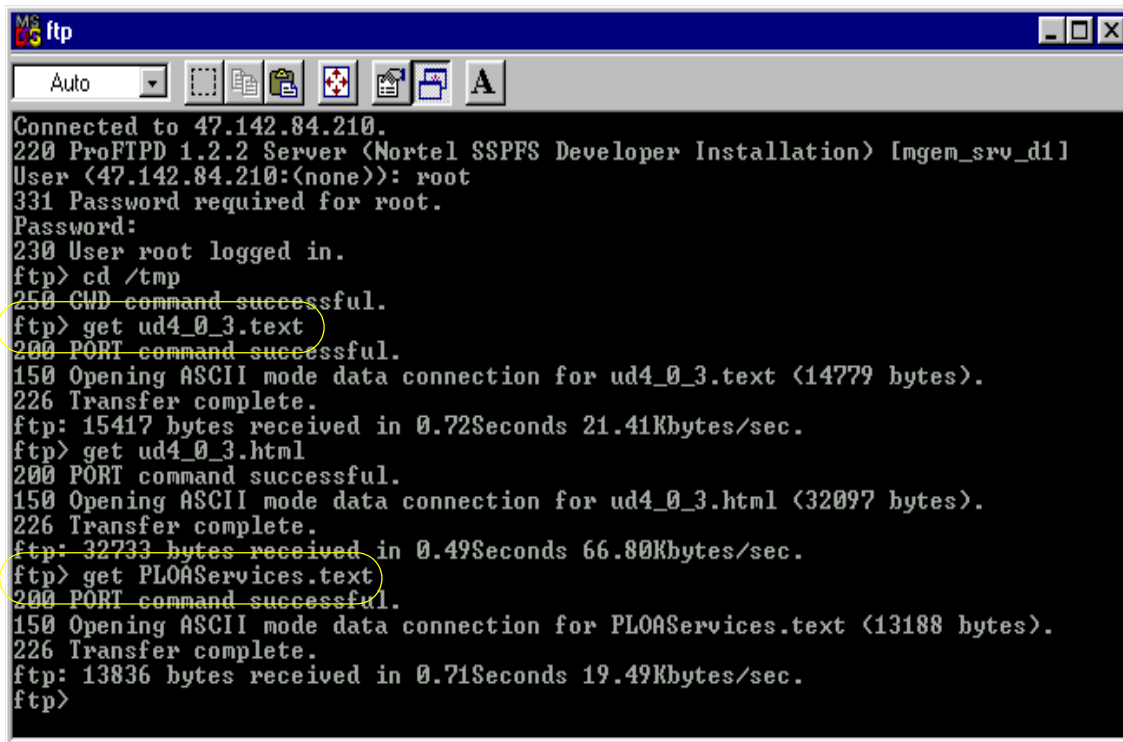
- 5 Record the IP address in the MG 9000 Manager IP Address field.

## Properties View



- 6 FTP to the address recorded in step 5 and copy the files in the /tmp directory to a secure location, such as your desktop or permanent server before proceeding.

## FTP files to secure location



```
MS ftp
Auto
Connected to 47.142.84.210.
220 ProFTPD 1.2.2 Server (Nortel SSPFS Developer Installation) [mgem_srv_d1]
User (47.142.84.210:(none)): root
331 Password required for root.
Password:
230 User root logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> get ud4_0_3.text
200 PORT command successful.
150 Opening ASCII mode data connection for ud4_0_3.text (14779 bytes).
226 Transfer complete.
ftp: 15417 bytes received in 0.72Seconds 21.41Kbytes/sec.
ftp> get ud4_0_3.html
200 PORT command successful.
150 Opening ASCII mode data connection for ud4_0_3.html (32097 bytes).
226 Transfer complete.
ftp: 32733 bytes received in 0.49Seconds 66.80Kbytes/sec.
ftp> get PLOAServices.text
200 PORT command successful.
150 Opening ASCII mode data connection for PLOAServices.text (13188 bytes).
226 Transfer complete.
ftp: 13836 bytes received in 0.71Seconds 19.49Kbytes/sec.
ftp>
```

### *At the MG 9000 frame*

- 7 Power up the shelves in the frame by reinstalling the fuse modules on the IBIP. Restore all fuses left to right in the frame.
- 8 Connect a laptop PC to the active DCC card and launch the local craft interface (LCI).
- 9 Wait for the restart to complete and for all cards initialize, typically takes 5 minutes. The Administrative State of all common cards will be Locked.
- 10 From the LCI, Unlock the active DCC OC-3/DS1 IMA card by selecting the Admin. State Unlock radio button. Wait for the status at the LCI to change to Enabled, Online, and Unlocked.
- 11 From the LCI continue to unlock the common cards in the following order until all are unlocked and online:
  - active ITX
  - active ITP
  - OC-3 carriers on the active OC-3 DCC card
  - inactive DCC

- inactive ITX
  - inactive ITP
  - OC-3 carriers on the inactive OC-3 DCC card
  - DS1 cards (if provisioned)
  - ABI cards (if provisioned)
- 12** Initiate rediscovery by sending a cold start trap from the LCI.

***At the MG 9000 Manager***

- 13** Monitor the MG 9000 network element and wait until the discovery process is complete.
- 14** Wait for the network element to show it is operational, then check for dial tone.
- 15** You have completed this procedure.



## Geographic survivability

---

Geographic survivability is the distribution of components across a geographic area to make sure services continue in the event of a disaster. A disaster can include fire, flood, tropical storm, or act of terrorism. Geographic survivability includes the distribution of hardware across multiple locations.

The Automatic Backup and Accelerated restore feature, 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 and will be located at a different site from the target system. Remote backup performs the backup via TCP/IP connection and stores an exact copy on the standby server which can be quickly and remotely activated. This remote backup copies all files in each file system marked for backup using the same behavior as a full system backup.

A remote backup configuration tool is provided to set the necessary parameters and schedule for automatic backup which can be scheduled to automatically occur from once a day to four times per day. This tool also provides a facility for manually initiating a backup and monitoring its progress. 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 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.

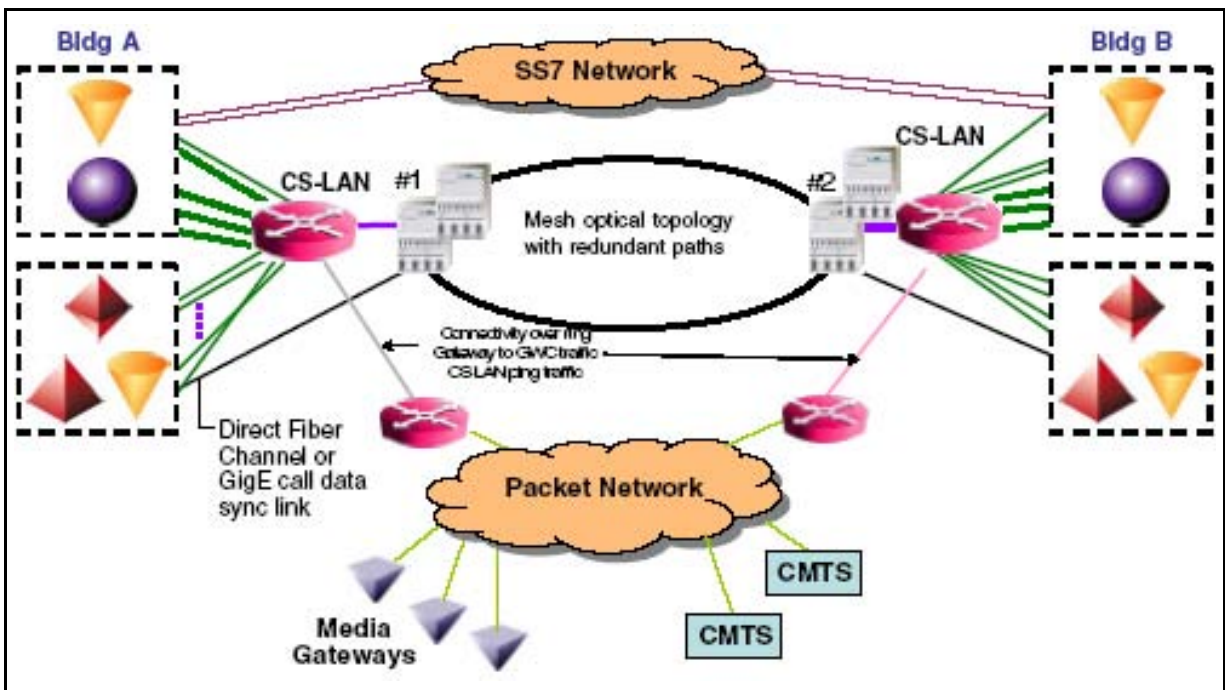
For a communication server, geographic survivability requires that redundant components (other than OAM components) must reside at different sites (referred to as Site A and Site B). The CS 2000 - Compact supports geographic survivability through the fail-over and sparing functionality of individual nodes. The configuration for the CS 2000 Management Tools and IEMS servers and the Core and Billing Manager (CBM) 850 is as follows:

- Site A is configured with the CS 2000 Management Tools and IEMS high availability server pairs
- Site B is configured with the CBM 850 high availability server pairs (referred to as CBM 850 HA u0 and u1)

- Site A is configured with an additional CBM in to be used in the event of disaster at Site B (referred to as CBM 850 standby u0)
- Site B is configured with an additional server for the CS 2000 Management Tools and IEMS in the event of disaster at Site A

The following figure shows the topology of CS 2000 - Compact support for geographic survivability.

**Figure 1**  
**Geographic survivability topology**



Geographic survivability for the CS 2000 - Compact has the following limitations:

- The physical distance between sites is limited to 120 KM/75 miles.
- Geographic survivability requires the USP - Compact.
- Each site must have a single Ethernet Routing Switch 8600 with dual switch fabric and CPU blades, or third part equivalent.

### Site failure in a geographic survivable configuration

There are two scenarios for recovery of a geographic survivable network configuration:

- [Site A failure](#)
- [Site B failure](#)



**Site A failure**

A loss of Site A would include a loss of the CS 2000 Management Tools and Integrated EMS servers. This loss would result in the following losses of functionality:

- all OAM&P functions of the CS 2000 Management Tools and IEMS, including GUI access, element management, alarms, and non-Core logs
- access to the CS 2000-Compact Core Manager on the CBM 850

The responsive action in this scenario would be to bring the standby CS 2000 Management Tools and IEMS servers into service at Site B.

**Site B failure**

A loss of Site B would include a loss of the CBM 850 servers. This loss would result in the following losses of functionality:

- transfer of billing records from the Core to the CBM 850
- billing records resident in the CBM 850 that had not been offloaded to an OSS
- ability to receive scheduled Core OMs and logs (resulting in them being discarded)
- access to the CS 2000-Compact Core Manager
- backup bootp load repository

The responsive action in this scenario would be to bring the standby CBM 850 into service at Site A.

**Maintaining a sites in a geographic survivable configuration**

There are three options for maintaining a geographic survivable network configuration. Based on your estimated amount of weekly

maintenance versus your acceptable downtime in the event of site failure, choose one of the options presented in the following tables.

**Table 1 Site A maintenance (for CS 2000 Management Tools/IEMS servers)**

| Maintenance level | Predictability of successful failover | Estimated downtime                               | Estimated weekly maintenance | Procedures to execute in advance                                                                                  | Procedures to execute upon Site A failure                                                                                                                                                                                                                                                                    |
|-------------------|---------------------------------------|--------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Medium            | Medium-High                           | 3-4 hours depending on the amount of backup data | 10 hours                     | As needed:<br><br><a href="#">Communication Server 2000 Management Tools Geographic Survivability on page 651</a> | <a href="#">Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 639</a><br><br><a href="#">Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600 on page 643</a><br><br><a href="#">Communication Server 2000 Management Tools Geographic Survivability on page 651</a> |

**Table 1 Site A maintenance (for CS 2000 Management Tools/IEMS servers)**

| Maintenance level | Predictability of successful failover | Estimated downtime                               | Estimated weekly maintenance | Procedures to execute in advance                                                                                                                                                                                                                                                                                                                                                     | Procedure to execute upon Site A failure                                                                                                                                                                                                                                                                            |
|-------------------|---------------------------------------|--------------------------------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High              | High                                  | 3-4 hours depending on the amount of backup data | 13-14 hours                  | <p>As needed:</p> <p><a href="#">Communication Server 2000 Management Tools Geographic Survivability on page 651</a></p> <p>Weekly:</p> <p><a href="#">Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 639</a></p> <p><a href="#">Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600 on page 643</a></p> <p>(continued on next page)</p> | <p><a href="#">Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 639</a></p> <p><a href="#">Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600 on page 643</a></p> <p><a href="#">Communication Server 2000 Management Tools Geographic Survivability on page 651</a></p> |

**Table 1 Site A maintenance (for CS 2000 Management Tools/IEMS servers)**

| Maintenance level | Predictability of successful failover | Estimated downtime                               | Estimated weekly maintenance | Procedures to execute in advance                                                                | Procedure to execute upon Site A failure |
|-------------------|---------------------------------------|--------------------------------------------------|------------------------------|-------------------------------------------------------------------------------------------------|------------------------------------------|
| High (continued)  | High                                  | 3-4 hours depending on the amount of backup data | 13-14 hours                  | <a href="#">Communication Server 2000 Management Tools Geographic Survivability on page 651</a> |                                          |

**Table 2 Site B maintenance (for CBM 850 servers)**

| Maintenance level | Predictability of successful failover | Estimated downtime | Estimated weekly maintenance | Procedures to execute in advance                                                                    | Procedures to execute upon Site B failure                                                                                                                                                                                                                                                                                                                              |
|-------------------|---------------------------------------|--------------------|------------------------------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Low               | Low                                   | 3 hours            | 0 hours                      | As needed:<br><br><a href="#">Core and Billing Manager 850 Geographic Survivability on page 647</a> | <a href="#">Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 639</a><br><br><a href="#">Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600 on page 643</a><br><br><a href="#">Fresh pre-install of CBM 850 cold u0 on page 609</a><br><br><a href="#">Core and Billing Manager 850 Geographic Survivability on page 647</a> |

**Table 2 Site B maintenance (for CBM 850 servers)**

| Maintenance level | Predictability of successful failover | Estimated downtime | Estimated weekly maintenance | Procedures to execute in advance                                                                                                                                            | Procedure to execute upon Site B failure                                                                                                                                                                                                                                                       |
|-------------------|---------------------------------------|--------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Medium            | Medium-High                           | 2.5 hours          | 7 hours                      | As needed:<br><br><a href="#">Core and Billing Manager 850 Geographic Survivability on page 647</a><br><br><a href="#">Fresh pre-install of CBM 850 cold u0 on page 609</a> | <a href="#">Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 639</a><br><br><a href="#">Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600 on page 643</a><br><br><a href="#">Core and Billing Manager 850 Geographic Survivability on page 647</a> |

**Table 2 Site B maintenance (for CBM 850 servers)**

| Maintenance level | Predictability of successful failover | Estimated downtime | Estimated weekly maintenance | Procedures to execute in advance                                                                                                                                                                                                                                                                                                                                                                               | Procedures to execute upon Site B failure                                                                                                                                                                                                                                                             |
|-------------------|---------------------------------------|--------------------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High              | High                                  | 2 hours            | 10 hours                     | <p>As needed:</p> <p><a href="#">Core and Billing Manager 850 Geographic Survivability on page 647</a></p> <p><a href="#">Fresh pre-install of CBM 850 cold u0 on page 609</a></p> <p>Weekly:</p> <p><a href="#">Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 639</a></p> <p><a href="#">Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600 on page 643</a></p> | <p><a href="#">Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 639</a></p> <p><a href="#">Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600 on page 643</a></p> <p><a href="#">Core and Billing Manager 850 Geographic Survivability on page 647</a></p> |

(continued on next page)



**Table 2 Site B maintenance (for CBM 850 servers)**

| Maintenance level | Predictability of successful failover | Estimated downtime | Estimated weekly maintenance | Procedures to execute in advance                                                                                                                          | Procedure to execute upon Site B failure |
|-------------------|---------------------------------------|--------------------|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| High (continued)  | High                                  | 2 hours            | 10 hours                     | <a href="#">Fresh pre-install of CBM 850 cold u0 on page 609</a><br><br><a href="#">Core and Billing Manager 850 Geographic Survivability on page 647</a> |                                          |

**Fresh pre-install of CBM 850 cold u0**

To reduce the duration of downtime during an outage, it is recommended that the CBM 850 cold u0 be pre-installed. Contact your next level of support for this task.

**Geographical Survivability impacts to CS 2000-Compact**

A new sub-panel is added to the Call Agent Card View Provisioning panel (tab) that allows you to either enable or disable the feature. The following figure shows an example configuration with Geographic Survivability enabled.

**Figure 2 Call Agent Card View Provisioning panel: Geographic Survivability enabled**

The screenshot shows the provisioning interface for OTT4 CA-1 Slot 6. The 'Provisioning' tab is selected and circled. The 'Geographical Survivability' sub-tab is also selected and circled. The 'Enable' checkbox is checked. The 'Backup Path' section shows two GEO UNIT IP addresses: 10.72.0.12 and 10.72.0.20, both with a mask of 255.255.255.248. Other fields include IP (10.72.17.22), Subnet Mask (255.255.240.0), MAC Address (0001AF12AFA0), Gateway IP (10.72.16.1), FW Version (RM03-2.4), MAC 2 (0001AF12AF9F), Primary NTP (47.135.43.193), Secondary NTP (47.135.43.196), Server IP (47.135.43.193), Path (/3pc), and Load (ncgl\_cca\_image\_7.02.1.0). A 'Get Load Files' button is present. At the bottom, there are buttons for 'Modify', 'Save', 'Clear', 'Cancel', 'Details...', and 'Help'.

### Failure scenarios

The following table provides summaries of system responses during various failure scenarios when Geographical Survivability is enabled.

The scenarios assume redundant configurations are located in two separate buildings.

**Table 3 System response summaries**

| Scenario                                                    | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ethernet Routing Switch 8600 failure in one building</b> | <p><b><i>In the building with the failed routing switch...</i></b></p> <ul style="list-style-type: none"> <li>• All nodes lose mate connectivity via Ethernet.</li> <li>• The Call Agent loses WAN backup connectivity.</li> <li>• FC backup remains up.</li> <li>• The Call Agent detects IST loss, but cannot disable OSPF.</li> <li>• USPC detects isolation and takes down SS7 links at the site with the 8600 failure.</li> </ul> <p><b><i>In the building with the in-service routing switch...</i></b></p> <ul style="list-style-type: none"> <li>• The Call Agent remains active if it is already active. No outage occurs. If the Call Agent was not active, it takes activity within 2 seconds.</li> <li>• SOS goes through a warm or cold restart (approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor and 30 seconds for the NTRX51GZ card with the MPCN765 processor).</li> <li>• Other nodes go active and follow the Call Agent example after losing mate connectivity.</li> <li>• If Site B has the in-service router, the cold standby CS 2000 Management Tools (CMT) server must be brought into service (see the note below).</li> <li>• If Site A has the in-service router, the cold standby Core Billing Manger (CBM) must be brought into service (see the note below).</li> </ul> <p><b>Note:</b> Consider using this option based on the estimated time to recover the fault or failure of the CS LAN versus time and effort to bring up the cold standby system and recover the high availability (HA) pair afterward.</p> <p>For example, if the time to recover the CS LAN is estimated to be 10 hours, it might not be worth activating the cold standby CMT server or CBM.</p> |

**Table 3 System response summaries**

| Scenario                                     | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Optical frame failure in one building</b> | <p><b><i>In the building with the failed optical frame...</i></b></p> <ul style="list-style-type: none"> <li>• All nodes lose mate connectivity via Ethernet.</li> <li>• The Call Agent loses FC backup connectivity.</li> <li>• WAN backup remains up.</li> <li>• The active Call Agent remains active, but without sync. No outage occurs <i>The remainder of this scenario assumes the active Call Agent is in this building.</i></li> <li>• Other nodes go active and follow the Call Agent example after losing mate connectivity. (Done without mate connectivity.)</li> </ul> <p><b><i>In the building with the in-service optical frame...</i></b></p> <ul style="list-style-type: none"> <li>• The Call Agent detects IST loss, and disables OSPF.</li> <li>• Other nodes go inactive and follow the Call Agent example after losing mate connectivity. (Done without mate connectivity.)</li> <li>• USPc detects isolation from the active Call Agent, and takes down SS7 links at the site with the inactive USP.</li> <li>• If Site B has the failed optical frame, the cold standby CBM must be brought into service at Site A (see the note below).</li> <li>• If Site A has the failed optical frame, the cold standby CMT must be brought into service at Site B (see the note below).</li> </ul> <p><b>Note:</b> Consider using this option based on the estimated time to recover the fault or failure of the CS LAN versus time and effort to bring up the cold standby system and recover the high availability (HA) pair afterward.</p> <p>For example, if the time to recover the CS LAN is estimated to be 10 hours, it might not be worth activating the cold standby CMT server or CBM.</p> |

**Table 3 System response summaries**

| <b>Scenario</b>                                          | <b>Response</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>One building is destroyed in a catastrophic event</b> | <p data-bbox="570 359 1081 394"><b><i>In the building that is destroyed...</i></b></p> <ul data-bbox="570 407 1393 520" style="list-style-type: none"><li data-bbox="570 407 889 443">• There is no activity.</li><li data-bbox="570 455 1393 520">• The SS7 network takes down the links to the destroyed building.</li></ul> <p data-bbox="570 533 1138 569"><b><i>In the building that is not destroyed...</i></b></p> <ul data-bbox="570 581 1393 1224" style="list-style-type: none"><li data-bbox="570 581 1081 617">• All nodes lose mate connectivity.</li><li data-bbox="570 630 1393 695">• The Call Agent loses all mate connectivity, including the backup WAN link, and drops sync.</li><li data-bbox="570 707 1393 800">• If the Call Agent is active, it remains active. No outage occurs. If the Call Agent is not active, it takes activity within 2 seconds.</li><li data-bbox="570 812 1393 982">• If the Call Agent is inactive, it takes activity within 2 seconds followed by a warm or cold SOS restart (approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor).</li><li data-bbox="570 995 1300 1060">• Other nodes go active, and follow the Call Agent example after losing mate connectivity.</li><li data-bbox="570 1073 1393 1138">• If Site B was destroyed, the cold standby CBM must be brought into service at Site A.</li><li data-bbox="570 1150 1393 1224">• If Building A was destroyed, the cold standby CMT must be brought into service at Site B.</li></ul> |

**Table 3 System response summaries**

| Scenario                                                     | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Active Call Agent card fails in one building</b>          | <p><b><i>In the site with the failed Call Agent...</i></b></p> <ul style="list-style-type: none"> <li>All nodes in the site can communicate with their mates.</li> </ul> <p><b><i>In the site with the mate Call Agent...</i></b></p> <ul style="list-style-type: none"> <li>All nodes in the site can communicate with their mates.</li> <li>The (inactive) Call Agent detects loss of connectivity with the mate, detects local and WAN connectivity, takes activity, and restarts the SOS.</li> <li>Other nodes experience disconnection from the SOS for approximately 20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor (normal restart behavior).</li> </ul> |
| <b>Inactive Call Agent card fails in one building</b>        | <p><b><i>In the site with the failed inactive Call Agent...</i></b></p> <ul style="list-style-type: none"> <li>All nodes in the site can communicate with their mates.</li> </ul> <p><b><i>In the site with the mate Call Agent...</i></b></p> <ul style="list-style-type: none"> <li>All nodes in the site can communicate with their mates.</li> <li>The (active) Call Agent detects loss of connectivity with the mate, detects local and WAN connectivity, and stays active.</li> <li>No SWACT or restart is required.</li> </ul>                                                                                                                                                                                                         |
| <b>Recovery from isolation split brain (Active/Inactive)</b> | <p><b><i>In both sites...</i></b></p> <ul style="list-style-type: none"> <li>Once the Call Agents can communicate with their mates, they recognize that both are active. The Call Agent that was inactive backs down, leaving the other Call Agent active. The fallout is to force Unit 0 active and Unit 1 inactive.</li> <li>Other nodes can communicate with their mates, negotiate activity, and resume normal operations.</li> </ul>                                                                                                                                                                                                                                                                                                     |

**System impact of failures**

Failures could cause the following system impacts:

- When negotiating activity, the Call Agent preference is always to remain on the same side, if that side supports activity.
- If failover of the Call Agent is necessary, the Call Agent switches activity in less than two seconds. When the Call Application performs a restart, call processing is interrupted for approximately

20 seconds for the NTRX51HZ card with the MCPN905 processor, and 30 seconds for the NTRX51GZ card with the MCPN765 processor (normal restart behavior). Failovers of other Callp nodes follow the Call Agent failover within two seconds.

- In configurations where the solution contains Message Controller (MC) cards connected to Message Switches (MS), ENET and TDM peripherals, the MC cards and MSes are co-located in one of the main geographically redundant sites.

During site isolation, when determining the appropriate master site, preference is given to the site that contains the MC cards. This assumes that the site is able to take activity. If necessary, activity is switched to this side during the activity negotiation.

*This configuration is supported only in Enterprise (CS2100) solutions.*

### Recovery scenarios

The following table provides a summary of system responses during recovery.

**Table 4 System response summary**

| Scenario                                                     | Response                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Recovery from isolation split brain (Active/Inactive)</b> | <ol style="list-style-type: none"> <li>1. When Call Agents can communicate with their mates, they recognize that both are active. The Call Agent that was inactive before the failure backs down, leaving the other Call Agent active. The fallout is to force Unit 0 active, and Unit 1 inactive.</li> <li>2. Other nodes can communicate with their mates, negotiate activity and resume normal operations.</li> </ol>                                                           |
| <b>General recovery behavior</b>                             | <p>All elements:</p> <ul style="list-style-type: none"> <li>• continually monitor connections with their mates, and with other network elements with which they normally communicate. When connectivity is not present, they continue to monitor the connections for restored connectivity. (The elements continue monitoring regardless of their activity state.)</li> <li>• negotiate activity and services when connectivity recovers, and resume normal operations.</li> </ul> |

### System impact of recovery

Recovery could cause the following system impacts:

- When negotiating activity, the Call Agent preference is always to leave activity on the same side. When recovering to a full system configuration, activity remains on the same unit, without impact.
- During recovery from a split system (caused by incorrect message routing), node activity resolves in a few seconds. Call processing could require up to 15 minutes to recover completely.

### Limitations and restrictions

Please note the following restrictions for the Geographic Survivability feature for the Call Agent:

- In hybrid configurations (with TDM equipment homed at one site), the TDM equipment is not geographically redundant. In determining the master site, preference is given to the TDM side only when either side can support Callp. If necessary, a SWACT is performed to the TDM side to allow Callp on that side.

*This configuration is supported in Enterprise (CS2100) solutions.*

- Because the Call Agent interacts with the Ethernet Routing Switch 8600, the feature requires that each site have only one routing switch and IST links configured between sites. Dual ERS 8600's at each site and SMLT links between sites are not supported. Interactions between the Call Agent and the CS LAN are supported to prevent split brain scenarios (by disabling OSPF) when the ERS 8600's are used for the CS LAN. CS 2100 upgrades from previous releases in the geographic survivable configuration (which have dual 8600's at each site) require that the dual 8600's be migrated to a single 8600 site.
- When a total loss of communication between sites occurs (that is, all three master links are down), the two Call Agents cannot negotiate activity decision. The decision is based on connectivity check from each site the WAN network.
  - While unlikely, it could be possible to have an active/active (split brain) scenario, or an inactive/inactive scenario (no processing).
  - The WAN backup path mitigates the risk of optical ring failure. The WAN connection check helps resolve activity when the backup path is down.
- CS 2000 - Compact supports only a single time zone setting. If the two physical sites are in different time zones, it recommended that the time zone be set to either GMT or the time zone of one of the sites.



- Both Session Server units of a pair are located at the same site. For offices with Message Controllers, it is recommended that the Session Servers be located at the same site as the TDM components.
- For maximum redundancy, the WAN backup path must be configured separately from the optical network, as follows:
  - special vlans configured on Ethernet Routing Switch 8600 for backup path use only
  - vlans route over the WAN network instead of over the optical ring
  - vlans are not disabled with OSPF disable
  - alarm generated for lack of connectivity
- Gateways and services node components of CS 2000 - Compact are single units, and are not geographically redundant. Where the nodes are located and how they are connected to the network affects whether they survive a failure. Although the same nodes are supported in configurations with and without Geographic Survivability, there is no change in configuration or connection in the configuration with the Geographic Survivability configuration.

For more information about Geographic Survivability for offices configured with Message Controllers, refer to *Geographic Survivability Planning Guide*, 555-4031-901.



## Installing the remote backup server

This procedure is used to install the remote backup server for GEO Survivability. The remote backup server provides a standby backup system that is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with system configuration data and files accurate to the last synchronization.

### Prerequisites

Use the table below to ensure that you have the following information ready for input during the procedure.

| System Variable                                    | Actual value |
|----------------------------------------------------|--------------|
| Hostname                                           |              |
| IP address (IP of remote backup server)            |              |
| Netmask                                            |              |
| Router (default gateway IP)                        |              |
| DNS (Yes, No)                                      |              |
| Unit 0 IP address (IP of primary cluster unit 0)   |              |
| Daily backup time (up to four) in format:<br>HH:MM |              |
| where<br>HH = hours (00-23)<br>MM = minute (00-59) |              |

## Action

### Installing SPFS on a GEO Survivability standby server

#### *At your workstation or the remote server console*

- 1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server

| If you want to log in by means of | Enter                                                                                                                        |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| ssh                               | ssh -1 root <server><br><br>where<br><br><server><br><br>is the name of the N240 server.<br><br>Go to <a href="#">step 2</a> |
| telnet                            | telnet <server><br><br>where<br><br><server><br><br>is the name of the N240 server.<br><br>Go to <a href="#">step 2</a>      |
| the remote server console         | <a href="#">step 2</a>                                                                                                       |

- 2 Log in to the server through the console (port A), and when prompted enter the root user ID and password.
- 3 Bring the system to the {0} ok prompt by typing:  
**# init 0**
- 4 Enter the following command to verify that the auto-boot option is set to true:  
**{0} ok eeprom auto-boot?**  
If it is set to false, enter the following command:  
**{0} ok eeprom auto-boot?=true**
- 5 Insert disk 1 of the SPFS0\*\* (090) CD set into the DVD drive on the standby unit.

- 6 Install the remote backup server for GEO Survivability:  
**{0} ok boot cdrom - rbackup**
- 7 In response to the prompt, type ok and then press Enter to acknowledge restriction on your use of the software.
- 8 In response to the prompt, select the rbackup server profile for the system.
- 9 In response to the prompt, enter no to not select the default settings. The N240 server must be connected to the network and must have access to the default gateway. This allows you to enter the server's settings for the installation.
- 10 In response to the prompts, enter the following site-specific information. Refer to the information you entered in the table located at the beginning of this procedure.
  - a Enter the hostname for this system.
  - b Enter the IP address for the remote backup server.
  - c Enter the subnet mask for this network.
  - d Enter the IP address for this network's router.
  - e Enter the timezone for this system.

**Note:** The default is US/Eastern. Enter ? for a list of supported time zones.
  - f Will this system use DNS?

**Note:** Enter yes or no. If you answer yes you will be prompted for the DNS domain name, name server IP addresses, and the search domains. You may enter several name servers and search domains. To stop entry enter a blank line.
- 11 In response to the prompt, enter ok to accept current settings.
- 12 The installation of the first CD takes approximately 25 minutes. No action is required until the system response shown below displays:  
Example system response:  
Media:
  1. CD/DVD
  2. Network File System
  3. SkipMedia[1]:

- 13 Enter 1 and then press Enter to select CD/DVD as the Media type for the installation of Solaris 9.  
The system ejects the disk 1 CD automatically.
- 14 Remove the SPFS disk 1 CD from the server.
- 15 Place the SPFS disk 2 CD (the second SPFS CD in the set of 3 disks) into the DVD drive and then press Enter. This step takes approximately 15 minutes to complete.
- 16 In response to the prompt, enter 2 to continue with the installation.
- 17 In response to the prompt, press Enter to reboot the system. The installation of the Solaris Patches starts after the system reboots.
- 18 The installation of the second CD takes approximately 20 minutes. No action is required until the system prompts you to enter the third CD, as shown in the system response example below.  
Example system response:  
Done Installing Solaris Patches...  
  
Insert SSPFS Deadstart CDROM Disk 3 in the Drive  
  
Type "ok" when Ready:
- 19 Remove the SPFS disk 2 CD from the server.
- 20 Place the SPFS disk 3 CD (the third SPFS CD in the set of 3 disks) into the DVD drive.
- 21 In response to the prompt, enter ok and then press Enter to start the installation of the third CD.
- 22 The installation of the third CD takes approximately 50 minutes. You may be required to press Enter to have the login prompt reprinted to the screen after the reboot.  
Example system response:  
<Hostname> console login:
- 23 Log in to the server using the root user ID and password.
- 24 After you have logged in to the server, remove the SPFS disk 3 CD from the server:  
**eject cdrom**
- 25 Enter the command line interface (cli) tool:  
**cli**

- 26 Enter the number next to the Configuration option in the menu.
- 27 Enter the number next to the Succession Element Configuration option in the menu.
- 28 Enter the number next to the PSE Application Configuration option in the menu.
- 29 Enter the number next to the Configure PSE option in the menu.
- 30 In response to the prompt, enter the primary/cluster IP address of CS 2000 Management Tools server. This will be the address of the NPM server.
- 31 In response to the prompt, enter y to confirm the IP address.  
*Note:* You may receive the error message, “Can’t configure PSE on remote backup unit to enable NPM”. This message can be ignored.
- 32 Enter x to exit each level until you have exited from the cli tool.
- 33 Start the PSE server:  
**# pse start**
- 34 Verify that the server has started. If the server does not start, contact your next level of support.  
**# pse status**
- 35 At this point enter NPM on the CS 2000 Management Tools server and follow patching procedures to apply all relevant patches.
- 36 You have completed this procedure.





## Scheduling automatic backups of the remote server

### Target

Use this procedure to schedule automatic backups to the remote server. Backing up the primary server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with data and files accurate to the last synchronization.

### Action

#### Scheduling automatic backups of the remote server

##### *At your workstation or the remote server console*

- 1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server

| If you want to log in by means of | Do                                                                         |
|-----------------------------------|----------------------------------------------------------------------------|
| ssh                               | Type ssh <server> and press the Enter key. Go to <a href="#">step 2</a>    |
| telnet                            | Type telnet <server> and press the Enter key. Go to <a href="#">step 2</a> |
| the remote server console         | <a href="#">step 2</a>                                                     |

where

**<server>**

is the name of the N240 server.

- 2 When prompted, enter the root user ID and password.
- 3 Start the command line interface tool by entering:  
**cli**  
The system responds by displaying a menu.
- 4 Select the Configuration menu.  
The system displays the Configuration menu.
- 5 Select the Remote Backup option.

Response:

Remote Backup Configuration

```

1-rbackup_display (Display Remote Backup
Configuration)
2-rbackup_config (Remote Backup Configuration)
3-rbackup_exec (Execute Remote Backup Now)
X-exit

```

**6** Select:**2-rbackup\_config (Remote Backup Configuration)**

The system responds with the IP address of the primary server that is currently configured as the remote server, and the times that are currently configured for automatic backups.

**7** Enter the unit 0 IP address of the primary server to be backed up.

Response:

```
<nnn.nnn.nnn.nnn> is alive
```

where

```
<nnn.nnn.nnn.nnn>
```

is the IP address that you entered

**8** Use the following table to determine your next step.

| If the system                             | Do                                      |
|-------------------------------------------|-----------------------------------------|
| prompts you to accept the ssh key         | Enter yes. Go to <a href="#">step 9</a> |
| does not prompt you to accept the ssh key | Go to <a href="#">step 9</a>            |

Response:

```
Enter a time for a daily backup to occur
(HH:MM) :
```

where

**HH**

is hours. Valid values are 00 to 23.

**MM**

are minutes. Valid values are 00 to 59.

**9** Enter the first time for a daily backup to occur

**Note:** You can configure up to four times for daily backup to occur.

**Response:**

Enter a second time for a daily backup to occur (HH:MM) or enter "x" to stop provisioning backup times:

- 10** Use the following table to determine your next step.

| <b>If you</b>                                                  | <b>Do</b>                                                                      |
|----------------------------------------------------------------|--------------------------------------------------------------------------------|
| want to enter another time for a remote backup to occur        | Enter a second time for a daily backup to occur. Go to <a href="#">step 11</a> |
| do not want to enter another time for a remote backup to occur | Enter x. Go to <a href="#">step 13</a>                                         |

- 11** Use the following table to determine your next step.

| <b>If you</b>                                                  | <b>Do</b>                                                                     |
|----------------------------------------------------------------|-------------------------------------------------------------------------------|
| want to enter another time for a remote backup to occur        | Enter a third time for a daily backup to occur. Go to <a href="#">step 12</a> |
| do not want to enter another time for a remote backup to occur | Enter x. Go to <a href="#">step 13</a>                                        |

- 12** Use the following table to determine your next step.

| <b>If you</b>                                                  | <b>Do</b>                                                                      |
|----------------------------------------------------------------|--------------------------------------------------------------------------------|
| want to enter another time for a remote backup to occur        | Enter a fourth time for a daily backup to occur. Go to <a href="#">step 13</a> |
| do not want to enter another time for a remote backup to occur | Enter x. Go to <a href="#">step 13</a>                                         |

- 13** Use the following table to determine your next step.

| <b>If you want to</b> | <b>Do</b>                                                          |
|-----------------------|--------------------------------------------------------------------|
| commit changes        | Go to <a href="#">step 14</a>                                      |
| exit                  | Enter quit. Go to <a href="#">step 16</a>                          |
| re-enter settings     | Enter anything other than ok or quit. Go to <a href="#">step 9</a> |

- 14 Enter  
ok  
Response:  
=== "rbackup\_config" completed successfully
- 15 To test the backup capability, perform a remote backup of the primary server in the HA cluster the standby server will emulate in the event of an extended outage. Enter the number next to the rbackup\_exec (Execute Remote Backup Now) option in the menu.  
  
*Note:* Executing a backup can take an hour or more to complete. Therefore, either you may choose to perform this backup now to ensure the standby server is ready in the event of a primary site disaster, or you may choose to run the backup later at your earliest convenience.
- 16 Exit the Remote Backup Configuration level by typing  
x  
and pressing the Enter key.
- 17 Verify that the system has successfully completed the backup:  
# **less /var/adm/messages**  
In response, the system displays the contents of the log file.
- 18 The procedure is complete.

## Viewing configuration information for remote server backups

### Target

Use this procedure to view the current configuration information for remote server backups. The system displays the IP address of the target system that is configured as the remote server, and the times at which automatic backups of the target system occur.

### Action

#### Viewing configuration information for remote server backups

##### *At your workstation or the remote server console*

- 1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server

| If you want to log in by means of | Do                                                                         |
|-----------------------------------|----------------------------------------------------------------------------|
| ssh                               | Type ssh <server> and press the Enter key. Go to <a href="#">step 2</a>    |
| telnet                            | Type telnet <server> and press the Enter key. Go to <a href="#">step 2</a> |
| the remote server console         | <a href="#">step 2</a>                                                     |

where

**<server>**

is the name of the N240 server.

- 2 Start the command line interface tool by entering:

**cli**

The system responds by displaying a menu.

- 3 Select the Configuration menu.

The system displays the Configuration menu.

- 4 Select the Remote Backup option.

Response:

Remote Backup Configuration

1-rbackup\_display (Display Remote Backup Configuration)

2-rbackup\_config (Remote Backup Configuration)

3-rbackup\_exec (Execute Remote Backup Now)

X-exit

**5** Select

**1-rbackup\_display (Display Remote Backup Configuration)**

Response:

Current settings:

Target system is: <nnn.nnn.nnn.nnn>

Back up times are: <Time 1>...<Time n>

where

**<nnn.nnn.nnn.nnn>**

is the IP address of the remote server

**<Time 1>... <Time n>**

is the set of times at which automated backups occur

**6** Exit the Remote Backup Configuration level by typing

**x**

and pressing the Enter key.

**7** The procedure is complete.

## Performing a manual backup of the remote server

### Target

Use this procedure to perform a remote backup of the remote server for the HA cluster it will emulate in the event of an extended outage. Backing up the remote server provides a standby backup system which is ready to provide service if the primary system is unavailable for an extended period of time. The remote server can assume the identity of the primary server with data and files accurate to the last synchronization.

### Action

#### Performing a manual backup of the remote server

##### *At your workstation or the remote server console*

- 1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server

| If you want to log in by means of | Do                                                                         |
|-----------------------------------|----------------------------------------------------------------------------|
| ssh                               | Type ssh <server> and press the Enter key. Go to <a href="#">step 2</a>    |
| telnet                            | Type telnet <server> and press the Enter key. Go to <a href="#">step 2</a> |
| the remote server console         | <a href="#">step 2</a>                                                     |

where

**<server>**

is the name of the N240 server.

- 2 When prompted, enter the root user ID and password.
- 3 Start the command line interface tool by entering:  
**cli**  
The system responds by displaying a menu.
- 4 Select the Configuration menu.  
The system displays the Configuration menu.
- 5 Select the Remote Backup option.

**Response:**

Remote Backup Configuration

1-rbackup\_display (Display Remote Backup Configuration)

2-rbackup\_config (Remote Backup Configuration)

3-rbackup\_exec (Execute Remote Backup Now)

X-exit

**6** Select:

**3-rbackup\_exec (Execute Remote Backup Now)**

**7** A backup will now automatically be made.

**8** Exit the Remote Backup Configuration level by typing:

**x**

and pressing the Enter key.

**9** The procedure is complete.



## Viewing logs from a remote backup

### Target

Use this procedure to view logs associated with a backup of the remote server. Logs are created during automatic and manual backups of the remote server.

### Action

#### Viewing logs from a remote backup

##### *At your workstation or the remote server console*

- 1 Determine how to log in to the Sun Netra 240 (N240) server that is installed as the remote backup server

| If you want to log in by means of | Do                                                                         |
|-----------------------------------|----------------------------------------------------------------------------|
| ssh                               | Type ssh <server> and press the Enter key. Go to <a href="#">step 2</a>    |
| telnet                            | Type telnet <server> and press the Enter key. Go to <a href="#">step 2</a> |
| the remote server console         | <a href="#">step 2</a>                                                     |

where

**<server>**

is the name of the N240 server.

- 2 Enter:  
**less /var/adm/messages**  
The system responds by displaying the contents of the log file.
- 3 The procedure is complete.



---

## Initiating a recovery back to the cluster

---

### Prerequisites

It is expected that the primary server is in the shut-down mode.

If the box was previously a CBM HA cluster, any billing files not already sent to a down-stream billing server should be removed prior to performing 'Installing the remote backup server.'

### Target

When completed, this procedure will reboot unit 0 of the cluster (configured as a remote backup server in step 1) after a remote backup of the original remote server located on the opposite side of the ring. Unit 0 will become the cluster and Unit 1 will clone Unit 0 and the HA Cluster (Primary Server) will then be completely recovered.

### Action

#### Initiating a recovery back to the cluster

##### *At your workstation*

- 1 Follow the 'Installing the remote backup server' procedure.  
**Note:** In his case, the unit0 server of the cluster is used as a remote backup server. Use the same hostname and IP address that was used to configure the remote backup server in the first place
- 2 Follow the 'Scheduling automatic backup of the remote server' procedure.  
**Note:** Use only one automated schedule and make sure to select a time that will not be invoked shortly.
- 3 Follow the 'Performing a manual backup of the remote server' procedure.
- 4 Bring down the machine currently active by following the procedure 'Two-server (cluster) configuration' in chapter 'Shutting down an SSPFS-based server' of the document ATM/IP Solution-level Fault Management NN10408-900.
- 5 Follow the 'Initiating a switch over to the remote backup server' procedure to bring the services back to unit0 of the cluster.
- 6 Follow the 'Cloning the image of one server in a cluster to the other server' procedure of the document ATM/IP Solution-level Security and Administration NN10402-600.

- 7** You **MUST** remove any outstanding billing records, not already sent to a downstream billing server, from the remote server (if that is a CBM) before continuing otherwise the billing records on that box will be lost.
- 8** Reinstall the backup server following the (Installing the remote backup server' procedure.
- 9** Reconfigure the backup server following the 'Scheduling automatic backups of the remote server' procedure.
- 10** The procedure is complete.

---

## Initiating a switch over to the remote backup server

---

### Prerequisites

Prior to starting this procedure the Cluster machine must be shut down.

To carry this out, refer to section 'Two-server (cluster) configuration' in chapter 'Shutting down an SSPFS-based server', of the document ATM/IP Solution-level Fault Management NN10408-900.

The user must be logged in as the root user in order to initiate the switch command.

### Target

When completed, this procedure will reboot the remote backup server as the unit0 of the cluster.

### Action

#### Initiating a switch over to the remote backup server

##### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  

```
<server>
```

is the IP address or host name of the SSPFS-based remote backup server
- 2 When prompted, enter your user ID and password.
- 3 Invoke the switch by typing  

```
$ /opt/sspfs/rbks/switch
```

and pressing the Enter key.
- 4 When ready, indicate you want to proceed by typing  

```
OK
```

and pressing the Enter key.
- 5 The procedure is complete.



## Disabling Ethernet Routing Switch 8600 WAN Edge routing

### Purpose

#### ATTENTION

Perform this procedure immediately after a site failure occurs to limit effects to Call Processing.

This procedure is required to workaround a deficiency in the architecture when the active in-service and SYSB (out of service) GWC send messages to a gateway provisioned off the GWC causing mismatches in the gateway resulting in loss of call processing.

This procedure will impact every element sitting off the ERS 8600.

There are two options for this procedure. The first option will disable all dynamic routing on the chassis and no traffic will be able to leave or enter the VLANs configured on that chassis when using Open Shortest Path First (OSPF). Static routes and Local communication is still possible.

The second option will disable the WAN Edge Interface. All traffic, whether through dynamic or static routes will not be able to leave or enter the chassis.

### Prerequisites

None

### Procedure

#### Disabling Ethernet Routing Switch 8600 WAN Edge routing

##### *At the Ethernet Routing Switch 8600 Workstation*

- 1 Determine which option you will use.

If you will use	Do
option 1	<a href="#">step 2</a>
option 2	<a href="#">step 4</a>

- 2 Disable OSPF by typing  
**#config ip ospf disable**  
 and pressing the Enter key.

- 3 Go to [step 7](#).
- 4 Identify the WAN Edge VLAN ID by typing

```
#show vlan info basic
```

and pressing the Enter key.

Example response

```
=====
Vlan Basic
=====
```

VLAN ID	NAME	TYPE	STG ID	PROTOCOLID	SUBNETADDR	SUBNETMASK
1	Default	byPort	1	none	N/A	N/A
2	SmartBits4Alteon	byPort	1	none	N/A	N/A
9	FP8600-MLT	byPort	1	none	N/A	N/A
10	IST	byPort	1	none	N/A	N/A
11	OM3500-RPR-cards	byPort	1	none	N/A	N/A
12	WAN-Jun-00	byPort	1	none	N/A	N/A
14	toRTPS-1	byPort	1	none	N/A	N/A
15	Backup Path	byIpSubnet	1	none	172.30.242.168	255.255.255.248
19	Alteon6614	byPort	1	none	N/A	N/A
20	RTP4-NGSS	byPort	1	none	N/A	N/A
50	MCS-CallP	byPort	1	none	N/A	N/A

- 5 Identify the ports used for WAN Edge connectivity by typing
- ```
#show vlan info ports <vlan_id>
```
- and pressing the Enter key.

where

**vlan\_id**

is the VLAN ID obtained in [step 4](#)

Example response

```
=====
Vlan Port
=====
```

| VLAN ID | PORT MEMBER | ACTIVE MEMBER | STATIC MEMBER | NOT_ALLOW MEMBER |
|---------|-------------|---------------|---------------|------------------|
| 12      | 1/2         | 1/2           |               |                  |

- 6 Disable the ports used for WAN Edge connectivity by typing
- ```
#config ethernet <port_range_1> state disable
#config ethernet <port_range_2> state disable
...
#config ethernet <port_range_n> state disable
```



and pressing the Enter key.

where

**port\_range\_1**

is a range of ports used for WAN Edge (example: 3/1-3/48)

**port\_range\_2**

is a second range of ports used for WAN Edge (example:  
4/1-4/48)

**port\_range\_n**

is the final range of ports used for WAN Edge

- 7** You have completed this procedure.



---

## Disabling and re-enabling the router ports on the Ethernet Routing Switch 8600

---

### Purpose

When a failure occurs such that Sites A and B are isolated from each other, this procedure should be used to disable and re-enable the Ethernet Routing Switch 8600 router ports that are connected to the GWC in the inactive site.

### Prerequisites

The list of router ports connected to the GWCs should be known.

### Procedure

#### Disabling the router ports on the Ethernet Routing Switch 8600

##### *At the Ethernet Routing Switch 8600 Workstation*

- 1 Confirm which site has the active Call Agent.
- 2 Confirm that the GWCs in the active site are active.
- 3 Disable the ports to the GWC units on the inactive site by typing

```
#config ethernet <port_range_1> state disable
#config ethernet <port_range_2> state disable
...
#config ethernet <port_range_n> state disable
```

and pressing the Enter key.  
where

```
port_range_1
  is a range of ports connected to the GWC (example:
  3/1-3/48)

port_range_2
  is a second range of ports connected to the GWC
  (example: 4/1-4/48)

port_range_n
  is the final range of ports connected to the GWC
```
- 4 If you disabled OSPF in the procedure [Disabling Ethernet Routing Switch 8600 WAN Edge routing on page 639](#), re-enable it by typing

```
#config ip ospf enable
```

and pressing the Enter key.

- 5 If you disabled the ports used for WAN Edge connectivity, re-enable those ports by typing

```
#config ethernet <port_range_1> state enable
#config ethernet <port_range_2> state enable
...
```

```
#config ethernet <port_range_n> state enable
```

and pressing the Enter key.

where

**port\_range\_1**

is a range of ports used for WAN Edge obtained in [step 5](#) of the procedure [Disabling Ethernet Routing Switch 8600 WAN Edge routing](#)

**port\_range\_2**

is a second range of ports used for WAN Edge obtained in [step 5](#) of the procedure [Disabling Ethernet Routing Switch 8600 WAN Edge routing](#)

**port\_range\_n**

is the final range of ports used for WAN Edge obtained in [step 5](#) of the procedure [Disabling Ethernet Routing Switch 8600 WAN Edge routing](#)

- 6 Check the time by typing

```
#date
```

and pressing the Enter key.

Example response

```
local time: THU MAR 31 17:32:57 2005 EST
hardware time: THU MAR 31 22:32:57 2005 UTC
```

- 7 Allow at least one minute to pass to ensure that internal GWC audits set the units to inactive.

- 8 Check the time by typing

```
#date
```

and pressing the Enter key.

Example response

```
local time: THU MAR 31 17:33:59 2005 EST
hardware time: THU MAR 31 22:33:59 2005 UTC
```

- 9 If the inactive building is accessible, verify the inactive GWC units have gone inactive.
  - a Connect the terminal to the console port on the GWC.
  - b Enter PMDEBUG and perform the 'T', 'N', and 'A' commands.
  - c Confirm that the state is inactive. if not, repeat steps 3 through 8 on those ports.
- 10 Re-enable the ports to the GWC units in the inactive site by typing

```
#config ethernet <port_range_1> state enable
#config ethernet <port_range_2> state enable
...
#config ethernet <port_range_n> state enable
```

and pressing the Enter key.

where

**port\_range\_1**  
is a range of ports connected to the GWC (example:  
3/1-3/48)

**port\_range\_2**  
is a second range of ports connected to the GWC  
(example: 4/1-4/48)

**port\_range\_n**  
is the final range of ports connected to the GWC
- 11 You have completed this procedure.



---

## Core and Billing Manager 850 Geographic Survivability

---

### Overview

#### **Core and Billing Manager 850 (CBM 850) hardware and software**

The CBM 850 hardware resides on a carrier-grade, NEBS-compliant Sun Netra 240 server. The hardware can be provisioned either in a PTE2000 cabinet or in an MIS cabinet. The Sun Netra 240 server is designed for high-availability, containing two processors, redundant hot-swap power supplies, and two internal 73 GByte, 15K RPM hot-swap RAID-1 mirrored hard disk drives that provide redundant copies of system data.

The CBM 850 software is built on top of the Nortel Succession Server Platform Foundation Software (SSPFS), which include the Solaris operating system and several software components, tools, and utilities used for managing system equipment and software. SSPFS provides a hardened operating system, routinely exercised with standard security vulnerability detection software.

The base components of the CBM 850 software consist of the process management and platform service subsystems. The process management subsystem provides control, monitoring, alarming, and recovery of the applications and other system processes. The platform services (SSPFS) provide general tools, such as backup and restore, used for administration and maintenance of the platform hardware and software.

#### **Geographic survivability strategy**

The Geographic survivability strategy is built upon the physical distribution of redundant components of the CS 2000 Compact architecture between two different locations and upon utilizing application layer protection. CS 2000 Compact servers can be installed in buildings up to 120 cable kilometers apart. This configuration ensures that operation can resume in the event of catastrophic fault condition at either of the two locations.

### Terminology used in the CBM 850 Geographic Survivability procedures

The following table defines the terms used the CBM 850 Geographic Survivability procedures:

Term	Definition
CBM 850 HA	The high-availability CBM 850, which consists of two Sun Netra 240 servers both commissioned with the Core and Billing Manager SSPFS profile, and installed with cluster=ON.
CBM for GS	One additional CBM 850 server for geographic survivable configurations commissioned as a standby unit, located at a different physical location. This unit is prepared for implementation of the failover procedure in the event of a catastrophic fault condition at the local, main CBM 850 site.
Cluster	Two interconnected redundant units. One unit is active, and the other unit is inactive. The active unit has applications in service (INSV), and ensures that the inactive unit replicated filesystems are updated in real-time. In the event of an automatic cluster failover, the currently-inactive unit becomes the active unit and the formerly-active unit becomes the inactive unit. An automatic cluster failover takes a maximum of 30 seconds.
Sites A and B	The two geographic survivability sites.
CBM 850 HA u0	Unit 0 of the CBM 850 cluster at site B, of the cluster configuration formed by units A0 and A1. This is the mate of CBM 850 HA u1.
CBM 850 HA u1	Unit 1 of the CBM 850 cluster at site B, of the cluster configuration formed by units A0 and A1. This is the mate of CBM 850 HA u0.
CBM 850 u0	The single standby CBM 850 unit at site A. Although clustering is configured on this unit because it will be restored from CBM 850 HA u0 or u1, this unit never has a mate unit.



Term	Definition
Active CBM 850 unit	The CBM 850 HA unit at Site B, (CBM 850 HA u0 or CBM 850 HA u1) which has the application states as in-service (INSV)
Inactive CBM 850 unit	The CBM HA unit at Site A (either CBM 850 HA u0 or CBM 850 HA u1) which has the application states as STANDBY.

### Distribution of OAMP platform

#### CS 2000 Management Tools

The CS 2000 Management Tools and Integrated Element Management System (IEMS) high availability server pairs are located at site A.

#### CBM 850 HA cluster

The CBM 850 high availability server pair is located at site B.

#### Standby Sun servers

In the event of a catastrophic fault condition at one site, the standby Sun servers are brought into service through the manual failover procedure. The Sun servers are positioned, as follows:

- The CS 2000 Management Tools/IEMS standby server will be located in the COAM frame at site B.
- The CBM 850 standby server is located in the Centralized Operations Administration and Maintenance (COAM) frame at site A.

### CBM 850 geographic survivability

The following procedures contain information for OA&M auto backup and accelerated restore capability.

- [Core and Billing Manager 850 Geographic Survivability](#)
- [Scheduling automatic backups of the remote server](#)
- [Viewing configuration information for remote server backups](#)
- [Performing a manual backup of the remote server](#)
- [Viewing logs from a remote backup](#)
- [Initiating a recovery back to the cluster](#)
- [Initiating a switch over to the remote backup server](#)



## Communication Server 2000 Management Tools Geographic Survivability

### Overview

The Communication Server 2000 (CS 2000) Management Tools configuration for Geographic Survivability for the SN08 release consists of two CS 2000 Management Tools active servers at site A which are commissioned as a local HA cluster and one CS 2000 Management Tools (hitherto referred to as CKMT) server at site B which acts as a standby. The standby server is brought into service using a recovery procedure if there is a catastrophic site outage at site A. This section contains the CS 2000 Management Tools manual recovery procedure for disaster recovery by switching activity between sites in the event of a catastrophic fault condition on the CKMT cluster.

### Terminology

The following table defines the terms used in the CKMT Geographic Survivability procedures:

Term	Definition
CKMT HA	The high-availability CKMT product which consists of two Sun Netra 240 servers both commissioned with the CKMT SSPFS profile, and installed with cluster=ON.
CKMT for GS	An additional standby server located at a different physical location. This unit is prepared for implementation of the manual recovery procedure in the event of a catastrophic fault condition at the local, main CKMT HA site.
Cluster	Two interconnected redundant units. One unit is active, and the other is inactive. The active unit has applications in-service (INSV), and ensures that the inactive unit replicated filesystems are updated in real-time. In the event of an automatic cluster failover, the currently inactive unit becomes the active unit and the formerly active unit becomes the inactive unit.
Sites A and B	The two geographic survivability sites. Each site has duplicate configured hardware, with the exception of the CBM 850 and CKMT units.
CKMT HA u0	Unit 0 of the CKMT cluster at site A. One half of the cluster configuration formed by units A0 and A1. This unit is the mate of CKMT HA u1.

Term	Definition
CKMT HA u1	Unit 1 of the CKMT cluster at site A. One half of the cluster configuration formed by units A0 and A1. This unit is the mate of CKMT HA u0.
CKMT u0	The single standby CKMT server at site B. Although clustering is configured on this unit because it will be restored from CKMT HA u0 or u1, it does not have a mate unit.
Active CKMT unit	The CKMT HA unit at site A (either CKMT HA u0 or CKMT HA u1) which has the application states as in-service (INSV).
Inactive CKMT unit	The CKMT HA unit at site A (either CKMT HA u0 or CKMT HA u1) which has the application states as STANDBY.

### Distribution of OAMP platform

The components in an OAMP platform are distributed as follows: The scenarios assume redundant configurations are located in two separate buildings:

- CKMT HA - The CKMT and Integrated Element Management Systems (IEMS) high-availability (HA) server pairs are located at site A.
- CBM 850 HA - The Core and Billing Manager (CBM) high-availability server pair are located at site B.
- Standby Sun servers - In the event of a catastrophic fault condition at one site, the standby Sun servers are brought into service through the manual recovery procedure. The Sun servers are positioned as follows:
  - The CBM 850 standby server is located in the Centralized Operations Administration and Maintenance (COAM) frame at site A.
  - The CS 2000 Management Tools/IEMS standby server is located in the COAM frame at site B.
  - The standby server is brought into service using a manual recovery procedure if there is a total loss of connectivity at the other site.

**Note:** All three servers need to be able to connect to the OAMP LAN. However, if the servers at both site locations are permitted to function on the OAMP LAN at the same time, networks problems with clustering and duplicate IP addresses will occur.

### Required backups on the CKMT servers

There are two types of required backups needed to restore the standby server to functionality following a catastrophic fault condition:

- a full filesystem backup that makes a copy of all the filesystems on the server with the exception of the Oracle filesystem. The OS and third party software application configuration data is captured on DVD-RW discs. The amount of data on the server determines the number of DVD-RW discs required to complete the backup.
- a data-only backup for the data stored in the Oracle database and other application-specific data.

### Prerequisites

Adhering to the prerequisites in this section and the subsequent procedures will help ensure successful completion of geographical survivability manual recovery while holding the maximum out-of-service time for the failover to approximately four hours.

If the documented procedures are not adhered to strictly, longer restoration times will result. Failure to perform the following tasks properly will result in problems:

- full filesystem backup and data backup on the CKMT cluster
- full filesystem restore and data restore to the standby CKMT/IEMS server
- ensuring the CKMT cluster at site A (CKMT HA u0 and u1) and the standby CKMT unit in site B (CKMT u0) are not on-line at the same time

**Note:** Nortel recommends that you perform a full filesystem backup before and after every install, upgrade, or patch application to the CKMT server. The application data in the Oracle database is not automatically backup up, therefore, Nortel recommends daily backups of this data for the best recovery outcomes.

### Communication Server 2000 Management Tools geographic survivability

The following procedures contain information for OA&M auto backup and accelerated restore capability:

- [Installing the remote backup server](#)
- [Scheduling automatic backups of the remote server](#)
- [Viewing configuration information for remote server backups](#)
- [Performing a manual backup of the remote server](#)

- [Viewing logs from a remote backup](#)
- [Initiating a recovery back to the cluster](#)
- [Initiating a switch over to the remote backup server](#)

## Restore operations

Restore operations are performed when it is necessary to apply previously backed-up data to the current component. The following table lists the procedures used to restore CVoIP components.

### Component restoration procedures

Component	Procedure (s)	Page
NETWORK INTELLIGENCE		
CS 2000	<a href="#">Booting the XA-Core from a Reset Terminal</a>	659
Call Agent	<a href="#">Restoring a Call Agent</a> <a href="#">Restoring files from a DVD-RW</a>	665 669
SAM21	<a href="#">SAM21 Shelf Controller reload or restart</a>	681
GWC	<a href="#">Restart or reboot a GWC card</a>	683
Session Server	<a href="#">Session Server - Trunks restore</a>	687
Policy Controller	<a href="#">Prepare for a database restore on a Policy Controller unit</a> <a href="#">Perform a database restore to a Policy Controller unit</a>	673 679
Ethernet Routing Switch 8600	<a href="#">Resetting the Ethernet Routing Switch 8600 using a saved configuration file</a>	699
UAS	<a href="#">Restoring UAS configuration files</a> <a href="#">Restoring audio files to a UAS node</a>	701 705
MS 2000 Series	<a href="#">Restoring audio files to a Media Server 2000 Series node</a>	707
APS	<a href="#">Restoring the APS-specific Oracle database and application files</a>	709
USP	<a href="#">USP Restore Operations</a>	713
Real-time Transport Protocol (RTP) Media Portal	RTP Media Portal Basics, NN10367-111	
CICM	CICM Security and Administration, NN10252-611	
CORE NETWORK		

**Component restoration procedures**

<b>Component</b>	<b>Procedure (s)</b>	<b>Page</b>
Multiservice Switch or Media Gateway devices	<a href="#">Restoring Multiservice Switch or Media Gateway service data</a>	<a href="#">725</a>
<b>GATEWAYS</b>		
MG 9000	none (See <a href="#">Note 1</a> )	
MG 4000	none (See <a href="#">Note 1</a> )	
IW SPM	none (See <a href="#">Note 1</a> )	
<b>NETWORK MANAGEMENT</b>		
Core Element Manager (CEM)	<a href="#">Restoring Core Element Manager data on page 731</a>	<a href="#">731</a>
CS 2000 Core Manager or CBM	<a href="#">Performing a full restore of the software from S-tape</a> <a href="#">Performing a partial restore of the software from S-tape</a> <a href="#">Recovering backup files from lost backup volumes</a>	<a href="#">733</a> <a href="#">745</a> <a href="#">757</a>
CS 2000 Management Tools	<a href="#">Restoring the oracle data on an SSPFS-based server</a> <a href="#">Performing a full system restore on an SPFS-based server</a>	<a href="#">767</a> <a href="#">793</a>
IEMS	<a href="#">Restoring the oracle data on an SSPFS-based server</a> <a href="#">Performing a full system restore on an SPFS-based server</a>	<a href="#">767</a> <a href="#">793</a>
IEMS centralized security server	<a href="#">Restoring the central security server on page 813</a>	<a href="#">813</a>
MG 9000 Manager	<a href="#">Restoring the oracle data on an SSPFS-based server</a> <a href="#">Performing a full system restore on an SPFS-based server</a>	<a href="#">767</a> <a href="#">793</a>
MDM	none (See <a href="#">Note 2</a> )	



**Component restoration procedures**

<b>Component</b>	<b>Procedure (s)</b>	<b>Page</b>
USP Manager	none (See <a href="#">Note 3</a> )	
<p><b>Note 1:</b> The IW SPM and MG 4000 are automatically restored when the CS 2000 is restored. The MG 9000 is restored when the MG 9000 Manager is restored.</p> <p><b>Note 2:</b> The MDM is restored by copying files from tape or an off box storage system through UNIX commands or CRON jobs.</p> <p><b>Note 3:</b> The USP Manager is restored using the two disaster recovery disks created in the "<a href="#">Creating USP Disaster Recovery Floppy Disks</a>" procedure. Insert Disaster Recovery Disk #1 into the A: drive of your OAM&amp;P workstation and follow the instructions.</p>		



## Booting the XA-Core from a Reset Terminal

### ATTENTION

Booting the switch causes the switch to drop all calls.

This procedure boots the XA-Core from a reset terminal display.

**Note:** An image loads from a small computer systems interface (SCSI) device. The SCSI device can be in a disk or a digital audio tape (DAT).

### Common Procedures

There are no common procedures.

### Stepwise Procedure

Use this procedure to boot the XA-Core from a reset terminal display.



#### CAUTION

##### Call your next level of support

Contact your next level of support before performing this procedure.



#### CAUTION

##### Extended service interruption

A longer recovery time occurs for a switch boot from tape than a switch boot from disk.

To minimize recovery time, boot from disk.



#### CAUTION

##### Extended service interruption

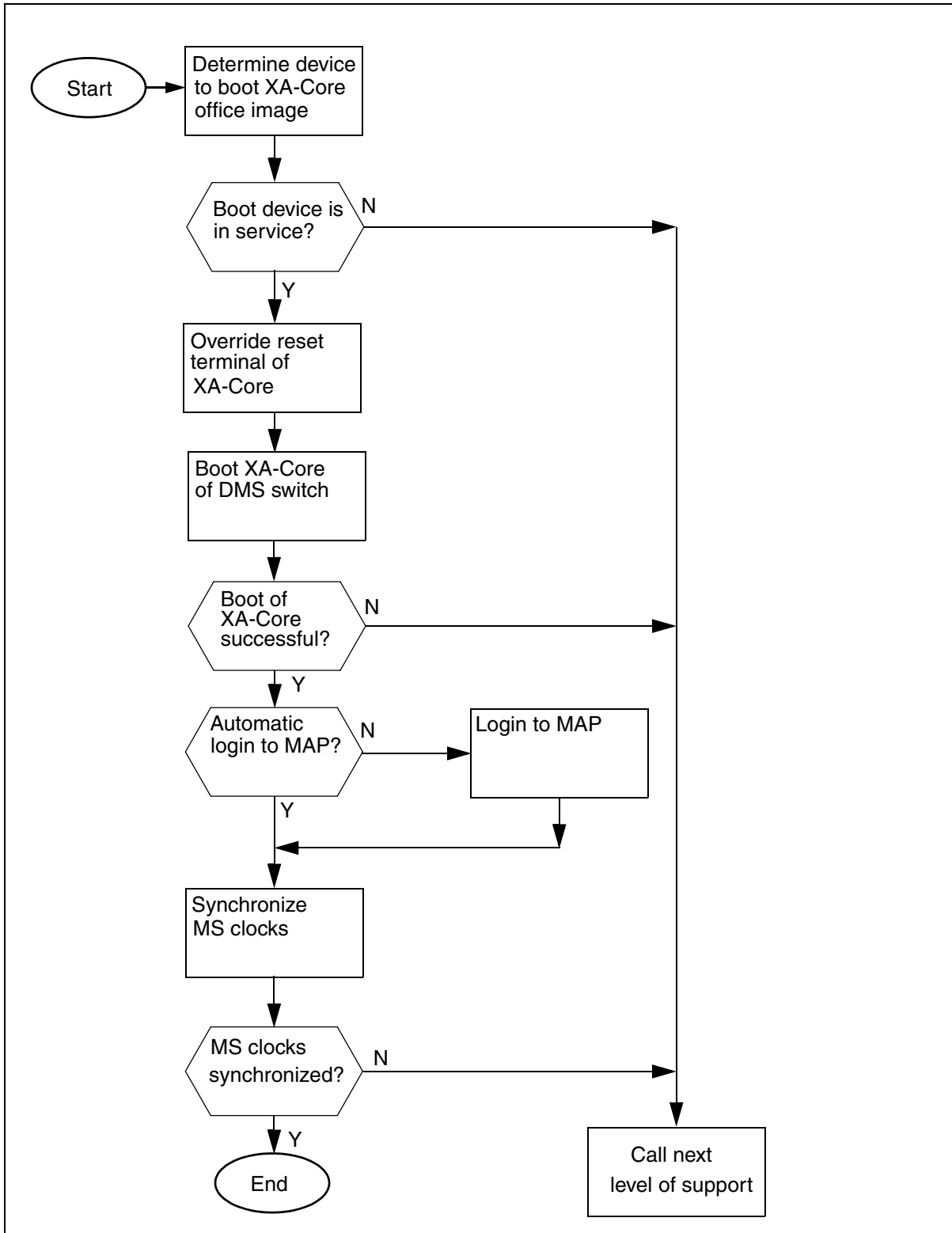
Log-in procedures can vary depending on your office configuration.

If you need additional help, contact your next level of support.

The following flowchart summarizes this recovery procedure.

**Note:** Press the <ENTER> key to execute typed commands.

**Booting an XA-Core from a reset terminal**



## How to boot an XA-Core from a reset terminal

### At your current location

- 1 Refer to office records and determine the name of the XA-Core recording device that contains the last office image file.

**Note:** The XA-Core recording device is a disk drive or a tape drive for a digital audio tape (DAT). Record the name of the XA-Core device.

### At the XA-Core shelf

- 2 Make sure that the disk drive or the tape drive that you recorded in [step 1](#) is in-service.

**Note:** The device is in-service when the green light-emitting diode (LED) is on (illuminated).

If the device is	Do
in service	<a href="#">step 3</a>
not in service	<a href="#">step 13</a>

### At the XA-Core reset terminal

- 3 Override the XA-Core reset terminal by typing:

**>\OVERRIDE**

*Example of a reset terminal response*

```
NOW IN SERVICE AFFECTING MODE
```

- 4 Boot the XA-Core by typing:

**>\BOOT <nn> <s> <p>**

Where:

<nn> is the slot number parameter value to indicate the number of the physical shelf slot - 0 to 18

<s> is the side parameter value to indicate the circuit pack or packlet location in the physical shelf - front (f) or rear (r)

<p> is the position parameter value that indicates the IOP bay - either upper (u) or lower (l)

**Example**

**>\BOOT 4 F L**

*Example of system response:*

Warning: Boot command will take it out of service.

Please confirm ("YES", "Y", "NO", or "N")

Type **Y** to confirm the command.

- 5** Monitor the reset terminal display to determine if the switch has booted.

**Note:** The reset terminal displays a response to indicate a boot in progress. The response also displays diagnostic messages and alphanumeric addresses. When the switch has completely booted, a prompt appears on the display.

*One possible example of a reset terminal response*

CI:

>

*Another possible example of a reset terminal response*

FWCI>

If the response has	Do
a prompt	<a href="#">step 6</a>
no prompt after approximately 15 min	<a href="#">step 13</a>

**At the MAP terminal**

- 6** Press the <BREAK> key to determine if you have to log in.

**Note:** The log-in message indicates that you have to manually log in. An automatic log in can occur if the office parameters have automatic log in.

*Example of a MAP response*

Please Login.

If log in is	Do
not automatic	<a href="#">step 7</a>
automatic	<a href="#">step 10</a>

- 7** Login to the MAP terminal by typing:

>**LOGIN**

*Example of a MAP response*

Enter User Name

- 8** Enter your user name by typing:

**><user\_name>**

Where:

&lt;user\_name&gt; is the name of the user for the account.

*Example of a MAP response*

Enter Password

- 9** Enter the password by typing:

**><password>**

Where:

&lt;password&gt; is the name of the password for the account.

*Example of a MAP response*

SuperNode\_1 Logged in on 1997/01/15 at 20:37:17

- 10** Access the MS Clock level of the MAP display by typing:

**>MAPCI;MTC;MS;CLOCK**

- 11** Synchronize the clocks by typing:

**>SYNC**

<b>If the MAP response is</b>	<b>Do</b>
a successful completion	<a href="#">step 12</a>
a failure	<a href="#">step 13</a>

- 12** You have completed this procedure.

***Non-standard condition found***

- 13** For additional help, contact your next level of support.



## Restoring a Call Agent

This procedure describes how to restore an archived call processing application image from tape.



### CAUTION

#### Possible service interruption

Do not use this procedure when in an emergency situation with no stable call processing application image.

If in a situation without a restartable image, contact Nortel Global Network Product Support (GNPS) immediate. Attempting to use this method without a valid call processing application image could fail due to constant resets on the Call Agent.

### At the SDM

- 1 Insert the DAT cassette with the image to restore.

### At the CS 2000 Core Manager

- 2 Restore the image from tape. This step requires root privilege.

```
# cd /swd/3pc
# tar xvf /dev/rmt0
```

### At the Call Agent Manager

- 3 Log in to the inactive Call Agent and change directory to the location in which to restore the image. Verify that enough disk space exists to hold the image.

```
[mtc@hostname mtc]$ cd /3PC/sd00/image0
[mtc@hostname image0]$ df -h .
Filesystem                Size      Used Avail Use% Mounted on
172.16.16.24:/nfsserv/3pc/cs/sd00
                           8.0G     6.6G   1.4G   82% /3PC/sd00
```

- 4 Open a file transfer protocol (FTP) session to the CS 2000 Core Manager, and transfer the image. It may be necessary to become the super user to transfer the file.

```
[mtc@hostname image0]$ su
Password:<root_password>
[root@hostname image0]# ftp <core_manager_ip>
Connected to <core_manager_ip>
220 <core_manager_ip> SFTPD Server (Version 19.0.0.0 Nov 14
Name (<core_manager_ip>:mtc): root
Password: <root_passwd>
230 User root logged in.
ftp> bin
200 Type set to I.
ftp> cd /swd/3pc %% or location of restored image
250 CWD command successful.
ftp> get IMG_TO_RESTORE
local: IMG_TO_RESTORE remote: IMG_TO_RESTORE
227 Entering Passive Mode (10,40,44,6,195,224)
150 Opening data connection for IMG_TO_RESTORE (binary mode)
226 Transfer complete.
225820860 bytes received in 332 secs (6.7e+02 Kbytes/sec)
ftp> bye
221 Goodbye.
```

### **At the MAP**

- 5 Enter the DISKUT level and use the **IMPORT** command to make the image available to the call processing application.

```
CI:
>DISKUT
Disk utility is now active.
DISKUT:
>IMPORT SD00IMAGE0 IMG_TO_RESTORE IMAGE 1020
  IMG_TO_RESTORE : Failed to get record length.
Import: IMG_TO_RESTORE      size: 199 MB
      as: IMG_TO_RESTORE    lrecl: 1020      type: image.

Attempting to import 1 file selected on SD00IMAGE0.

Imported IMG_TO_RESTORE as IMG_TO_RESTORE.

Imported 1 file successfully of 1 attempt on SD00IMAGE0.
>
```

**Note:** If additional space is needed to import the image, the **IMPORT** command offers to expand the volume.

## 6 Set the image in the Image Table of Contents (ITOC).

```
>QUIT ALL
CI:
>ITOC CI
ITOC User Interface is now active.
ITOC CI:
>SBF CM IMG_TO_RESTORE 15
IMG_TO_RESTORE is registered in CM ITOC.
The updated ITOC is listed directly below.
Image Table Of Contents:
  A Registered          Generic Device      File
  L Date              Time                    Name
  R MM/DD/YYYY HH:MM:SS
-- -
0 * 02/21/2003 16:59:04 SD01ADUMP1          3PC_LAB1_CSNNC06
1   02/24/2003 11:00:53 SD01ADUMP1          3PC_LAB1_CSNNC06
2   02/28/2003 08:15:29 SD00IMAGE0          IMG_TO_RESTORE
>
```

- 7 The restored image is now available for booting.  
This procedure is complete.



## Restoring files from a DVD-RW

### Application

Use this procedure to restore office images from a digital video disk read write optical disk (DVD-RW). Do not restore an image and overwrite one with the same name.

To restore a volume from DVD-RW, contact Nortel support personnel.

### Interval

Perform this procedure when required by your office.

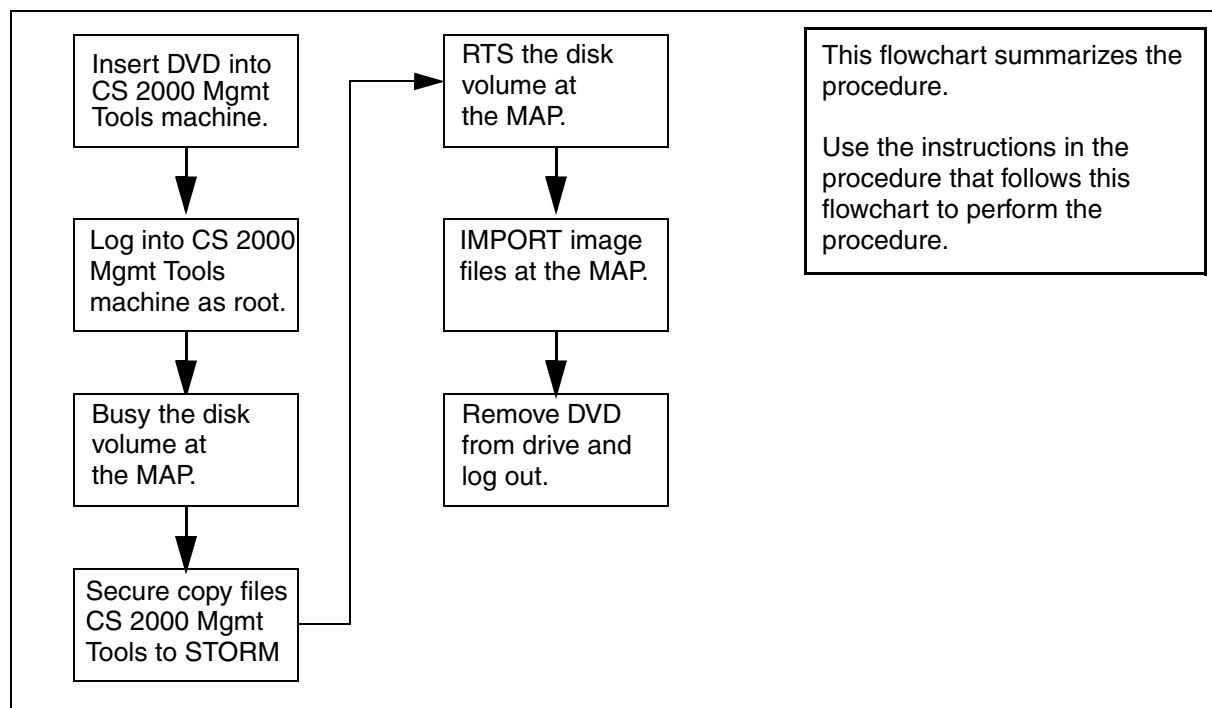
### Common procedures

Understanding of the **IMPORT** command in DISKUT, **SCANF** for listing volumes, and the **CBF**, **LBF**, and **SBF** commands in ITOCCI is required. The IP addresses of the STORM units are needed. Use the **mount** command from a Call Agent card to determine the addresses.

### Action

This procedure contains a summary flowchart as a summary of the procedure. Follow the exact steps to perform this procedure.

#### Summary of restoring files from a DVD-RW



**At the CS 2000 Management Tools server**

- 1 Insert the DVD-RW into the DVD tray. If the CS 2000 Management Tools server is a pair of Sun Microsystems Netra 240s, put the DVD in the unit with the USER LED lit.  
*Volume management software on the CS 2000 Management Tools server operating system mounts the DVD-RW.*
- 2 List the contents:  

```
$ ls -as /cdrom/cdrom0
```

*The contents of the DVD are printed.*
- 3 Change directory to the DVD-RW:  

```
$ cd /cdrom/cdrom0
```

**At the MAP**

- 4 Enter the DISKADM level and busy the volumes to copy:

```
> DISKADM <sd0x>; BSY <volname>
```

```
> QUIT
```

**sd0x**

is SD00 or SD01

**volname**

is the name of the volume such as TEMP

*The BSY command fails if applications have open files on any volume for the device. A busied disk may affect data recording or retrieval for applications. Consider [step 6](#) to RTS the volume as soon as possible or convenient after copying the files.*

*If applications are active and writing to the volume, determine if the application can ROTATE the disk writing activity to a backup volume. If unsure, contact your next level of support.*

**At a CS 2000 Management Tools server terminal**

- 5 Secure copy the files from the DVD-RW on the CS 2000 Management Tools server to one STORage Management (STORM) unit:

```
$ scp "<image_files>"  
"root@<stormip>:</path_to_files>"
```

**image\_files**

is the file name for a single image file, or a wildcard expression such as "\*\_CM"

**stormip**

is the IP Address of the STORM unit such as 172.18.96.6

**/path\_to\_files**

is the absolute path to the files on the STORM unit to place the files such as /nfsserv/3pc/cs/sd00/image1

**Example**

Copy an office image named S040210135002\_CM to SD00IMAGE1:

```
$ scp S040210135002_CM  
"root@<stormip>:/nfsserv/3pc/cs/sd00/image1"
```

**Note:** The first time this command is issued, the secure copy program provides a prompt to exchange keys. Confirm the exchange with a "y."

*The secure copy program provides a progress indicator during the copy. Wait for the copy to complete and the \$ prompt to return.*

**At the MAP**

6 Enter the DISKADM level and RTS the volume:

```
> DISKADM <sd0x>; RTS <volname>  
> QUIT
```

7 Enter the DISKUT level and IMPORT the image files:

```
> DISKUT; IMPORT SD00IMAGE1  
> QUIT
```

*The status of the IMPORT command is printed.*

**IMPORT result**

```
> IMPORT SD00IMAGE1  
Attempting to import 1 fileselected on SD00IMAGE1.  
Imported S040210135002_CM as S040210135002_CM IMAGE 1020.  
Imported 1 file successfully of 1 attempt on SD00IMAGE1.
```

8 List the contents of the volume so the file can be added to the Image Table of Contents (ITOC) in the next step:

```
> SCANF SD00IMAGE1
```

*The contents of the volume are printed.*

- 9 Enter ITOCCI and register the image in the ITOC:
- ```
> ITOCCI
> SBF CM S040210135002_CM <itoc_pos> <alr_flag>
```
- itoc\_pos**  
is an integer between 0 and 15, and is a free position in the ITOC.
- alr\_flag**  
if this image should be booted for the next restart, specify **ALR**. Otherwise, leave the field blank.
- Note:** To determine if a free position is available, use the **LBF CM** command. If all positions are used, clear the file in position 15. Determine which volume the position 15 is on, use **SCANF** to list that volume, and then use the **CBF CM FILE <image\_name>** command.

***At a CS 2000 Management Tools server terminal***

- 10 Unmount the DVD-RW, eject it, and exit from root privilege:
- ```
$ eject cdrom
```

***At the CS 2000 Management Tools server***

- 11 Remove the DVD-RW from the tray and close the tray.
- 12 Store the DVD-RW per office procedure.
- 13 This procedure is complete.



---

## Prepare for a database restore on a Policy Controller unit

---

### Purpose of this procedure

Use this procedure to prepare for a restoration of the Policy Controller application database from a backup copy.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of the high level upgrade activity “Perform an emergency maintenance release rollback activity” found in the Policy Controller Upgrades NTP, NN1xxxx-461.

### Limitations and Restrictions



#### CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

#### ATTENTION

For security reasons, you can only copy the database file from a remote server to the /users/mtc directory on the unit and you must use the secure copy command scp to perform this activity.

Automatic backup of the Policy Controller application database occurs at 1:00 AM each day on both Policy Controller units. This configuration setting cannot be modified and does not impact the use of this procedure.

The name of the backup database file is *solid.db*. Do not modify this name.

### Prerequisites

You must have secure copy (scp) access to the Policy Controller unit from the remote system or other server location from where the database backup file *solid.db* is copied.

## Action

### *From the remote server where the backup database file is located*

- 1 Log onto the remote server, locate and navigate to the directory where the backup copy of the database file is stored.
- 2 Secure copy the database file to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
$ scp solid.db mtc@<PC_IP_address>:
```

and pressing the Enter key.

where

#### **PC\_IP\_address**

is the IP address of the Policy Controller unit

*The database file is copied to the /user/mtc directory on the target Policy Controller unit. This is the only Policy Controller directory that files can be copied into from an external server.*

### *At a Policy Controller command line interface*

- 3 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
> ssh -l <userid> <PC_IP_address>
```

and pressing the Enter key.

where

#### **userid**

is a valid userid (like mtc) on the Policy Controller

#### **PC\_IP\_address**

is the IP address of the Policy Controller

#### **Example**

```
ssh -l mtc 45.128.54.12
```

- 4 Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 5 When prompted, enter the root password.

- 6 Move the `solid.db` file you copied in [step 2](#) from the `/user/mtc` directory to the `/opt/apps/database/solid/backup` directory by typing  

```
$ mv /users/mtc/solid.db  
/opt/apps/database/solid/backup
```

and pressing the Enter key.
- 7 Change directory to the backup database directory by typing  

```
$ cd/opt/apps/database/solid/backup
```

and pressing the Enter key.
- 8 Verify that the correct version (based on the file date) of the `solid.db` database file that you want to restore is located in the directory by typing  

```
$ ls -l /opt/apps/database/solid/backup
```

and pressing the Enter key.
- 9

**ATTENTION**

The `restorebackup.sh` script does not run if you do not have the `solid.ini` and `solmsg.out` files located in the correct directory.

- Verify that the presence of files `solid.ini` and `solmsg.out` files are also in the `/opt/apps/database/solid/backup` directory.
- 10 If the `solid.ini` file is not present, copy it into the backup directory by typing  

```
$ cp /opt/apps/database/solid/dbfiles/solid.ini  
/opt/apps/database/solid/backup/solid.ini
```

and pressing the Enter key
  - 11 If the `solmsg.out` file is not present, copy it into the backup directory by typing  

```
$ cp  
/opt/apps/database/solid/dbfiles/solmsg.out  
/opt/apps/database/solid/backup/solmsg.out
```

and pressing the Enter key
  - 12 Change the ownership of all files in the backup directory by typing  

```
$ chown soliddb *
```

and pressing the Enter key.

- 13 Change the group of all files in the backup directory by typing  
`$ chgrp adm *`  
and pressing the Enter key.
- 14 Change the access permissions for all files in the backup directory by typing  
`$ chmod 600 *`  
and pressing the Enter key.
- 15 The database is now ready to be restored. You have completed this procedure. Return to the high-level activity.

### Additional information

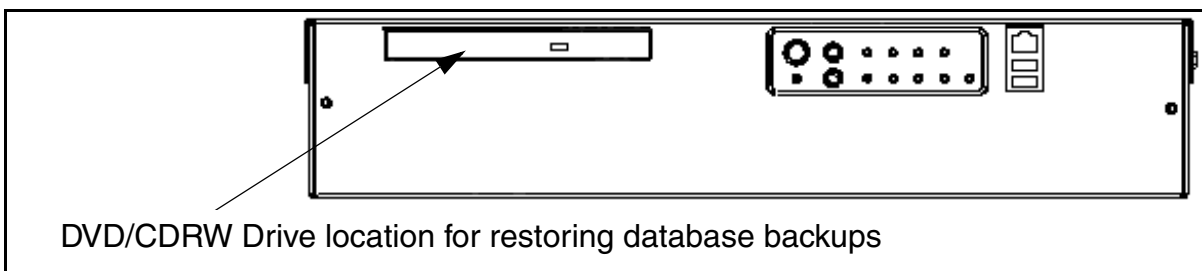
This section provides additional information regarding database restore activities.

#### To restore a backup database saved to a CD.

If you must restore a database backup that has been saved to a CD, you must first copy the database file from the CD to the default backup directory on the active Policy Controller unit. The selected backup database file must be restored to the following location:

*/opt/apps/database/solid/backup/solid.db*

To restore a backup of the database file to the backup directory, you must use a Policy Controller command line interface to copy the database file from a CD or CD-RW disk containing a copy of the backup database file to the `opt/apps/database/solid/backup` directory.



Ensure that you remove the CD disk from the DVD/CDRW drive, and store it in a safe place when you are done.

#### To restore a database backup save to another system

If you must restore a database backup that has been saved to another system, you must first copy the database file from the remote system back to the default backup directory on the active Policy Controller unit.

The selected backup database file must be restored to the following location:

*/opt/apps/database/solid/backup*

To restore a backup of the database to the backup directory you must use a Policy Controller command line interface to copy the database file `solid.db` from the remote system to the `opt/apps/database/solid/backup` directory. You may also be able to remote copy the backup database file from the remote system to the Policy Controller `opt/apps/database/solid/backup` directory. However, for security reasons, you may need to consult your site network administrator for instructions and permission to perform a remote copy.



---

## Perform a database restore to a Policy Controller unit

---

### Purpose of this procedure

Use this service impacting procedure to restore a Policy Controller application database from a backup copy to either the active or inactive Policy Controller units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of the high level upgrade activity “Perform an emergency maintenance release rollback activity” found in the Policy Controller Upgrades NTP, NN10431-461.

### Limitations and Restrictions



#### CAUTION

Performing a restore of the Policy Controller application database is a service affecting activity and can cause data mismatches at the Communication Server 2000.

### Prerequisites

You must first have completed procedure [Prepare for a database restore on a Policy Controller unit on page 673](#).

### Action

#### *At a Policy Controller command line interface*

- 1 Open a secure shell to the Policy Controller unit you are restoring a backup copy of the database to by typing

```
> ssh -l <userid> <PC_IP_address>
```

and pressing the Enter key.

where

**userid**

is a valid userid (like mtc) on the Policy Controller

**PC\_IP\_address**

is the IP address of either Policy Controller unit

**Example**

```
ssh -l mtc 45.128.54.12
```

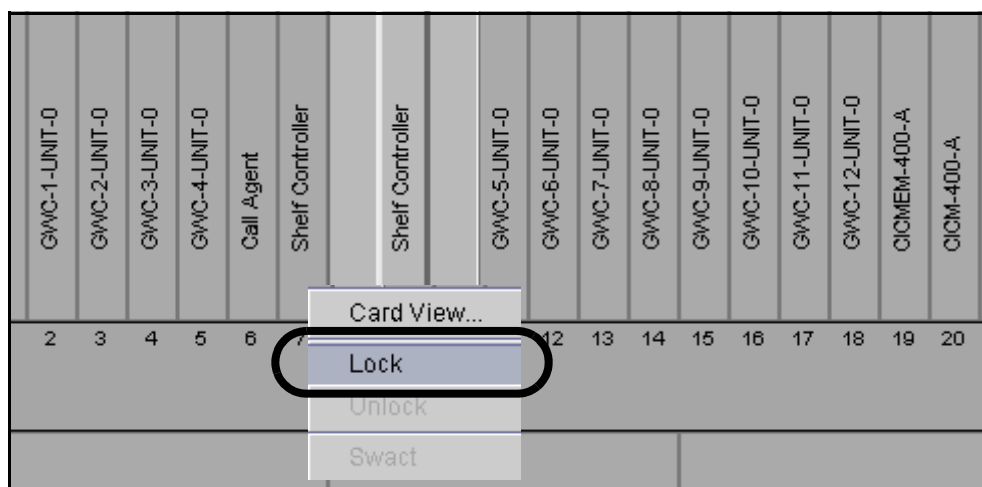
- 2 Change to the root user by typing  
**\$ su - root**  
and pressing the Enter key.
- 3 When prompted, enter the root password.
- 4 Change directories by typing  
**\$ /opt/apps/database/solid\_install**  
and pressing the Enter key.
- 5 Run the database restore script by typing  
**\$ ./restorebackup.sh**  
and pressing the Enter key.
- 6 You have completed this procedure. Return to the high-level activity.



## SAM21 Shelf Controller reload or restart

### *At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right click on the card and select Lock from the context menu.



- 2 Wait for the lock icon to appear on the selected card and the other SAM21 Shelf Controller to indicate that it is in simplex (alarm 2C on the other SAM21 Shelf Controller).
- 3 Right click on the card again and select Unlock from the context menu.  
The card resets, downloads software, and reboots.
- 4 This procedure is complete.



---

## Restart or reboot a GWC card

---

### Purpose of this procedure

Use this procedure to stop all software processes on the GWC card, performs a hardware reset, and reloads the GWC card software from the CS 2000 Core Manager or Core and Billing Manager (CBM).

### When to use this procedure

Use this procedure when you need to reboot a GWC card and force a GWC to download and execute a software load from the The CS 2000 Core Manager or CBM.

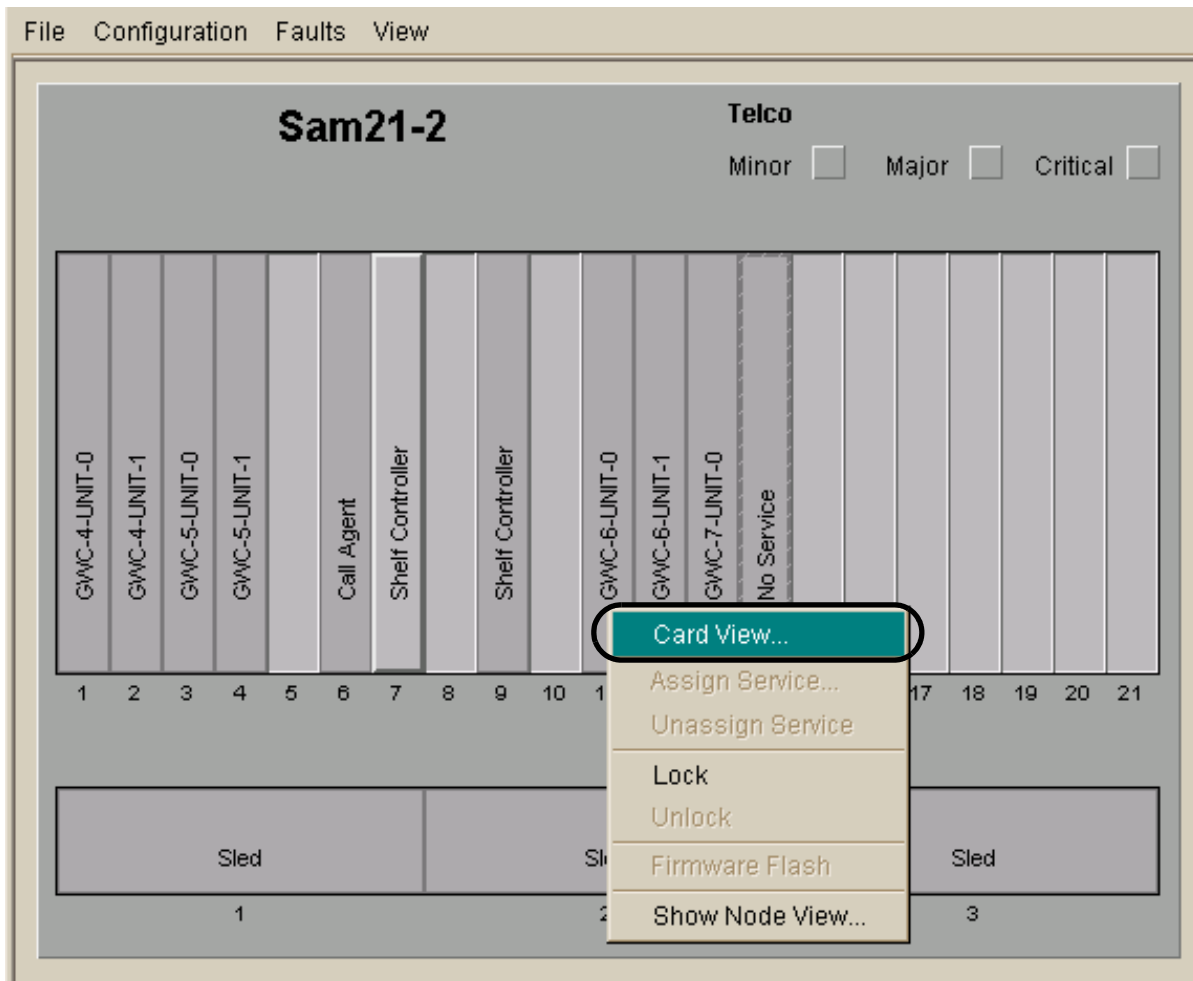
### Prerequisites

To reduce the risk of service interruption, you can first busy the GWC applications on specific GWC nodes using the CS 2000 GWC Manager. Refer to the Gateway Controller Security and Administration NTP, NN10213-611, for these procedures.

## Action

### *At the CS 2000 SAM21 Manager client*

- 1 From the Shelf View, right-click the GWC card you want to reboot and select **Card View** from the context menu.



- 2 At the Card View, select the **States** tab.

File View

### Sam21-2 : Slot 11

Alarms | Equip | **States** | Diags | Provisioning

Summary

Critical	Major	Minor
0	0	0

Details

Equip.	ID	Time	Type	Severity	Reason
--------	----	------	------	----------	--------

GWC-6-UNIT-0

11

- 3 Click the **Lock** button to lock the card.

**Note:** The card must be busy (disabled) before you can lock it. Refer to the procedure “Disable (Busy) GWC card services” in the Gateway Controller Security and Administration NTP, NN10213-611.

File View

### Sam21-2 : Slot 12

Alarms | Equip | **States** | Diags | Provisioning

OSI

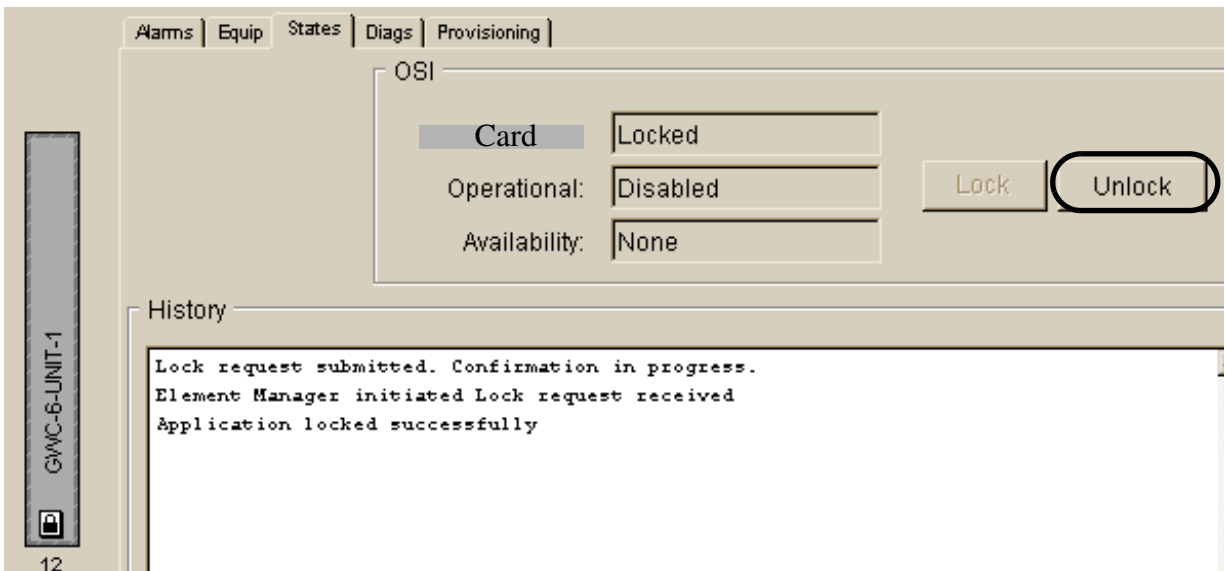
Card	Unlocked
Operational:	Enabled
Availability:	None

Lock Unlock

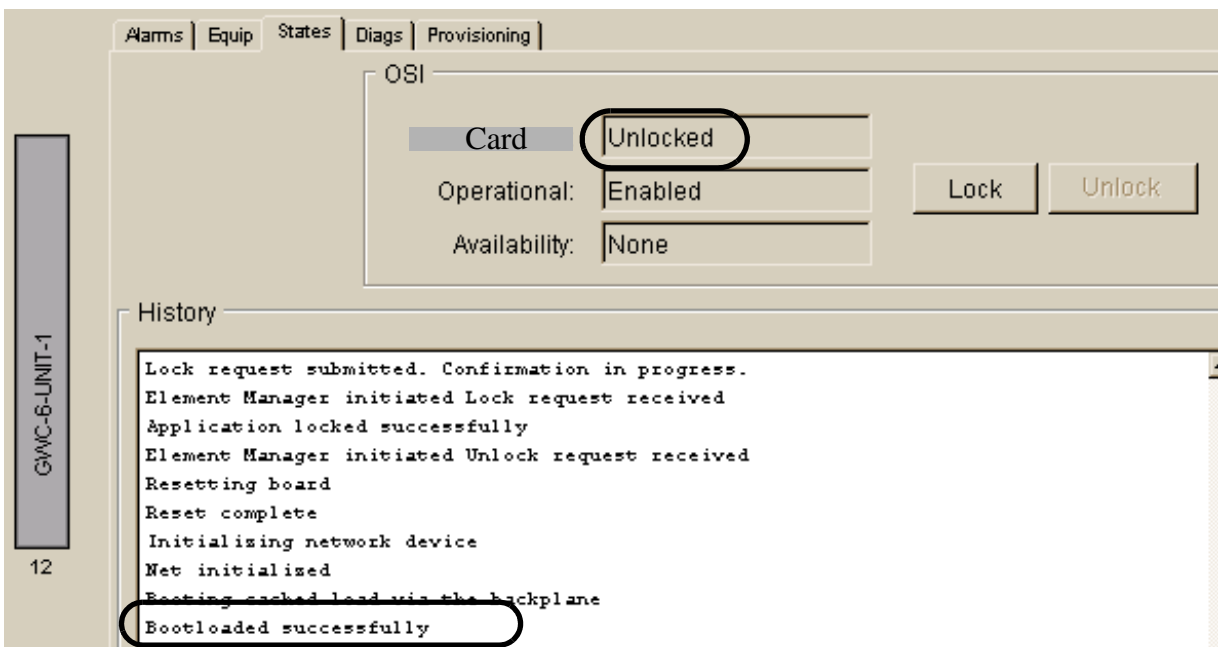
History

3-UNIT-1

- 4 Wait until the Card Status is Locked and the History window indicates “Application locked successfully”. Then, click the **Unlock** button.



- 5 Monitor the reboot process. Wait until the Card Status is “Unlocked” and the History window indicates “Bootloaded successfully”.



- 6 This procedure is complete.

---

## Session Server - Trunks restore

---

### Purpose of this procedure

Use this procedure to restore a backup copy of critical files to a unit.

### Limitations and Restrictions

**CAUTION****Possible service disruption**

Performing a restore of the SIP Gateway application database to the active unit is a service affecting activity and can cause data mismatches at the CS 2000.

### Prerequisites

You must have secure file transfer access, such as scp, to the unit from a remote host if the backup file is stored on a remote host.

Backups are also stored locally on each unit in directory /data/bkresmgr/backup.

### Action

***From the remote server where the backup database file is located***

- 1 If the backup is stored on a remote host, copy the backup file to the unit.

To use a secure copy, type

```
scp <backupfile> mtc@<ip_address>:<dest_dir>
```

where

**backupfile**

is a value like unit0.backupfile.2005-04-12\_17-10.tgz and is identified by the hostname, date, and time that the backup occurred

**ip\_address**

is the IP address of the unit

**dest\_dir**

is the location to put the backupfile and is either blank to place it in /users/mtc, or a full path such as /data/bkresmgr/restore

*The database file is copied to the target unit. If the local workstation is not on the CS LAN, copy the backup file to the server hosting the CS 2000 Management Tools first, and then transfer it between the server hosting the CS 2000 Management Tools and the Session Server - Trunks unit.*

**At the NCGL CLI or IEMS client**

- 2 Log in to the unit and change to the root user.
- 3 If the backup file was not transferred directly to /data/bkresmgr/restore, then move the backup file:

```
mv /users/mtc/<backupfile>  
/data/bkresmgr/restore
```

**Note:** If restoring a local backup, the backup file is located in /data/bkresmgr/backup.

- 4 Change directory to the restore directory:

```
cd /data/bkresmgr/restore
```

- 5 Uncompress the backup:

```
tar xvzf <backupfile>.tgz
```

*A listing of the files is printed to the screen and the files to restore are located in /data/bkresmgr/restore/data/bkresmgr/temp.*

- 6 Change directory to the files:

```
cd /data/bkresmgr/restore/data/bkresmgr/temp
```

**Jam the inactive unit and suspend call processing****At the CS 2000 Session Server Manager or IEMS client**

- 7 Select Session Server > Maintenance > Platform > Node Maintenance from the left side menu.

*The Node Maintenance panel opens in the right side.*

- 8 Click Jam.

*Two JInact alarms are raised.*

- 9 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.



*The SIP Gateway Maintenance page opens in the right side.*

- 10 Click Lock.
- 11 Click Suspend.
- 12 Perform any of the following restore activities and then perform [Unsuspend call processing and Unjam the inactive unit on page 692](#).
  - [Restore database on page 689](#)
  - [Restore system data on page 690](#)
  - [Restore web files on page 691](#)
  - [Manual restore of security related files on page 692](#) — these files are stored in a separate backup file, but restoring them as part of this procedure avoids an additional web server restart

### **Restore database**

Perform these steps only if the database corruption has occurred on both units. The database must be restored on the active unit.

#### ***At the NCGL CLI or IEMS client***

- 13 Copy the database files:

```
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
```
- 14 Set the attributes for the files in the backup directory:

```
chown soliddb /opt/apps/database/solid/backup/*
chgrp adm /opt/apps/database/solid/backup/*
chmod 700 /opt/apps/database/solid/backup/*
```
- 15 Restore the backup files:

```
/opt/apps/database/solid_install/restorebackup
.sh
```

*The following status is printed to the screen. The database on the inactive unit is synchronized to the restored database on the active unit.*

```
Restoring database from backup
Stopping dbwatchdog.sh:          [ OK ]
Stopping soliddb.sh:            [ OK ]
Starting soliddb.sh:            [ OK ]
Solid SQL Editor (teletype) v.04.10.0139
(C) Copyright Solid Information Technology Ltd 1993-2004
Execute SQL statements terminated by a semicolon.
Exit by giving command: exit;
Connected to 'tcp 1315'.
admin command 'hsb set primary alone'
  RC TEXT
  -- ----
  0 HotStandby server set to PRIMARY ALONE.
1 rows fetched.

admin command 'hsb netcopy'
  RC TEXT
  -- ----
  0 Copy started.
1 rows fetched.
```

- 16** If the database is the only item to restore, then unsuspend, unlock, and unjam the inactive unit. Refer to [Unsuspend call processing and Unjam the inactive unit on page 692](#) for assistance.

## Restore system data

### *At the NCGL CLI or IEMS client*

- 17** Copy the necessary files:
- ```
cd /data/bkresmgr/restore/data/bkresmgr/temp
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_host_rsa_key.pub
/opt/base/synch_local/common/etc/ssh
```

18 Set the permissions on the restored files:

```
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_host_
rsa_key.pub
```

## Restore web files

### *At the NCGL CLI or IEMS client*

19 Copy the files:

```
cd /data/bkresmgr/restore/data/bkresmgr/temp
cp -i redirect*.jsp
/opt/apps/webint/jakarta-tomcat-4.1.30/webapps
/<tag_name>/jsp
cp -i redirect_apps.php
/usr/local/apache/htdocs
```

## Unsuspend call processing and Unjam the inactive unit

### *At the CS 2000 Session Server Manager or IEMS client*

- 20 Select Session Server > Maintenance > Application > SIP Gateway from the left side menu.
- 21 Click Unsuspend.
- 22 Click Unlock.
- 23 Select Session Server > Maintenance > Platform > Node Maintenance from the left side menu.
- 24 Click Unjam.
- 25 This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.

## Manual restore of security related files

Security related files are not stored in the automatically generated backup to guard against compromise of the keys in the event that a backup is stolen or misplaced.

Restored security files must be the same on both units of a node.

Locate the manual backup of security related files and restore the following files:

- /opt/base/share/ssl/certificate.keystore
- /opt/base/share/ssl/gen\_cert.txt
- /opt/base/share/ssl/server.crt
- /opt/base/share/ssl/server.key
- /opt/base/share/ssl/trusted.crt

**Note:** If the unit is running SN09 software, optionally restore the files listed above to a location such as /users/mtc, and then use the cert\_mgnt tool with option 3, Import certificates and private key, to restore the files to /opt/base/share/ssl and set the permissions correctly.

- /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\_host\_rsa\_key

### *At the NCGL CLI or IEMS*

- 1 Become the root user.

- 2** Change directories to the location where the backup of the security certificates are stored:

```
cd /opt/base/share/ssl/<SNxx_ddmmyyyy>
```

where

**SNxx\_ddmmyyyy**

is the name of the backup directory

**Example**

```
cd /opt/base/share/ssl/SN09_12102005
```

- 3** Verify the contents of the backup directory:

```
ls -l
```

*Sample system response:*

```
-rw-r--r--  1 root   root   1858 Dec 10 11:11
certificate.keystore
-rw-r--r--  1 root   root    190 Dec 10 11:11
gen_cert.txt
-rw-r--r--  1 root   root   3249 Dec 10 11:11
server.crt
-rw-----  1 root   root    887 Dec 10 11:11
server.key
-rw-r--r--  1 root   root   1254 Dec 10 11:11
trusted.crt
```

- 4** Determine your next step:

| <b>If</b>  | <b>Do</b>   |
|--|---|
| the backup directory is empty or contains files other than those shown in the previous example   | You are either in the wrong backup directory or you did not properly back up the security certificates. If necessary, contact Nortel GNPS for assistance. This procedure is complete. |
| the backup directory contains files similar to the display and the running software load is SN09                                       | Run <b>cert_mgmt</b> and choose option 3. This restores the files and sets permissions correctly. This procedure is complete.   |
| the backup directory contains files similar to the example shown in the previous step and the running software load is older than SN09 | Continue to <a href="#">step 5</a> to copy the files and set permissions manually.  |

- 5 Copy the files to the /opt/base/share/ssl directory:

```
cp * /opt/base/share/ssl
```

**ATTENTION**

This step overwrites the current security certificates on this unit.

- 6 Change directories to the /opt/base/share/ssl directory:

```
cd /opt/base/share/ssl
```

- 7 Verify the contents of the backup directory were restored:

```
ls -l
```

*Sample system response:*

```
-rw-r--r-- 1 root root 1858 Dec 10 11:11
certificate.keystore
-rw-r--r-- 1 root root 190 Dec 10 11:11
gen_cert.txt
-rw-r--r-- 1 root root 3249 Dec 10 11:11
server.crt
-rw----- 1 root root 887 Dec 10 11:11
server.key
-rw-r--r-- 1 root root 1254 Dec 10 11:11
trusted.crt
```

**Note:** File size values will vary.

- 8 Set the permissions for the restored files:

```
chown root:root *
```

```
chmod 644 server.crt
```

```
chmod 644 gen_cert.txt
```

```
chmod 600 certificate.keystore
```

```
chmod 600 server.key
```

```
chmod 644 trusted.crt
```

- 9 Perform the steps in [Jam the inactive unit and suspend call processing on page 688](#).

- 10 Enter the following commands to restart the applications that use the restored files:

```
/usr/local/apache/bin/apachectl restart
```

```
/opt/apps/webint/tomcatd restart
```

```
/etc/init.d/sshd restart
```

- 11** Perform the steps in [Unsuspend call processing and Unjam the inactive unit on page 692](#)
- 12** Repeat this procedure on the mate unit.
- 13** This procedure is complete. If applicable, return to the higher level task flow or procedure that directed you to this procedure.





---

## Perform a database restore to a Session Server unit

---

### Purpose of this procedure

Use this service impacting procedure to restore a SIP Gateway application database from a backup copy to the active Session Server units.

This procedure should only be used as part of a high-level fault management activity for restoring a backup copy over a corrupted version of the database, or as part of a high level upgrade activity, found in the Session Server Upgrades NTP, NN10349-461.

### Limitations and Restrictions



#### CAUTION

This procedure can only be executed on the active unit. Performing a restore of the SIP Gateway application database to the active unit is service affecting, and can cause data mismatches at the CS 2000 call server.

### Prerequisites

You must first have completed procedure [Session Server - Trunks restore on page 687](#).

### Action

#### *At the Session Server CLI or Integrated EMS client*

- 1 Log onto the active Session Server unit you are restoring a backup copy of the database to, and change to the root user.
- 2 Change directories by typing  

```
$ cd /opt/apps/database/solid_install
```

and pressing the Enter key.
- 3 Run the database restore script by typing  

```
$ ./restorebackup.sh
```

and pressing the Enter key.
- 4 You have completed this procedure. Return to the high-level activity.



---

## Resetting the Ethernet Routing Switch 8600 using a saved configuration file

---

The Ethernet Routing Switch 8600 boot command allows you to reset or reboot the system using a saved configuration file. You must have access to the Boot Monitor CLI through a direct connection to the switch or a Telnet connection. For more information on accessing the Boot Monitor CLI, refer to "Managing the Ethernet Routing Switch 8000 Series Switch Using the Command Line Interface Release 3.2," 313194-A.

**Note:** You must be directly connected to the switch to initiate a Boot Monitor session. You can only connect using a Telnet connection if the Boot Monitor CLI is already active.

### Resetting the Ethernet Routing Switch 8600 using a saved configuration file

#### *At the Boot Monitor CLI*

- 1 Issue the boot command by typing

```
monitor# boot [<file>] [config <value>]
```

where

**file**

is the software image device and file name in the format [a.b.c.d:]<file> | /pcmcia/<file> | /flash/<file>. The file name, including the directory structure, can be up to 1024 characters.

**config <value>**

is the software configuration device and file name in the format [a.b.c.d:]<file> | /pcmcia/<file> | /flash/<file>. The file name, including the directory structure, can be up to 1024 characters.

- 2 You have completed this procedure.



---

## Restoring UAS configuration files

---

At the time of installation, the UAS is configured to automatically back up configuration files each day at 2:00 am. If an APS node is configured in the network, all UAS nodes in the network can be backed up to the APS node. If an APS node is not configured in the network, the configuration files for UAS nodes in the network can be backed up, instead, to a remote UNIX server.

The backed-up files can be restored should a catastrophic system event, such as a hard disk drive failure, create the need for a re-installation. The files are restored by manually transferring the files from the APS node or remote UNIX server to the UAS node after the UAS software (and NGS software, if necessary) has been re-installed. The backed-up files are located in the directory, /opt/uas/uas\_conf\_backup and include:

- C:\UAS\etc\UAS.conf (all configurations)
- C:\UAS\etc\ugw.conf (for a PRI gateway only)
- C:\UAS\etc\atmconn.con (ATM only)
- C:\UAS\etc\mainasa.conf (all configurations)
- C:\UAS\etc\atmhard.con (ATM only)
- C:\etc\srfconf\agt\snmpd.cnf (all configurations)
- C:\Winnt\system32\drivers\etc\hosts (all configurations)
- C:\UAS\etc\atmSvcProfile.con (ATM only)
- C:\UAS\etc\atmhardloop.con (ATM only)

This procedure enables you to restore backed-up UAS configuration files that are stored either on an APS node or on a remote UNIX server.

### Restoring UAS configuration files

#### ***At the Network Element Status panel of the Universal Audio Server Manager***

- 1 In the Network Elements pane, select the appropriate UAS node. Information about the node displays in the System Identification pane.
- 2 In the pull-down list in the box labeled, "Please select," select Maintenance.
- 3 In the Maintenance Tree pane, select "Node".

- 4 Click the node entry that displays in the table shown in the Node States pane.
- 5 Lock the node by clicking the “Lock Graceful” button located at the bottom of the Node States pane.

### ***At the Windows desktop interface***

- 6 Log in as Administrator.
- 7 Stop any applications that are running.
  - a Access the “Services” window as follows:  
**select Start -> Programs -> Administrative Tools -> Services**
  - b Right-click PMGRdaemon service and select Stop. Wait for notification that the applications have stopped.
- 8 Perform the following steps:
  - a Enter the following command:  
**cd \UAS\etc**
  - b Access the APS server directory containing the backed up configuration files by entering the following:  
**mount \* \\<APS IP address>\opt\uas\uas\_conf\_backup\<UAS node>\current (all of this command is entered on one line)**  
where <APS IP address> is the address of the server containing the backed up configuration files, and <UAS node> is the full directory path that contains the name of the UAS node that you are restoring the backed up configuration files to.
  - c Execute the following command to confirm that the directory containing the backed-up configuration files is mounted:  
**net use**
  - d Change directories to the location of the newly mounted configuration file backup directory by entering the following:  
**cd <mounted drive letter>**  
where <mounted drive letter> is the drive letter (for example, “F”) displayed as the result of the previous command.
  - e List the contents of the configuration file backup directory by entering the following command in response to the prompt:  
**ls -l**

The following backed up files should display:

- UAS.conf (for all configurations)
- ugw.conf (for a PRI gateway only)
- atmconn.con (for ATM only)
- mainsa.conf (for all configurations)
- atmhard.con (for ATM only)
- snmpd.cnf (for all configurations)
- hosts (for all configurations)
- atmSvcProfile.con (for ATM only)
- atmhardloop.con (for ATM only)

- f** Enter the following command to copy the contents of the mounted configuration file backup directory to the appropriate subdirectory on your UAS:

```
copy *.* c:\UAS\etc\
```

- g** Unmount the configuration file backup directory by entering the following command:

```
umount <drive letter>
```

where <drive letter> is the drive letter that you entered in step [d](#).

- h** At the system console, perform the following steps:

```
mv snmpd.cnf \etc\srconf\agt\snmpd.cnf
```

```
mv hosts \Winnt\system32\drivers\etc\hosts
```

- 9** Restart the network element by performing the following steps:

- a** Access the “Services” window as follows:

```
select Start -> Programs -> Administrative Tools -> Services
```

- b** Right-click PMGRdaemon service and select Start.

***At the Network Element Status panel of the Universal Audio Server Manager***

- 10** In the Network Elements pane, select the appropriate UAS node. Information about the node displays in the System Identification pane.
- 11** In the pull-down list in the box labeled, “Please select,” select Maintenance.

- 12** In the Maintenance Tree pane, select “Node”.
- 13** Click the node entry that displays in the table shown in the Node States pane.
- 14** Unlock the node by clicking the “Unlock” button located at the bottom of the Node States pane.
- 15** You have completed this procedure.



## Restoring audio files to a UAS node

In the event that a re-installation of a UAS node is required due to an error condition, audio files must be restored to the unit when it becomes operational. This procedure allows you to enable audio provisioning to the node and to specify which audio files are to be restored to it.

**Note:** For more information about re-installation of a UAS node, contact your Nortel Networks service representative.

### Restoring audio files to a UAS node

#### At your web browser interface

- 1 After the re-installation of the UAS node has been completed, determine whether you want to enable provisioning of the node occur during the next audio distribution cycle or immediately.

---

#### If

#### Do

you want to enable provisioning of the node to occur during the next audio distribution cycle

step [2](#)

you want audio provisioning of the node to occur immediately

step [3](#)

- 2 Perform the procedure “Enabling provisioning of a UAS node” in the document, NN10095-511, entitled “UAS Configuration Management,” in your UAS document suite.

**Note:** Provisioning of the node will begin during the next audio distribution cycle. The distribution cycle occurs once per hour.

- a Go to step [4](#).

- 3 Perform the procedure “Provisioning a UAS node” in the document, NN10095-511, entitled “UAS Configuration Management,” in your UAS document suite.

**Note:** Provisioning of the node will begin immediately although as much as a five-minute delay may occur before actual provisioning activity begins.

- 4 You have completed this procedure.



## Restoring audio files to a Media Server 2000 Series node

In the event that a re-installation of a Media Server 2000 Series node is required due to an error condition, audio files must be restored to the unit when it becomes operational. This procedure allows you to enable audio provisioning to the node and to specify which audio files are to be restored to it.

**Note:** For more information about re-installation of a Media Server 2000 Series node, contact your Nortel Networks service representative.

### Restoring audio files to a Media Server 2000 Series node

#### At your web browser interface

- 1 After the re-installation of the Media Server 2000 Series node has been completed, determine whether you want to enable provisioning of the node occur during the next audio distribution cycle or immediately.

---

#### If

you want to enable provisioning of the node to occur during the next audio distribution cycle

#### Do

step [2](#)

you want audio provisioning of the node to occur immediately

step [3](#)

---

- 2 Perform the “Enabling provisioning of a Media Server 2000 Series node” (refer to the Media Server 2000 Series Configuration Management document).

**Note:** Provisioning of the node will begin during the next audio distribution cycle. The distribution cycle occurs once per hour.

- a Go to step [4](#).

- 3 Perform the procedure “Provisioning a Media Server 2000 Series node” (refer to the Media Server 2000 Series Configuration Management document).

**Note:** Provisioning of the node will begin immediately although as much as a five-minute delay may occur before actual provisioning activity begins.

- 4 You have completed this procedure.



## Restoring the APS-specific Oracle database and application files

To ensure successful recovery from a system problem that causes database file corruption, you should periodically back up the database files that support operation of the APS. These files include:

- Oracle database
- Root database files
- Non-Root database files

The Succession Server Platform Foundation Software (SSPFS) base software provides utilities that enable you to restore these files. The “rsimpora” utility restores the APS Oracle database files. The “ufsrestore” utility restores the UNIX file system, including all of the “Root” and “Non-Root” APS database files.

The instructions for performing these backup procedures are found in the document titled *ATM/IP Configuration*, NN10276-500.

In addition to these two utilities, two additional APS utilities and procedures enable you to restore selected files when only the files required for APS operation must be restored. The “ips\_export\_db.sh -restore” utility restores only the APS Oracle database. A procedure that utilizes the UNIX “tar” command enables you to restore the non-Root files, “/audio\_files,” “/PROV\_data,” “/user\_audiofiles,” and Root file, “/etc/inet/hosts.”

This procedure enables you to restore the APS-specific Oracle database and application files (/PROV\_data, /audio\_files, and /user\_audio\_files).

### Restoring the APS-specific Oracle database and application files

#### *In a telnet connection to the APS server*

- 1 Open an xterm window and log in using the “maint” login and password.
- 2 Become the “root” user by entering:  
**su - root**
- 3 Determine whether you are restoring Oracle database files from tape or from disk.

---

**If**

you are restoring from tape

---

**Do**

step [4](#)

---

---

|  | <b>If</b>                   | <b>Do</b>              |
|--|-----------------------------|------------------------|
|  | you are restoring from disk | step <a href="#">9</a> |

---

- 4 Insert the appropriate “ORACLE” backup tape into the DDS-3 tape drive.
- 5 Rewind the backup tape by performing the following command:  

```
mt -f /dev/rmt/0c rewind
```
- 6 Start the restoration of the APS Oracle database from the tape by entering the following command:  

```
ips_export_db.sh -t /dev/rmt/0c -restore
```

**Note:** This command is entered on a single line.

Messages logging the progress of the restoration display on the screen. When you are prompted about continuing the restoration even if the current database will be destroyed, enter “y” (yes).
- 7 After the restoration of the Oracle database is complete, rewind the backup tape by performing the following command:  

```
mt -f /dev/rmt/0c rewind
```
- 8 Eject the backup tape and store it for possible use later.
  - a Go to step [10](#).
- 9 Start the restoration of the APS Oracle database from the disk by entering the following command:  

```
ips_export_db.sh -diskonly -restore
```

**Note:** This command is entered on a single line.

Messages logging the progress of the restoration display on the screen. When you are prompted about continuing the restoration even if the current database will be destroyed, enter “y” (yes).
- 10 Insert the appropriate “application file” backup tape into the DDS-3 tape drive.
- 11 Change directory to the root directory:  

```
cd /
```
- 12 Rewind the backup tape by performing the following command:  

```
mt -f /dev/rmt/0c rewind
```
- 13 Restore the application files (/PROV\_data, /audio\_files, and /user\_audio\_files) by entering the following command:  

```
tar xvf /dev/rmt/0c
```

- 14** When the restoration of the application files completes, remove the tape from the tape drive and store for possible use later. Insert another write-enabled DAT tape into the drive to be used for the automatic Oracle system back up that runs daily at 1:00 a.m.
- 15** Verify that the application files have been restored by entering the following commands:

```
cd /PROV_data  
ls -l
```

The files should display on the screen.

```
cd /user_audio_files  
ls -l
```

The files should display on the screen.

```
cd /audio_files  
ls -l
```

The files should display on the screen.
- 16** You have completed this procedure.





## USP Restore Operations

You can use the restore operation to return your system to a configuration that was saved during a backup operation. The typical use of the restore operation is as follows:

- An emergency situation occurs which requires you to restore a system configuration from a stored data snapshot.
- You use the file manager function to ensure that there are copies of the data snapshot to be restored on both RTC system nodes.
- You make the data snapshot the boot data snapshot for both RTC system nodes.
- You deactivate the linksets and change the path state of the application server process (ASP) paths to Down for your system, as appropriate.
- You perform a COR on your system, which means that you unseat the RTC system nodes, turn off both power switches on the shelf, reseat the RTC system nodes, and then restore power. Your stored data snapshot is now the running data snapshot.



### CAUTION

Performing a COR on your system is service affecting. Nortel Networks recommends that you do this during off-peak hours and that you ensure that a mated system is available.

The following sections contain procedures to restore data snapshots stored on your alternate boot server or on the RTC system nodes.

## Restoring a Data Snapshot from your Alternate Boot Server



### WARNING

Wear wrist straps, and use standard anti-static precautions.

To restore a system configuration from a data snapshot stored on your alternate boot server, perform the following steps:

**At the OAM&P workstation**

- 1 To open the File Manager window, click Administration on the main menu and click File Manager.  
**Note:** To have access to the file manager function, you must be working from the OAM&P workstation that is configured as an alternate boot server.
- 2 Select the disk drive in your alternate boot server where the data snapshot is stored from the Source field.
- 3 Select the RTC system node in slot 12 from the Destination list.
- 4 View the contents of the Snapshot field in the Destination portion of the window. If the data snapshot to be restored is not listed in the field, proceed to step 5. If the data snapshot to be restored is listed in the field, proceed to step 7.
- 5 In the Snapshot field in the Source portion of the window, select the data snapshot to be restored.
- 6 Initiate a copy operation by clicking the suitcase icon. An hourglass is displayed while the snapshot is being copied.  
When the copy operation is complete, the fields in the Destination portion of the window update with the information for the copied snapshot.
- 7 Open the RTC system node provisioning and maintenance window for the RTC system node in slot 12. To do this, return to the main menu, click the System Mgmt button to open the System Configuration window, click the icon for the control CAM shelf in the system to open the shelf\_name window, and click the icon for the RTC system node in slot 12.
- 8 Click Edit. The Edit button changes to Unedit button and the fields in the Provisioning portion of the window become editable.
- 9 Change the boot data snapshot setting for the RTC system node. To do this, click the button next to the Boot Data Snapshot field. The system displays the Boot Data Snapshot window. Select the data snapshot to be restored. The Boot Data Snapshot window closes.
- 10 Click Apply to save the changes. The change is reflected in the Boot Data Snapshot field.  
**Note:** When you change the boot data snapshot, a minor alarm is generated which indicates that the running data snapshot is different from the boot data snapshot. This alarm is cleared when you perform a COR on your system or if you should change the boot data snapshot back to match the running boot data snapshot.

- 11** If this RTC system node is the inactive RTC system node, perform the following steps. Otherwise, proceed to step 12.
  - a** If the RTC system node is locked, proceed to step 11b. Otherwise, click Lock and proceed to step 11b.
  - b** If the RTC system node is off-line, proceed to step 12. Otherwise, click Offline and proceed to step 12.
- 12** Repeat steps 3–11 for the RTC system node in slot 15.
- 13** Make note of which RTC system node is the active RTC system node. This information will be required later in the procedure.
- 14** Deactivate the linksets for your system, as appropriate. To do this, perform the following steps:
  - a** To open the SS7 MTP Linkset Administration window, click Network Mgmt on the main menu, click MTP on the Network Management window, and click Linksets on the SS7 MTP window.
  - b** Locate the linkset you want to deactivate.

All provisioned linksets are listed in the Linkset Records field. Click a linkset from the list. All data relating to this linkset automatically appears.

If you are unsure of the linkset name or far end point code, you must scroll through the entire list.

If you know the linkset name, you can easily find the linkset by clicking on the Find by Name radio button, entering the linkset name in the Linkset field, and clicking on the Apply button.

If you know the far end point code, you can easily find the linkset by clicking on the Find by PC radio button, entering the far end point code in the Far End PC field, and clicking on the Apply button.
  - c** Click the Deactivate button to deactivate the displayed linkset. All links in a linkset are deactivated by this command.
  - d** Repeat steps 14b and 14c for each linkset that you want to deactivate prior to performing a COR operation.
- 15** Change the path state of the ASP paths to Down, as appropriate. To do this, perform the following steps:
  - a** To open the Application Server Process Path Administration window, click Network Mgmt on the main menu, click IPS7 on the Network Management window, and click ASP Paths on the IPS7 window.

- b** Locate the path whose state you wish to change. All provisioned paths are displayed in the Application Server Process Path Records list, near the bottom of the window. Click a path from the list. All data relating to this path automatically appears.  
  
If you are unsure of the PID or ASP Name information, scroll through the list until you find the PID or ASP Name you want.
  - c** Click Down to change the state of the path to Down.
  - d** Repeat steps 15b and 15c for each ASP path that you want to bring down prior to performing a COR operation.
- 16** Click Exit on the main menu to close the GUI.
- 17** You may want to change the alternate boot data snapshot if the system configuration stored in the boot data snapshot is considerably different from the system configuration stored in the current alternate boot data snapshot. If you do not want to update the alternate boot data snapshot, proceed to step 18. If you do want to update the alternate boot data snapshot, perform the following steps:
  - a** Double-click the Universal Signaling Point icon on your desktop to display the Login window.
  - b** To open the Modify Site window, click Configure to open the Site Configuration window and click Modify Site.
  - c** Select your system from the Site Name list.
  - d** Select the boot data snapshot that you want to use as an alternate boot data snapshot from the Alt. Boot Data Snapshot list.
  - e** Click OK to save the change. The system displays a pop-up confirmation window.
  - f** Click OK to close the popup confirmation window. The system displays a message in a popup window to ask you if you want to modify the BOOTP tab window.
  - g** Click No to close the popup window.
  - h** Click Close to close the Site Configuration window.
- 18** To perform a COR on your system, use the following steps:
  - a** Unseat the RTC mission card for the inactive RTC system node. Ensure that the LED is off for the SCSI Disk Drive associated with this RTC system node before unseating the mission card.

To unseat the mission card, press outward on the top and bottom latches of the mission card to release it from the CAM shelf.

Grasp the top and bottom latches of the mission card and gently pull it toward you to disconnect it from the associated TM. Do not remove the mission card from the CAM shelf.

- b Repeat step 18a for the RTC mission card for the active RTC system node.
- c Turn off both the A and B power switches on the rear of the control CAM shelf of your system.

**Note:** Do not power down the shelf when the SCSI disk light on the RTC system node is on. To do so could cause a disk failure.

- d Reseat the RTC mission card for an RTC system node. To do this, gently slide the mission card back into place. Apply pressure to the faceplate until you feel resistance.

Snap the top and bottom latches of the mission card inward, toward one another. Two audible clicks can be heard when the mission card is seated properly.

- e Repeat step 18d for the RTC mission card for the other RTC system node.
- f Return power to the shelf. To do this, turn on both the A and B power switches on the rear of the control CAM shelf of your system.

**Note:** System start-up can take several minutes, depending on the configuration of your system.

- 19 Double-click Universal Signaling Point on your desktop to restart the GUI as soon as one of the RTC system nodes is enabled. This is indicated when an LED turns green on the front panel of the shelf below either slot 12 or 15.

**Note:** Nortel Networks recommends that you do not make any provisioning changes until the data in the shelf\_name window indicates that both RTC system nodes are enabled or that one RTC system node is enabled and the other is off-line.

- 20 Log into your system. To do this, select your system from the Site list, enter your user name in the User ID field, enter your password in the Password field, and click Connect. The system displays the main menu.

- 21 To open the RTC system node provisioning and maintenance window for the RTC system node in slot 12, click the System Mgmt button to open the System Configuration window, click the

- control CAM shelf to open the shelf\_name window, and click the RTC system node in slot 12.
- 22 Verify that the description of the data snapshot listed in the Running Data Snapshot field is the same as the description of the data snapshot you just attempted to restore.
  - 23 If the data snapshot descriptions match, proceed to step 24. If the snapshot descriptions do not match, return to step 1 and attempt the procedure again. If the procedure has failed twice in row, contact your next level of support.
  - 24 To update the system time settings in the Set Date/Time window, click Administration on the main menu to open the Administration window, and click Set Date/Time.
  - 25 The system time settings will be incorrect by as many minutes as the system took to perform the COR. Adjust the settings in the Time portion of the window appropriately.
  - 26 Click OK to save the new system time settings.

## Restoring a Data Snapshot from an RTC System Node



### WARNING

Do not power down the shelf when the SCSI disk light on the RTC system node is on. To do so could cause a disk failure.



### WARNING

Wear wrist straps, and use standard anti-static precautions.

Typically, when you are restoring a system configuration, the data snapshot is located on the disk drive for your alternate boot server. However, it might be necessary to restore a system configuration saved in a data snapshot that is not stored on the disk drive in your alternate boot server.

To restore a system configuration using a data snapshot stored on an RTC system node, perform the following steps:

**At the OAM&P workstation**

- 1 To open the File Manager window, click Administration on the main menu and click File Manager.  
**Note:** To have access to the file manager function, you must be working from the OAM&P workstation that is configured as an alternate boot server.
- 2 Select the RTC system node in which the data snapshot you want to restore is located from the Destination list.
- 3 Select the disk drive in your alternate boot server where the data snapshot will be stored from the Source list.
- 4 Initiate a copy operation by clicking the suitcase icon. An hourglass displays while the snapshot is being copied. The fields in the Source portion of the window will be updated with the information for the copied snapshot when the copy operation is complete.  
**Note:** The data snapshots are large and can take several minutes to copy from an RTC system node to your alternate boot server, depending on system activity.
- 5 Select the other RTC system node from the Destination field.
- 6 View the contents of the Snapshot field in the Destination portion of the window. If the data snapshot to be restored is not listed in the field, proceed to step 7. If the data snapshot to be restored is listed in the field, proceed to step 9.
- 7 In the Snapshot field in the Source portion of the window, select the data snapshot to be restored.
- 8 Initiate a copy operation by clicking the printer icon. An hourglass is displayed while the snapshot is being copied. When the copy operation is complete, the fields in the Destination portion of the window update with the information for the copied snapshot.
- 9 To open the RTC system node provisioning and maintenance window for the RTC system node in slot 12, click the System Mgmt button on the main menu, click the control CAM shelf to open the shelf\_name window, and click the RTC system node in slot 12.
- 10 Click Edit. The Edit button changes to Unedit and the fields in the Provisioning portion of the window become editable.
- 11 Change the boot data snapshot for the RTC system node. To do this, click next to the Boot Data Snapshot field. The system displays the Boot Data Snapshot window. Select the data

snapshot to be restored. The Boot Data Snapshot window closes.

- 12** Click Apply to save the changes. The change is reflected in the Boot Data Snapshot field.

**Note:** When you change the boot data snapshot, a minor alarm is generated to indicate that the running data snapshot is different from the boot data snapshot. This alarm is cleared when you perform a COR on your system or if you change the boot data snapshot back to match the running boot data snapshot.

- 13** If this RTC system node is the inactive RTC system node, perform the following steps. Otherwise, proceed to step [14](#).
- a** If the RTC system node is locked, proceed to step 13b. Otherwise, click Lock and proceed to step 13b.
  - b** If the RTC system node is off-line, proceed to step 14. Otherwise, click Offline and proceed to step 14.
- 14** Repeat steps 9–13 for the RTC system node in slot 15.
- 15** Make note of which RTC system node is the active RTC system node. This information will be required later in the procedure.
- 16** Deactivate the linksets for your system, as appropriate. To do this, perform the following steps:
- a** To open the SS7 MTP Linkset Administration window, click Network Mgmt on the main menu, click MTP on the Network Management window, and click Linksets on the SS7 MTP window.
  - b** Locate the linkset you want to deactivate.

All provisioned linksets are listed in the Linkset Records field. Click a linkset from the list. All data relating to this linkset automatically appears.

If you are unsure of the linkset name or far end point code, you must scroll through the entire list.

If you know the linkset name, you can easily find the linkset by clicking Find by Name, entering the linkset name in the Linkset field, and clicking Apply.

If you know the far end point code, you can easily find the linkset by clicking Find by PC, entering the far end point code in the Far End PC field, and clicking Apply.
  - c** Click the Deactivate button to deactivate the displayed linkset. All links in a linkset are deactivated by this command.



- d Repeat steps 16b and 16c for each linkset that you want to deactivate prior to performing a COR operation.
- 17** To change the path state of the ASP paths to Down, as appropriate, perform the following steps:
- a To open the Application Server Process Path Administration window, click Network Mgmt on the main menu, click IPS7 on the Network Management window, and click ASP Paths on the IPS7 window.
  - b Locate the path whose state you wish to change. All provisioned paths are displayed in the Application Server Process Path Records list, near the bottom of the window. Click a path from the list. All data relating to this path automatically appears.

If you are unsure of the PID or ASP Name information, scroll through the list until you find the PID or ASP Name you want.
  - c Click Down to change the state of the path to Down.
  - d Repeat steps 17b and 17c for each ASP path that you want to bring down prior to performing a COR operation.
- 18** Click Exit to exit the GUI.
- 19** You may want to change the alternate boot data snapshot if the system configuration stored in the data snapshot file is significantly different from the system configuration stored in the current alternate boot data snapshot. If you do not want to update the alternate boot data snapshot, proceed to step 20.
- If you do want to update the alternate boot data snapshot, perform the following steps:
- a Double-click the Universal Signaling Point icon on your desktop to display the Login window.
  - b To open the Modify Site window, click Configure to open the Site Configuration window and click Modify Site.
  - c Select your system from the Site Name list.
  - d Select the boot data snapshot that you want to use as an alternate boot data snapshot from the Alt. Boot Data Snapshot list.
  - e Click OK to save the change. A popup confirmation window appears.
  - f Click OK to close the popup confirmation window. The system displays a popup window with a message that asks you if you want to modify the BOOTP tab window.

- g Click No to close the popup window.
  - h Click Close to close the Site Configuration window.
- 20** To perform a COR on your system, use the following steps:
- a Unseat the RTC mission card for the inactive RTC system node. Ensure that the LED is off for the SCSI Disk Drive associated with this RTC system node before unseating the mission card.
 

To unseat the mission card, press outward on the top and bottom latches of the mission card to release it from the CAM shelf.

Grasp the top and bottom latches of the mission card and gently pull it toward you to disconnect it from the associated TM. Do not remove the mission card from the CAM shelf.
  - b Repeat step 20a for the RTC mission card for the active RTC system node.
  - c Turn off both the A and B power switches on the rear of the control CAM shelf of your system.
  - d Reseat the RTC mission card for an RTC system node. To do this, gently slide the mission card back into place. Apply pressure to the faceplate until you feel resistance.
 

Snap the top and bottom latches of the mission card inward, toward one another. Two audible clicks can be heard when the mission card is seated properly.
  - e Repeat step 20d for the RTC mission card for the other RTC system node.
  - f Return power to the shelf. To do this, turn on both the A and B power switches on the rear of the control CAM shelf of your system.

**Note:** System start-up can take several minutes, depending on the configuration of your system.

- 21** Double-click the Universal Signaling Point icon on your desktop to restart the GUI as soon as one of the RTC system nodes is enabled.

This is indicated when an LED turns green on the front panel of the shelf below either slot 12 or 15.

**Note:** Nortel Networks recommends that you do not make any provisioning changes until the data in the shelf\_name window indicates that both RTC system nodes are enabled or that one RTC system node is enabled and the other is off-line.

- 22 To log in to your system, perform the following steps:
  - a Select your system from the Site list.
  - b Enter your user name in the User ID field.
  - c Enter your password in the Password field.
  - d Click the Connect button. The main menu appears.
- 23 To open the RTC system node provisioning and maintenance window for the RTC system node in slot 12, click System Mgmt on the main menu, click the control CAM shelf to open the shelf\_name window, and click slot 12.
- 24 Verify that the description of the data snapshot listed in the Running Data Snapshot field is the same as the description of the data snapshot you just attempted to restore.
- 25 If the data snapshot descriptions match, proceed to step 26. If the snapshot descriptions do not match, return to step 1 and attempt the procedure again. If the procedure has failed twice in a row, contact your next level of support.
- 26 To update the system time settings in the Set Date/Time window, click Administration on the main menu to open the Administration window, and click Set Date/Time.
- 27 The system time settings will be off for as many minutes as the system took to perform the COR. Adjust the settings in the Time portion of the window appropriately.
- 28 Click OK to save the new system time settings.

## Performing a Restore Operation from a Backup Tape



### **DANGER**

This procedure can overwrite existing data files on your workstation. Make sure you have a current data backup before you begin this procedure.

To perform a restore operation from a backup tape, perform the following steps:

### ***At the OAM&P workstation***

- 1 Insert the tape containing the data that you want to restore.

- 2 Double-click the Backup Exec icon on the desktop if you are running a Veritas program or the Colorado Backup II icon if you are running a Colorado program.
- 3 Select Restore files using the Restore Wizard.
- 4 Click OK.
- 5 Click Next.
- 6 Select from media in the device.
- 7 Click Next. The system loads the information from the backup tape.
- 8 Select the backup date and time for the data that you want to restore.
- 9 Click OK. The system loads the information from the backup tape.
- 10 Click the + button on the tree control to expand the tree box next to the C: drive. Select any directories that you want to restore.
- 11 Click Next.
- 12 Click Next a second time.
- 13 Select Always replace the file on my computer.
- 14 Click Start. The system restores the backup data.
- 15 Click OK.
- 16 The data restore procedure is complete.

---

## Restoring Multiservice Switch or Media Gateway service data

---

This section describes using Service Data Backup and Restore to restore backed up service data from the backup site to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

The Service Data Backup and Restore tools provide three types of restore:

- A full restore restores all backed up service data to the selected device or devices.
- An incremental restore restores service data based on a specified date. Like the full restore, you can perform an incremental restore on either one or multiple devices.
- A selective restore restores specific service data that you select. Like the full restore, you can perform a selective restore on either one or multiple devices.

**Note:** It is not recommended that an active file (current view) be restored on a Multiservice Switch 7400/15000 or Media Gateway 7400/15000. When you restore the current view, you may overwrite the existing current view with different content. This action will cause an outage of the Backup and Restore tool.

The following information applies to using the Service Data Backup and Restore tool to perform a restore for Multiservice Switch 7400/15000 or Media Gateway 7400/15000 nodes:

- [Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the restore list](#)
- [Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the restore list](#)
- [Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device in the restore list](#)
- [Performing a full restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Performing an incremental restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Performing a selective restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device](#)
- [Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data](#)

## Adding Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices to the restore list

Use the following procedure to add devices to the Devices List.

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore
- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select the appropriate restore mode, from the Mode column (full or incremental).
- 6 If a specific userid and password is required for the device, enter the values in the User ID and Password fields and uncheck the Use default checkbox.
- 7 If you wish to use the default userid and password, click the Use default checkbox.
- 8 Click OK.

The IP addresses for the devices are retrieved from HGDS and the device displays in the Devices list.

For devices that are not in HGDS, you are prompted for their IP address. If you are prompted for an IP address, do [step 9](#).

- 9 If you know the IP address, enter the correct IP address in the form and click OK and the device is added to the Devices list.  
If the IP address is unknown or the device is not valid, press Cancel and the device is not added to the Devices list.

## Removing Multiservice Switch 7400/15000 or Media Gateway 7400/15000 devices from the restore list

Use this procedure to remove nodes from the list of nodes that you wish to backup.

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore

- 2 Select the Restore Configuration tab.
- 3 In the Device List, select the devices you wish to remove.
- 4 Click Remove.
- 5 In the confirmation dialog, select Yes to confirm or No to cancel the removal.

### **Defining a specific userid and password for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device in the restore list**

A specific userid and password can be defined when you add the device to the restore list or you can set it later using the following procedure.

#### ***Procedure steps***

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select a device.
- 3 In the Device Details section, enter a userid and password.
- 4 Clear the Use default checkbox.

### **Performing a full restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device**

Use the following procedure to copy all the files from the repository back to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

#### ***Procedure steps***

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->Passport Service Data Backup/Restore.
- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select a device from the Device List.
- 6 Click in the Mode title and select Full from the drop-down list.
- 7 Click Restore.

- 8 After a successful restore, you need to activate the restored data. See [Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data](#).

## Performing an incremental restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to copy files, based on a specific date, from the repository back to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->PassportService Data Backup/Restore.
- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select a device from the Device List.
- 6 Click in the Mode title and select Incremental from the drop-down list.
- 7 Define a date in the date column. (For example, July 4, 2003)  
All the files, with the date and time that are not greater than the specified date, will be restored.
- 8 Click Restore.
- 9 After a successful restore, you need to activate the restored data. See [Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data](#).

## Performing a selective restore for a Multiservice Switch 7400/15000 or Media Gateway 7400/15000 device

Use the following procedure to copy a specific file from the repository back to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.

### *Procedure steps*

- 1 Open the Backup and Restore window. From the MDM window, select Configuration->Passport Devices->Administration->PassportService Data Backup/Restore.



- 2 Select the Restore Configuration tab.
- 3 Click Add to open the Add Device dialog.
- 4 Select a group of devices or expand the group and use the Ctrl key to select a number of devices.
- 5 Select a device from the Device List .
- 6 Click in the Mode title and select Selective from the drop-down list.
- 7 In the View column, select the desired view from the repository using the drop-down list.  
**Note:** This step may take a few seconds to complete because the application must access the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 and list all the views names.
- 8 Click Restore.
- 9 After a successful restore, you need to activate the restored data. See [Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data](#).

## Activating the restored Multiservice Switch 7400/15000 or Media Gateway 7400/15000 data

Restore restores the backup configuration data onto the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk. After a successful restore, perform the following procedure to activate the restored data.

### **Procedure steps**

- 1 Establish a telnet session to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000.
- 2 Download to the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 any required application software missing from the Multiservice Switch 7400/15000 or Media Gateway 7400/15000 disk.
- 3 Enter provisioning mode.
- 4 Activate the restored view and confirm the activation.
- 5 If required, commit the activated view.



---

## Restoring Core Element Manager data

---

### Application

Use this procedure to restore Core Element Manager (CEM) data.

**Note:** The backup procedure is performed through the Synchronous backup restore manager (SBRM). See Synchronized Backup Manager overview in ATM/IP Solution-level Security and Administration, NN10402-600 for details. The information needed by the Core Element Manager to restore data is located in `/opt/nortel/cem/data/coreEMS/configBackup`.

### Prerequisites

You must have root user privileges to perform this procedure.

### Action

#### *At your workstation*

- 1 Telnet to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the server where the CEM resides
- 2 When prompted, enter your user ID and password.
- 3 Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.
- 4 When prompted, enter the root password.
- 5 Make sure that the `/opt/nortel/cem/data/coreEMS/configBackup` directory contains the following files:
  - `data_dir`
  - `ldapConfig.tar`
  - `nodes.tar`
  - `server`

Enter:

```
# ls /opt/nortel/data/coreEMS/configBackup
```

- 6 Make sure that CEM is not running by typing:

```
# servquery -status -group CEM
```

and pressing the Enter key.

Example response:

```
CEM server STOPPED
```

- 7 If the CEM server is running, stop the CEM server by typing:

```
# servstop CEM
```

and pressing the Enter key.

Example response:

```
CEM server successfully stopped
```

- 8 Run the restore script by typing

```
#!/opt/nortel/cem/data/coreEMS/nodes/server/bin/postRestore.sh
```

and pressing the Enter key.

- 9 You have completed this procedure.

---

## Performing a full restore of the software from S-tape

---

### Purpose

Use this procedure to perform a full restore of the core manager software load from the system image backup tape (S-tape).

### Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the core manager or how to display actions a user is authorized to perform, review the procedures in the following table.

### Application

**ATTENTION**

You must be a trained AIX system administrator authorized to perform fault-admin actions.

**ATTENTION**

You must mirror all volume groups on the core manager before you perform this procedure. If you perform this procedure when disk mirroring is not at the Mirrored state, the system displays an error message.

**ATTENTION**

If your system includes the SuperNode Billing Application (SBA), you must use tape drive DAT0 to perform this procedure.

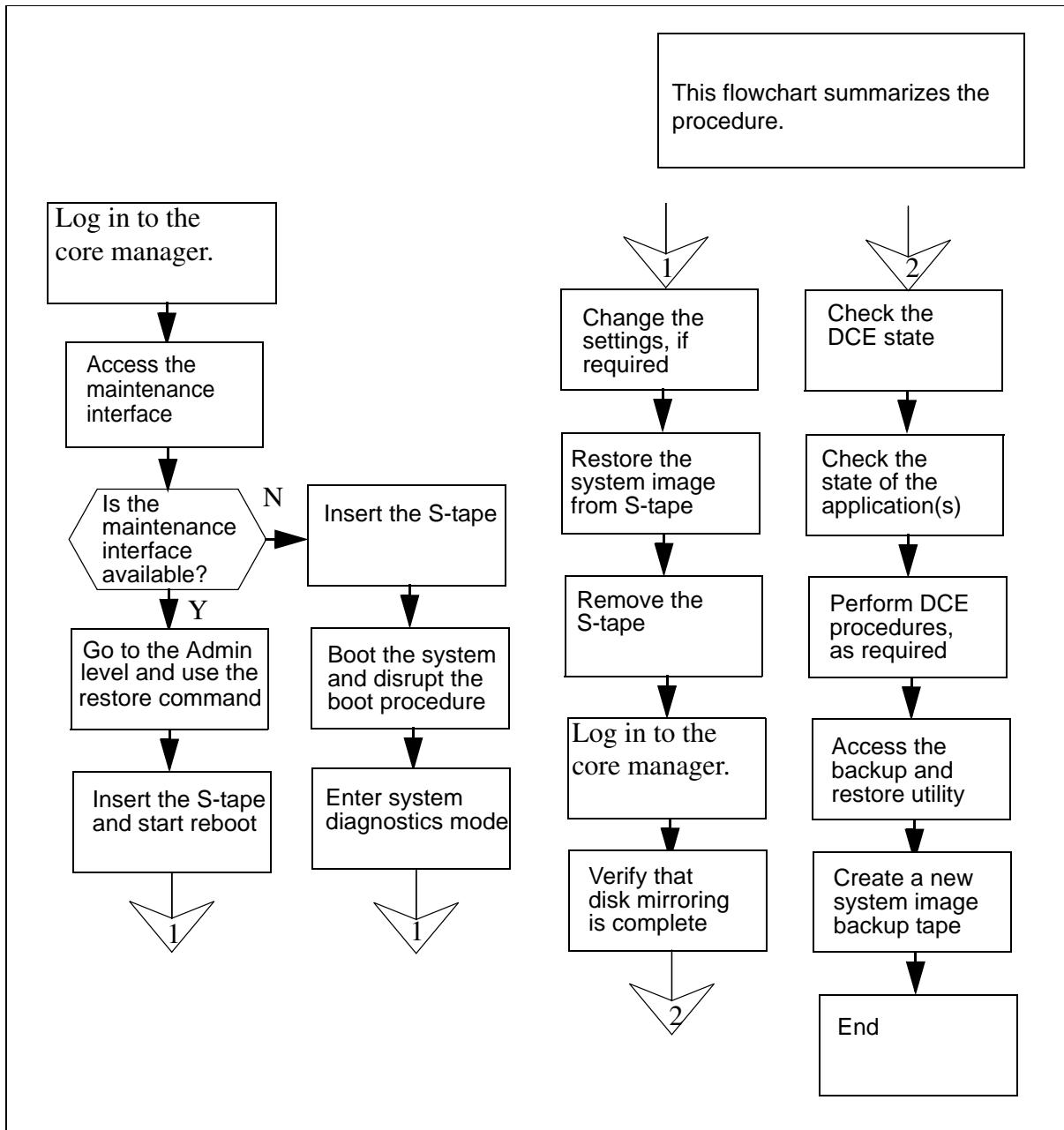
### Interval

Perform this procedure when the core manager is out-of-service due to a corrupted software load.

### Action

The following flowchart provides an overview of the procedure. Use the instructions in the procedure that follows the flowchart to perform the recovery tasks.

### Summary of performing a full restore of the software from the S-tape



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Performing a full restore of the software from S-tape

### At the local VT100 console

- 1 Log into the CS 2000 Core Manager as a user authorized to perform fault-admin actions.
- 2 Access the maintenance interface:  
**sdmmtc**
- 3 Determine if the core manager maintenance interface is available.

| If  | Do                      |
|---|-------------------------|
| core manager maintenance interface is available     | <a href="#">step 4</a>  |
| core manager maintenance interface is not available | <a href="#">step 10</a> |

- 4 Access the administration (Admin) level:  
**admin**
- 5 Perform a full restore of the core manager:  
**restore**

#### *Example response:*

Select the tape drive you want to restore from,  
or type Abort to abort:

Enter 0 for the tape drive in the main chassis  
slot 2.

Enter 1 for the tape drive in the main chassis  
slot 3.

- 6 Choose the tape drive to use.

| If  | Do      |
|---|---------|
| you want to use the tape drive in slot 2  | enter 0 |
| you want to use the tape drive in slot 13 | enter 1 |

- 7 When prompted, confirm that you want to proceed:

**y**

*Example response:*

Insert the backup-tape into the tape drive in the main chassis slot 2. When completed press [Enter] to start the restore.

- 8 Insert the back-up tape (S-tape) into the tape drive you specified (slot 2 or 13).

**Note:** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

- 9 Press the Enter key to start the restore process, and proceed to [step 17](#).

**Note:** When you press the Enter key, the system starts the restore procedure by rebooting the core manager from the selected tape drive.

#### ***At the core manager***

- 10 Ensure that one of the core manager tape drives (slot 2 or 13 in the main chassis) contains the system image backup tape (S-tape).

**Note:** Use tape drive DAT0 (option for performing a full restore from an S-tape) if your system also includes SBA.

#### ***At the Modular Supervisory Panel***

- 11 Reboot the core manager. If the prompt is available at a local VT100 console, reboot the core manager:

**shutdown -Fr**

If the prompt is not available, reboot the core manager by turning the power off, then on, using the MSP breaker that supplies power to the core manager.



**At the local VT100 console**

- 12 When the system displays “COLD Start”, press the Break key or the Esc key twice to interrupt the boot process. The system takes about 4 minutes to initialize.
- 13 Continue depending on the prompt displayed on the monitor.

| If the prompt is             | Do                      |
|------------------------------|-------------------------|
| FX-Bug                       | <a href="#">step 16</a> |
| FX-Bug and you are in a menu | <a href="#">step 14</a> |
| FX-Diag                      | <a href="#">step 15</a> |

- 14 From the selection menu, select Go to System Debugger:  
3  
Go to [step 16](#).
- 15 Switch the directory to FX-Bug:  
**sd**

- 16** View the input/output devices on the core manager to verify the address of the tape drive from the FX-Bug prompt. Enter:

**Fx-Bug> ioi**

*Example response:*

```

CLUN DLUN CNTRL-TYPE DADDR DTYPE RM Inquiry-Data
   1    0  IO          0    $00  N  SEAGATE
ST11200N ST
                                     31200 0660
   3    0  IO          0    $00  N  SEAGATE
ST12400N
                                     ST32430
0660
   1   50  IO          5    $01  Y  ARCHIVE
Python
                                     28388-XXX
5.45
   6    0  IO          0    $00  N  SEAGATE
ST11200N
                                     ST31230
0660
   8    0  IO          0    $00  N  SEAGATE
ST12400N
                                     ST32430
0660
   6   50  IO          5    $01  Y  ARCHIVE
Python
                                     28388-XXX
5.45

```

**Note:** In the example response, the tape drive is ARCHIVE.

- 17** If you receive the FX-Bug prompt, then continue with this step. Otherwise, go to [step 19](#).

**Fx-Bug> pboot <address\_for\_Archive\_Python>**

In the example, the following are valid choices:

- pboot 1 50 if the tape drive is located in slot 2
- pboot 6 50 if the tape drive is located in slot 13

- 18** Wait about 4 minutes until the system completes the reboot.
- 19** The system prompts you to define the console setting and the language setting. Define the console setting by selecting option 1 and pressing the Enter key.

**Note 1:** In case of any failures, contact your next level of support.

**Note 2:** When you define the console setting, the system does not echo the entry "1" on the screen.

- 20** Enter 1 to select the language setting, and press the Enter key. The Welcome to Base Operating System Installation and Maintenance menu is then displayed.
- 21** Select "Change/Show Installation Settings and Install":

**2**

The system displays the System Backup Installation and Settings menu.

*Example response:*

```
System Backup Installation and Settings
```

```
Either type 0 and press Enter to install with
the current settings, or type the number of the
setting you want to change and press Enter.
```

```
Setting:                               Current
Choice(s):
1 Disk(s) where you want to install    hdisk0...
    Use Maps                            No
2 Shrink File System                   No
```

```
>>> 0 Install with the settings listed above.
```

**Note:** The string "..." shown under Current Choice(s) indicates that more than one disk is currently in use.

- 22** The default disk for the installation is hdisk0 which is located in slot 2 of the main chassis. If your core manager contains one disk drive in each domain of the main chassis, accept the default setting. If you have additional disk drives, you may wish to change the settings.

| If                                      | Do                      |
|---|-------------------------|
| you want to change the current settings | <a href="#">step 23</a> |
| you want to use the current settings    | <a href="#">step 27</a> |

**23** Change the disks where you want to install the backup image:**1**

The system displays the Change Disk(s) Where You Want to Install menu.

*Example response:*

```
Change Disk(s) Where You Want to
Install
```

Type one or more numbers for the disk(s) to be used for installation and press Enter. To cancel a choice, type the corresponding number and Press Enter. At least one bootable disk must be selected. The current choice is indicated by >>>.

```

Name          Location Code Size(MB) VGStatus
Bootable Maps
>>>1 hdisk0 c1-f2-00-0,0 4056      rootvg
   Yes      No
>>>2 hdisk5 c1-f13-00-0,0 4056
   rootvg   Yes      No
   3 hdisk1 c1-f4-00-0,0 4056      other
vg   Yes      No
   4 hdisk2 c1-f4-00-1,0 4056      other vg
Yes   No
   5 hdisk3 c2-f1-00-0    02043     other vg
Yes   No
```

This menu displays the list of all available disks on which you can install the system backup image. The currently selected disks are indicated by >>> symbols.

**Note:** The system backup must be installed on one disk in each domain to achieve fault-tolerant operation. Valid choices in the example in [step 23](#) are hdisk0 and hdisk5. The rootvg disks for installation must have location codes

- c1-f2-00-0 for domain 0, and
- c1-f13-00-0 for domain 1.

**24** To select a disk or disks, enter the number of the disk, and press the Enter key.

**25** To deselect a selected disk, enter its number again and press the Enter key.

- 26** When you have finished entering the settings, the System Backup Installation and Settings menu is displayed. Enter

**0**

and return to [step 22](#).

- 27** Accept the current settings:

**0**

This begins the restore process and lasts at least 30 min. During the restore process, the monitor displays the approximate percentage of the tasks completed, and the elapsed time.

**Note 1:** If an error message appears at the end of the restore process, datavg did not import successfully. Contact the next level of support.

**Note 2:** You must manually re-boot the system if you are performing this procedure as part of the “Removing an I/O expansion chassis (NTRX50EC)” procedure in the Upgrades document. In this scenario, go to [step 28](#).

**Note 3:** As part of the restore process, the system reboots automatically and displays the login prompt. Continue with [step 29](#).

- 28** At the FX-bug prompt, manually boot the system:

```
FX-bug> pboot 1 0
```

***At the core manager***

- 29** Remove the S-tape from the tape drive when the reboot is completed, and store it in a secure location.

***At the local or remote terminal***

- 30** Log in to the core manager as a user authorized to perform fault-admin actions. Press the Enter key when you see the “TERM=(vt100)” prompt.

- 31** Start the core manager maintenance interface:

```
sdmmtc
```

**32** Access the storage level:**> storage***Example response:*

```

volume Groups      Status      Free (MB)
rootvg             Mirrored    2032
datavg             Mirrored    11712

Logical Volume     Location    Size (MB)    % full/
threshold 1 /     rootvg      11/80        88

2 /usr             rootvg      600          29/90
3 /var             rootvg      200          5/70
4 /tmp             rootvg      24           5/90
5 /home            rootvg      304          5/70
6 /sdm             rootvg      504          24/90
7 /data            datavg      208          7/ 80

Logical volumes showing: 1 to
7 or 7

```

**33** Determine the mirror status of the disks.

| If the disks are            | Do                      |
|-----------------------------|-------------------------|
| Mirrored                    | <a href="#">step 35</a> |
| Integrating or Not Mirrored | <a href="#">step 34</a> |

**34** You cannot continue this procedure until disk mirroring is Mirrored. If necessary, contact the personnel responsible for your next level of support. When disk mirroring is at the Mirrored state, continue this procedure.

**35** Access the LAN level:

**lan**

**36** Check the state of DCE.

*Example response:*

DCE State: SysB

- 37** Access the application (APPL) level to check the state of any DCE-based applications:

**appl**

and pressing the Enter key.

*Example response:*

```
# Application                               State
1 Table Access Service                       .
2 Log Delivery Service                       .
3 OM Access Service                          .
4 Secure File Transfer                       Fail
5 Enhanced Terminal Access                   Fail
6 Exception Reporting Fail
                                           Applications showing 1 to 6 of 6
```

- 38**

**ATTENTION**

DCE and DCE-based applications can fail if the key tab files restored from tape contain obsolete keys.

If the DCE state is displayed as SysB at the LAN menu level of the RMI ([step 35](#)), and the logs displayed indicate an error with the security client service in DCE, restore the service by performing the following procedures in the CS 2000 Core Manager Configuration Management document:

- “Removing a CS 2000 Core Manager from a DCE cell”
- “Configuring a CS 2000 Core Manager in a DCE cell”

- 39** If some DCE-based applications are faulty (Fail state, see [step 37](#)), try to restore them by busying (BSY) and returning to service (RTS) the applications from the SDM APPL level (see [step 37](#)).
- 40** If this approach fails, restore them by performing the procedure to add the application server to the DCE cell in the CS 2000 Core Manager Configuration Management document.
- 41** Reset passwords for users SDM01-04 on the core and SDM. Refer to procedure [Resetting SDM user passwords for DDMS on page 761](#).
- 42** You must create a new system image backup tape. Refer to the procedure “Creating system image backup tapes (S-Tapes)” in

the CS 2000 Core Manager Security and Administration document.

- 43** You have completed this procedure.



## Performing a partial restore of the software from S-tape

### Purpose

Use this procedure to restore individual files or sets of files from the system image backup tape (S-tape).

### Prerequisites

You must be a user authorized to perform fault-admin actions.

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Procedures related to this procedure

| Procedure  | Document                    |
|--|-----------------------------|
| Logging in to the CS 2000 Core Manager             | Security and Administration |
| Displaying actions a user is authorized to perform | Security and Administration |

For information on how to log in to the CS 2000 Core Manager or how to display actions a user is authorized to perform, review the procedures in the following table.

#### Procedures related to this procedure

| Procedure  | Document                    |
|--|-----------------------------|
| Logging in to the CS 2000 Core Manager             | Security and Administration |
| Displaying actions a user is authorized to perform | Security and Administration |



#### **CAUTION**

##### **Possible loss of data**

Use this procedure at the discretion of the system administrator.

Perform a partial restore only if you are familiar with the files, and know exactly which files are to be restored. If you restore the wrong files, you may inadvertently corrupt core manager software.

**ATTENTION**

This procedure must be performed by a trained AIX system administrator authorized to perform fault-admin actions.

**ATTENTION**

All volume groups on the core manager must be fully mirrored (Mirrored) before performing this procedure. If you attempt to perform this procedure when disk mirroring is not Mirrored, an error message is displayed on the screen.

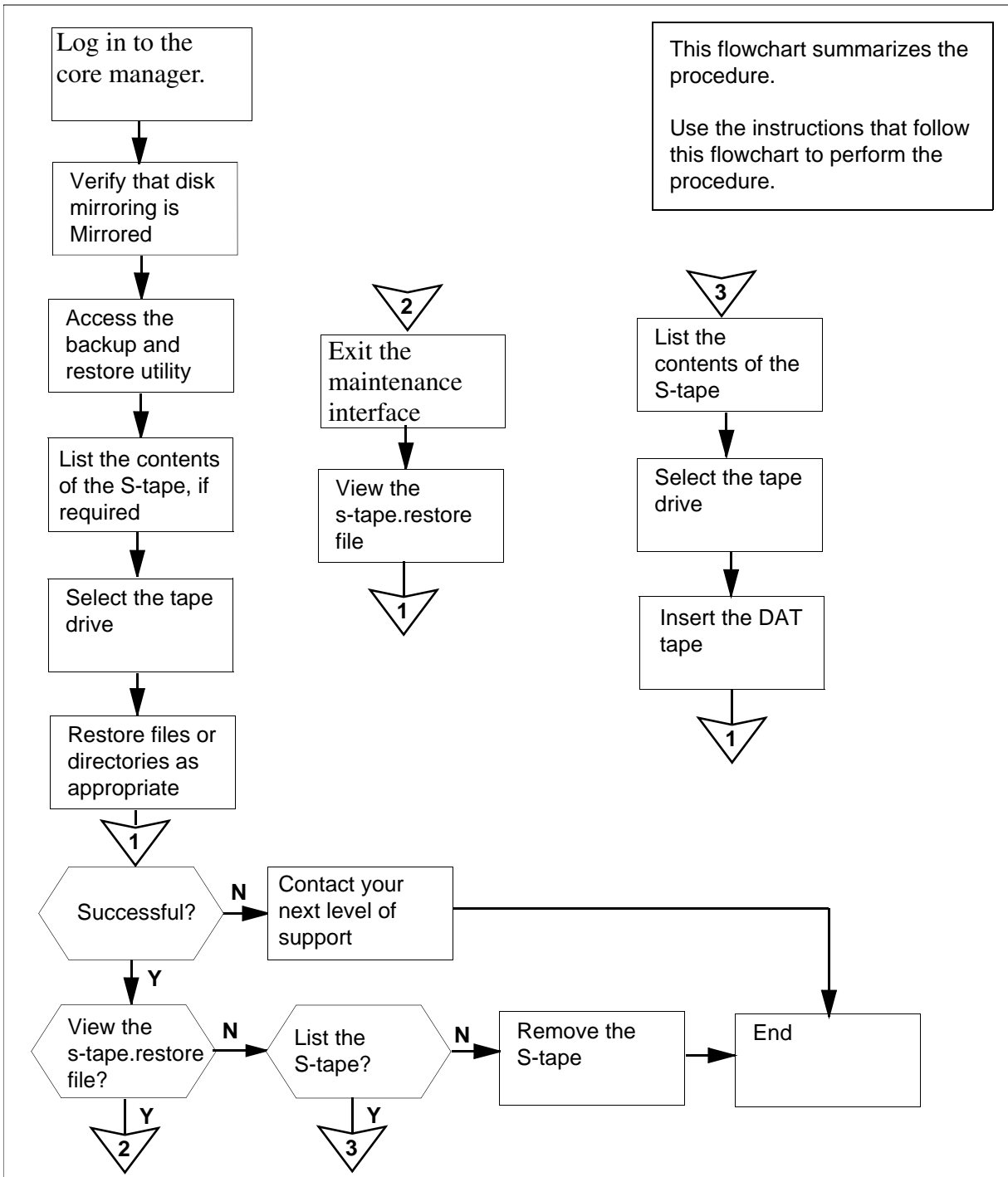
**ATTENTION**

If your system includes the SuperNode Billing Application (SBA), use tape drive DAT0 to perform this procedure.

**Action**

The following flowchart provides an overview of the procedure. Use the instructions in the step-action procedure that follows the flowchart to perform the recovery tasks.

### Summary of Partial restore from the system image tape (S-tape)



**Note:** Instructions for entering commands in the following procedure do not show the prompting symbol, such as #, >, or \$, displayed by the system through a GUI or on a command line.

## Partial restore from the system image tape (S-tape)

### At the local or remote console

- 1 Log into the core manager as the user authorized to perform fault-admin actions.
- 2 Access the maintenance interface:

```
sdmmtc
```

- 3 Access the storage level:

```
storage
```

*Example response:*

```
Volume Groups          Status          Free
(MB)
rootvg                 Mirrored       2032
datavg                 Mirrored       11712
```

```
Logical Volume      Location
  Size (MB)    %full/threshold 1 /
                rootvg          88          11/80
2 /usr          rootvg          600
  29/90
3 /var          rootvg          200
  5/70
4 /tmp          rootvg          24
  5/90
5 /home        rootvg          304
  5/70
6 /sdm         rootvg          504
  24/90
7 /data        datavg          208
  7/80
```

Logical volumes showing: 1

to 7 of 7

- 4 Determine the Mirror status of the disks.

| If the disks are | Do                     |
|------------------|------------------------|
| Mirrored         | <a href="#">step 6</a> |
| not Mirrored     | <a href="#">step 5</a> |

5

**CAUTION**

Possible loss of data

You cannot perform this procedure until disk mirroring of all volume groups is Mirrored.

If necessary, contact the personnel responsible for your next level of support. When disk mirroring is Mirrored, continue this procedure.

6 Access the administration (Admin) menu level of the RMI:

**admin**

7 Access the System Image Backup and Restore Menu:

**backup**

**Note 1:** If disk mirroring for all volume groups is not Mirrored, the system displays an error message. The system then prompts you to return to the System Image Backup and Restore menu.

**Note 2:** If another person attempts to use the backup and restore utility when it is in use, an error message is displayed on the screen.

*Example response:*

```
Currently there is a backup running on bnode73.
Please execute yours later.
Exiting...
```

8 Determine the contents of the tape.

| If you                         | Do                      |
|--------------------------------|-------------------------|
| wish to list the S-tape        | <a href="#">step 9</a>  |
| do not wish to list the S-tape | <a href="#">step 17</a> |

9 From the System Image Backup and Restore Menu, select “List Contents of the System Image Tape (S-tape)”:

3

- 10** After you select option 3, you are prompted to select the tape drive.

*Example response:*

Select a tape drive you wish to use:

```
Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
( 0, 1 or 2 ) ==>
```

**Note:** Use tape drive DAT0 (option 1) if your system also includes SBA.

- 11** Enter the number for the tape drive you want to use (1 or 2), and press the Enter key.

**Note:** If your system includes SBA, and you still wish to use DAT1 (option 2), the following message is displayed:

*Response:*

You have selected DAT 1. This is the default DAT drive for the Billing application, and may currently be in use for the emergency storage of billing records.

If you continue to use DAT 1, make sure that the correct tape is in the drive, and that billing records will not be lost during the backup restore operation.

Do you wish to continue with DAT 1? ( y | n )

- if you wish to continue using DAT1, enter y
- if you do not wish to use DAT1, enter n

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

- 12** After you select the tape drive, the system prompts you to insert the S-tape into the appropriate tape drive.

*Example response:*

```
Please insert your System Image Backup tape
(S-tape) into the tape drive DAT0 and allow at
least 5 minutes to complete the listing.
```

```
A log file will be saved in /tmp/s-tape.toc.
```

```
Are you ready to proceed? ( y | n )
```

***At the core manager***

- 13** Insert the S-tape into the tape drive you selected.

**Note:** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

***At the local or remote VT100 console***

- 14** When you are ready to continue this procedure, enter:

**y**

The contents of the S-tape are listed on the screen. When the listing is complete, the system prompts you to return to the System Image Backup and Restore Menu.

*Example response:*

```
Would you like to return to the previous menu?
( y | n )
```

- 15** Return to the System Image Backup and Restore Menu:

**y**

- 16** Determine if the file or directory has been restored.

| If you are listing the contents of the tape to verify | Do                      |
|---|-------------------------|
| that the file has been restored                       | <a href="#">step 25</a> |
| the file name or directory that you wish to restore   | <a href="#">step 17</a> |

- 17 From the System Image Backup and Restore Menu, select “Restore Files from the System Image Tape (S-tape)”:

4

- 18 After you select option 4, you are prompted to select the tape drive.

*Example response:*

Select a tape drive you wish to use:

```
Enter 0 to return to previous menu
Enter 1 for tape drive DAT0 in Main
Chassis-Slot 2
Enter 2 for tape drive DAT1 in Main
Chassis-Slot 13
( 0, 1 or 2 ) ==>
```

**Note:** Use tape drive DAT0 (option 1) if your system also includes SBA.

- 19 Enter the number for the tape drive you want to use (1 or 2).

**Note:** If your system includes SBA, and you still wish to use tape drive DAT1 (option 2), the following message is displayed:

*Example response:*

You have selected DAT 1. This is the default DAT drive for the Billing application, and may currently be in use for the emergency storage of billing records.

If you continue to use DAT 1, make sure that the correct tape is in the drive, and that billing records will not be lost during the backup/restore operation.

Do you wish to continue with DAT 1? ( y | n )

- if you wish to continue using DAT1, enter y
- If you do not wish to use DAT1, enter n

The system prompts you to return to the System Image Backup and Restore Menu if you do not wish to use DAT1.

- 20 After you select the tape drive, you are prompted to insert the S-tape into the appropriate tape drive. A warning is displayed advising that this procedure must only be completed by qualified core manager system administrators. The warning also advises



that files and directories must be entered exactly as they appear in the file listing. Insert the S-tape in the appropriate tape drive.

**Note:** Wait until the tape drive stabilizes (yellow LED is off) before you proceed.

*Example response:*

```
Are you ready to enter the name of the file or
directory? ( y | n )
```

- 21** Continue this procedure:

**y**

*Example response:*

```
Enter the name of the directory or file that you
wish to restore as
./<your-full-path>/<your-file-or-directory>.
```

Note: Tape processing may take a few minutes to complete. A log file /tmp/s-tape.restore will be created.  
==>

- 22** Enter the full path name of the directory or file that you wish to restore, exactly as shown in the file listing, including “/” at the beginning.

**Note 1:** A log file /tmp/s-tape.restore is created when the restore is completed.

**Note 2:** An error message is displayed if the restore is unsuccessful. If this occurs, go to [step 25](#).

- 23** During the restore process, the screen does not display any additional information. When the file restore is complete, the file you have restored is displayed. The system then prompts you to return to the System Image Backup and Restore Menu.

*Example response:*

```
Would you like to return to the previous menu?
( y | n )
```

**Note:** If the restore has failed, an error message is displayed before the prompt, advising you to list the contents of the tape, and perform the procedure again.

- 24** Return to the System Image Backup and Restore Menu:

**y**

- 25** Determine if the restore was successful. The system displays the file that you have restored, as described in [step 23](#). You may

also wish to view the s-tape.restore file or list the files on the S-tape.

| If                                       | Do                                 |
|--|------------------------------------|
| the restore is successful                | <a href="#">step 32</a>            |
| the restore failed                       | contact your next level of support |
| you wish to view the s-tape.restore file | <a href="#">step 26</a>            |
| you wish to list the S-tape              | <a href="#">step 9</a>             |

- 26** Exit the System Image Backup and Restore Menu:  
0
- 27** Exit the maintenance interface:  
**quit all**
- 28** Access the s-tape.restore file:  
**cd /tmp**
- 29** Scroll through the file:  
**more s-tape.restore**
- 30** Continue pressing the Enter key until the files that you have restored, and the date of the restore, are displayed.
- 31** Determine if the restore was successful.

| If         | Do                                 |
|------------|------------------------------------|
| successful | <a href="#">step 33</a>            |
| failed     | contact your next level of support |

- 32** Exit the System Image Backup and Restore Menu:  
0

**Note:** If you then wish to exit the maintenance interface, type quit all and press the Enter key.

***At the core manager***

- 33** Remove the S-tape and store it in a secure place.
- 34** You have completed this procedure.



---

## Recovering backup files from lost backup volumes

---

### Application

You need to recover backup files from lost backup volumes if the SBA becomes unaware of backed up files when the SWACT and RESTART processes occur when you are configuring backup volumes.

The following procedure swaps back old volumes as the primary backup volumes.

### Prerequisites

Before starting the procedure, you need

- the names of the swapped out volumes
- to have configured backup volumes, following the procedure found in NTP NN10125-811NN10126-811NN10363-811, at which point, the SBA completed its recovery of the volumes from the backup volumes you configured during these procedures.

### Action

#### Recovering backup files from lost backup volumes

##### *At the MAP*

- 1 Post the billing stream by typing  

```
> mapci;mtc;appl;sdbil;post <x>
```

and pressing the Enter key.  
*Where*  
<x> is the name of the billing stream.
- 2 Quit back to the appl;sdbil level by typing  

```
> quit
```

and pressing the Enter key.

- 3 Confirm that the names of the billing stream's existing backup volumes are the swapped in volumes you created earlier by typing
 

```
> conf view <x>
```

 and pressing the Enter key.
 

*Where*

<x> is the name of the billing stream.

**Note:** SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.
- 4 Reference the notes you made when you configured the backup volumes, to confirm that the backup volumes are those that you created during these procedures.
- 5 Refer to the following table to determine your next step.

| If the backup volume Do names are                              |  |
|--|--|
| the names you setup when you configured the backup volumes     | continue with step <a href="#">6</a>   |
| not the names you setup when you configured the backup volumes | determine if someone else re-configured the backup volumes before you continue with step <a href="#">6</a> |

- 6 Configure the billing stream of the logical volumes you created, once you receive confirmation that the files are successfully created by typing
 

```
> conf set <x> <y> <z>
```

 and pressing the Enter key.
 

*Where*

<x> is the name of the stream, <y> is the dms\_backup\_1 volume, and <z> is the dms\_backup\_2 volume.

**Note:** SBA does not support configuring more than one billing stream at a time from multiple workstations. The last billing stream that is configured is the one that is saved.
- 7 Quit back to the command prompt by typing
 

```
> quit all
```

and pressing the Enter key.

**Note 1:** The non-empty backup volumes are automatically detected by the SBA audits. In addition, the SBA places the billing stream into recovery mode and the volumes from the original backup volumes are sent to the SDMCS 2000 Core ManagerCBM.

**Note 2:** You must alert all operating company personnel who are associated with the DMS switch as to the names of the old and new backup volumes and the procedure you used to swap the volumes. These same personnel must be made aware of that any RESTARTs or SWACTs that occur before the billing stream returns to normal mode can cause a serious loss of billing records.

- 8 You have completed this procedure.





---

## Resetting SDM user passwords for DDMS

---

### Application

Use this procedure to reset the passwords for users SDM01-04 when both of the following conditions have occurred:

- the DDMS applications, OSS Comms Svcs and OSS and Application Svcs, remain in in-service trouble (ISTb) after busying and returning the DDMS applications to service
- the QUSER command from the core does not show users SDM01-04

Resetting the passwords for users SDM01-04 consists of

- [Resetting the passwords on the CM on page 761](#)
- [Changing passwords in the DDMS configuration file on page 762](#)

### Prerequisites

To complete this procedure you need the following:

- access to the core
- root-user access to the CS 2000 Core Manager
- passwords for users SDM01-04

### Action

Complete all the steps that follow to reset the password for users SDM01-04.

#### Resetting the passwords on the CM

##### *At the CLI prompt on the switch*

- 1 Enter each of the following commands:
  - > `unpermit sdm01`
  - > `unpermit sdm02`
  - > `unpermit sdm03`
  - > `unpermit sdm04`
- 2 Enter each of the following commands:
  - > `permit sdm01 <sdm01_pswd> 4 10000 english all`
  - > `permit sdm02 <sdm02_pswd> 4 10000 english all`
  - > `permit sdm03 <sdm03_pswd> 4 10000 english all`

```
> permit sdm04 <sdm04_pswd> 4 10000 english all
```

Where

**<sdm0n\_pswd>**

is the password for user SDM0n

**Note 1:** If Enhanced Password Control is in effect on the CM, the password must be at least six characters in length.

**Note 2:** If Enhanced Password Control is in effect on the CM, and any of the SDM01-SDM04 passwords are changed on the CM, you need to apply the same password changes in the DDMS configuration file. Refer to [Changing passwords in the DDMS configuration file](#).

- 3 You have completed this procedure. Proceed to [Changing passwords in the DDMS configuration file on page 762](#).

### Changing passwords in the DDMS configuration file

#### *At the CS 2000 Core Manager*

- 1 Log in to the CS 2000 Core Manager as the root user.
- 2 Access the application level of the maintenance interface by typing

```
# sdmmtc appl
```

and pressing the Enter key.
- 3 Locate and busy OSS Comms Svcs by typing

```
> bsy <n>
```

and pressing the Enter key.

**<n>**  
is the number next to the OSS Comms Svcs fileset
- 4 Locate and busy OSS and application Svcs by typing

```
> bsy <n>
```

and pressing the Enter key.

**<n>**  
is the number next to the OSS and application Svcs fileset
- 5 Exit the application level by typing

```
> quit all
```

and pressing the Enter key.

- 6 Access the configuration level of the maintenance interface by typing  
**# sdmmtc config**  
 and pressing the Enter key.
- 7 Access the OSS Comms Svcs configuration level by typing  
**> config <n>**  
 and pressing the Enter key.  
     **<n>**  
         is the number next to the OSS Comms Svcs fileset
- 8 Press Enter to begin configuration.
- 9 When prompted to enter the logroute tool, as shown in table [DDMS logroute tool banner](#), press Enter.

### DDMS logroute tool banner

```
#####
#
# Adding DDMS logroute configuration
#####
#
Please add DDMS log routing:

    Device type      = file
    File             = /data/logs/ossaps/ossapslog
    Routing          = addrep
    log_type         = DDMS

Press <RETURN> when ready
```

The Logroute Main Menu appears, as shown in figure [Logroute tool main menu](#).

## Logroute tool main menu

```
Logroute Main Menu

1 - Device List
2 - Global Parameters
3 - CM Configuration File
4 - GDD Configuration
5 - Help
6 - Quit Logroute

Enter Option ==>
```

- 10** Enter the number next to Quit Logroute.

The CM User Setup screen is displayed as shown in the example that follows.

## Example of DDMS CM User Setup screen

```
CM User Setup

0. QUIT
1. Add user
2. Delete user(by ID)
3. Update passwd(by ID)
4. Display users(ID)

Enter choice:
```

- 11** Enter the number next to Display users(ID).  
**12** Note the user ID next to SDM01-04.  
**13** Enter the number next to Update passwd(by ID).  
**14** Enter the user ID (not user name) for SDM01.  
**15** Enter new password for SDM01.

The passwords for SDM0n must be the same as that entered in [Resetting the passwords on the CM on page 761](#).

**Note:** The userIDs and passwords are not case sensitive.

- 16 Repeat step [15](#) for SDM02, SDM03, and SDM04, then proceed to step [17](#).
- 17 Enter the number next to QUIT in the CM User Setup screen.
- 18 Exit all levels of the maintenance interface by typing  

```
> quit all
```

and pressing the Enter key.
- 19 Access the application level of the maintenance interface by typing  

```
# sdmmtc appl
```

and pressing the Enter key.
- 20 Locate and return OSS Comms Svcs to service by typing  

```
> rts <n>
```

and pressing the Enter key.  

```
<n>
```

is the number next to the OSS Comms Svcs fileset
- 21 Locate and return OSS and application Svcs to service by typing  

```
> rts <n>
```

and pressing the Enter key.  

```
<n>
```

is the number next to the OSS and application Svcs fileset
- 22 Exit all levels of the maintenance interface by typing  

```
> quit all
```

and pressing the Enter key.  
You have completed this procedure.



---

## Restoring the oracle data on an SSPFS-based server

---

### Application

Use this procedure to restore the oracle data from a backup tape, CD or DVD on a Succession Server Platform Foundation Software (SSPFS)-based server (Sun Netra t1400 or Sun Netra 240). Also use this procedure to restore the data that was automatically backed up to a file on the server by the backup restore manager.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

**Note:** Restoring the oracle data is not applicable to the CBM as it does not use an oracle database.

### Prerequisites

This procedure requires the oracle data backup tape, CD or DVD. If the data was saved through the backup restore manager, the name of the file located in directory “/data/bkresmgr/backup” is required.

### Action

Use the following table to determine how to start this procedure.

If	Start at
restoring from tape, CD or DVD	<a href="#">step 1</a>
restoring from a file	<a href="#">step 2</a>

#### **At the server**

- 1 Insert the tape, CD, or DVD containing the oracle data backup into the drive and proceed to [step 2](#).

**At your workstation**

- 2** Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the SSPFS-based server on which you are performing the data restore

- 3** When prompted, enter your user ID and password.

- 4** Change to the root user by typing

```
$ su - root
```

and pressing the Enter key.

- 5** When prompted, enter the root password.

- 6** Verify the permissions on the restore log directory (bkslog) by typing

```
# ls -alrt /var/opt/nortel
```

and pressing the Enter key.

Example response

```
total 22
lrwxrwxrwx  1 root      succssn      28 Dec 22
2003 gwc -> /net/47.141.126.131//swd/gwc
drwxrwxr-x  4 root      other        512 Dec 22
2003 .
drwxr-xr-x  7 root      sys          512 Sep 10
12:41 ..
drwxr-xr-x  2 oracle    oinstall     512 Dec  8
15:58 db
drwxrwxrwt  2 root      other        6656 Dec 15
19:56 bkslog
```

If the permissions of bkslog	Do
are drwxrwxrwt	<a href="#">step 8</a>
are not drwxrwxrwt	<a href="#">step 7</a>



- 7 Change the permissions of bkslog by typing  

```
# chmod 777 /var/opt/nortel/bkslog
```
- 8 Determine if server applications have been stopped by typing  

```
# servquery -status all
```
- 9 If not already done, stop any running server applications on the server.

For	Refer to
CS 2000 Management Tools server applications	<a href="#">Stopping the SESM server application</a> <a href="#">Stopping the SAM21 Manager server application</a> <a href="#">Stopping the NPM server application</a> <i>ATM/IP Security and Administration,</i> NN10402-600
MG 9000 Manager and mid-tier server applications	<i>the MG9000 Security and Administration,</i> NN10162-611
Integrated EMS server application	<i>IEMS Security and Administration,</i> NN10336-611

- 10 Use the following table to determine your next step.

If	Do
restoring from tape, CD or DVD	substep <a href="#">a</a>
restoring from a file	substep <a href="#">b</a>

- a Restore the database from backup tape, CD or DVD by typing

```
$ /opt/nortel/sspfs/bks/rsdata
```

and pressing the Enter key.

Proceed to [step 11](#).

- b** Restore the database from the backup file by typing

```
$ /opt/nortel/sspfs/bks/rsdata -f  
/data/bkresmgr/backup/<filename>
```

and pressing the Enter key.

where

**filename**

is the name of the backup file created by the backup restore manager

Proceed to [step 12](#).

- 11** Remove the tape from the drive, or eject the CD or DVD from the drive as follows:

- a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

- b** Eject the CD by typing

```
# eject cdrom
```

and pressing the Enter key.

**Note:** If the DVD drive tray does not open (if not busy or being read from or written to), then enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Press the eject button located on the front of the DVD drive.

- c** Remove the CD or DVD from the drive.

- 12** Verify that the database restored properly by typing

```
# queryAllFaults
```

If an alarm appears like the following, the database was not restored properly:

```
*** SPFS330 Import of Oracle data caused  
corruption ORA-22337: Error importing Oracle  
data  
cs2kaps=rtp6backupsesm;NODE=rtp6backupsesm;CLA  
SS=SW;SWTYPE=Database Fri Jun 10 15:48:59 2005
```

Use the information in the following table to determine the next step.

If	Do
no alarm appears	<a href="#">step 13</a>
the database did not restore properly	contact Nortel

**13** Start the server applications that run on the server.

For	Refer to
CS 2000 Management Tools server applications	<a href="#">Starting the SESM server application</a> <a href="#">Starting the SAM21 Manager server application</a> <a href="#">Starting the NPM server application</a> <i>ATM/IP Security and Administration,</i> NN10402-600
MG 9000 Manager and mid-tier server applications	<i>the MG9000 Security and Administration,</i> NN10162-611
Integrated EMS server application	<i>IEMS Security and Administration,</i> NN10336-611

**Note:** If one or more applications do not start, contact Nortel for assistance.

You have completed this procedure.



## Stopping the SESM server application

### Application

Use this procedure to stop the Succession Element and Subelement Manager (SESM) server application on the CS 2000 Management Tools server.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

#### *At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

<b>If using</b>	<b>Do</b>
telnet (unsecure)	step <a href="#">2</a>
ssh (secure)	step <a href="#">3</a>

- 2 Log in to the server using telnet (unsecure) as follows:
  - a Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the CS 2000 Management Tools server, or the physical IP address of the active server in a two-server configuration
  - b When prompted, enter your user ID and password.
  - c Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.

- d When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

Proceed to step [4](#).

- 3 Log in using ssh (secure) as follows:

- a Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the CS 2000 Management Tools server, or the physical IP address of the active server in a two-server configuration

**Note:** If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

- b When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

- 4 Verify the status of the SESM server application by typing

```
# servman query -status -group SESMSERVICE
```

and pressing the Enter key.

If the response indicates	Do
running	step <a href="#">5</a>
not running	step <a href="#">8</a>

- 5 Stop the SESM server application by typing  
**# servstop SESMService**  
and pressing the Enter key.
- 6 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to stop.
- 7 Verify the SESM server application stopped as follows:
  - a Verify the SESM services stopped by typing  
**# servman query -status -group SESMService**  
and pressing the Enter key.  
Example response:  
CS2K Management Tools are not running
  - b Verify the SESM applications stopped by typing  
**# ptmctl status**  
and pressing the Enter key.  
Example response:  
SESM STATUS -----  
  
          COMPONENT                          STATUS  
          -----  
Proxy Agent                          NOT RUNNING  
RMI Regisry                          NOT RUNNING  
Snmpfactory                          NOT RUNNING  
MI2 Server                           NOT RUNNING  
  
Current number of SESM processes running: 0  
(of 4)  
  
SESM APPLICATION STATUS: No Applications are  
ready
- 8 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.





## Stopping the SAM21 Manager server application

### Application

Use this procedure to stop the SAM21 Manager server application on the SSPFS-based server that is hosting the CS 2000 Management Tools.

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

#### *At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step <a href="#">2</a>
ssh (secure)	step <a href="#">3</a>

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the CS 2000 Management Tools server, or the physical IP address of the active server in a two-server configuration

- b When prompted, enter your user ID and password.

- c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- d When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

Proceed to step [4](#).

- 3 Log in using ssh (secure) as follows:

- a Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the CS 2000 Management Tools server, or the physical IP address of the active server in a two-server configuration

**Note:** If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

- b When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

- 4 Verify the status of the SAM21 Manager server application by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

If SAM21EM is	Do
running	step <a href="#">5</a>
not running	step <a href="#">7</a>

- 5 Stop the SAM21EM server application by typing  
**# servstop SAM21EM**  
and pressing the Enter key.
- 6 Verify the SAM21EM server application stopped by typing  
**# servman query -status -group SAM21EM**  
and pressing the Enter key.  
Example response:  
  
Executing: /opt/servman/bin/servquery -status  
-group SAM21EM  
  
Succession SAM21 Element Manager version:  
SAM21EM\_9\_020\_0  
  
Current status of the Succession SAM21 Element  
Manager:  
    SNMP Access Gateway is not running.  
    SAM21 Element Manager Server is not running.
- 7 You have completed this procedure. If applicable, return to the  
high level task or procedure that directed you to this procedure.



---

## Stopping the NPM server application

---

### Application

Use this procedure to stop the Network Patch Manager (NPM) server application on a Succession Server Platform Foundation Software (SSPFS)-based server.

### Prerequisites

You need root user privileges to perform this procedure.

It is recommended that all users exit the NPM CLUI and GUI before stopping the NPM server application.

### Action

Perform the following steps to complete this procedure.

**ATTENTION**

In a two-server configuration, perform the steps that follow on the Active server.

#### *At your workstation*

- 1 Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the SSPFS-based server where the NPM server application resides

**Note:** In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).

- 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.

**Note:** In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the

Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display ClusterIndicatorACT, which indicates you are on the Active server.

- 5 Verify the status of the NPM server application by typing  
**# servman query -status -group NPM**  
and pressing the Enter key.

If the NPM server application is	Do
running	step <a href="#">6</a>
not running	you have completed this procedure

- 6 Stop the NPM server application by typing  
**# servstop NPM**  
and pressing the Enter key.
- 7 Verify the NPM server application is no longer running by typing  
**# servman query -status -group NPM**  
and pressing the Enter key.  
You have completed this procedure.

## Starting the SESM server application

### Application

Use this procedure to start the Succession Element and Subelement Manager (SESM) server application on the SSPFS-based server.

### Prerequisites

None

### Action

Perform the steps that follow to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

#### *At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step <a href="#">2</a>
ssh (secure)	step <a href="#">3</a>

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

> **telnet <server>**

and pressing the Enter key.

where

**server**

is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

- b When prompted, enter your user ID and password.

- c Change to the root user by typing

\$ **su -**

and pressing the Enter key.

- d When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

Proceed to step [4](#).

- 3 Log in using `ssh (secure)` as follows:

- a Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

**Note:** If this is the first time you are logging in using `ssh`, the system will request that you confirm to continue connecting. Enter yes at the prompt.

- b When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

- 4 Verify the status of the SESM server application by typing

```
# servman query -status -group SESMSERVICE
```

and pressing the Enter key.

If the response indicates	Do
not running	step <a href="#">5</a>
running	step <a href="#">8</a>



- 5 Start the SESM server application by typing  
**# servstart SESMService**  
and pressing the Enter key.
- 6 Wait approximately 3 to 5 minutes before you proceed to the next step to allow the SESM server application to start.
- 7 Verify the SESM server application started as follows:
  - a Verify the SESM services started by typing  
**# servman query -status -group SESMService**  
and pressing the Enter key.  
Example response:  
CS2K Management Tools are running
  - b Verify the SESM applications started by typing  
**# ptmctl status**  
and pressing the Enter key.  
Example response:  
SESM STATUS -----  
  
          COMPONENT                          STATUS  
          -----  
Proxy Agent                          RUNNING  
RMI Regisry                          RUNNING  
Snmpfactory                          RUNNING  
MI2 Server                           RUNNING  
  
Current number of SESM processes running: 4  
(of 4)  
  
SESM APPLICATION STATUS: All Applications  
Ready
- 8 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.



## Starting the SAM21 Manager server application

### Application

Use this procedure to start the SAM21 Manager server application on the SSPFS-based server that is hosting the CS 2000 Management Tools.

### Prerequisites

None

### Action

Perform the following steps to complete this procedure.

#### ATTENTION

In a two-server configuration, perform the steps that follow on the active server.

#### *At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

<b>If using</b>	<b>Do</b>
telnet (unsecure)	step <a href="#">2</a>
ssh (secure)	step <a href="#">3</a>

- 2 Log in to the server using telnet (unsecure) as follows:
  - a Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration
  - b When prompted, enter your user ID and password.
  - c Change to the root user by typing  

```
$ su -
```

and pressing the Enter key.

- d When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

Proceed to step [4](#).

- 3 Log in using ssh (secure) as follows:

- a Log in to the server by typing

```
> ssh -l root <server>
```

and pressing the Enter key.

where

**server**

is the IP address or host name of the SSPFS-based server, or the physical IP address of the active server in a two-server configuration

**Note:** If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

- b When prompted, enter the root password.

**Note:** In a two-server configuration, ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

- 4 Verify the status of the SAM21 Manager server application by typing

```
# servman query -status -group SAM21EM
```

and pressing the Enter key.

If SAM21EM is	Do
not running	step <a href="#">5</a>
running	step <a href="#">7</a>

- 5 Start the SAM21EM server application by typing  
**# servstart SAM21EM**  
and pressing the Enter key.
- 6 Verify the SAM21EM server application started by typing  
**# servman query -status -group SAM21EM**  
and pressing the Enter key.  
Example response:  

```
Executing: /opt/servman/bin/servquery -status  
-group SAM21EM  
  
Succession SAM21 Element Manager version:  
SAM21EM_9_020_0  
  
Current status of the Succession SAM21 Element  
Manager:  
    SNMP Access Gateway is running.  
    SAM21 Element Manager Server is running.
```
- 7 You have completed this procedure. If applicable, return to the high level task or procedure that directed you to this procedure.



---

## Starting the NPM server application

---

### Application

Use this procedure to start the Network Patch Manager (NPM) server application on a Succession Server Platform Foundation Software (SSPFS)-based server.

### Prerequisites

You need root user privileges to perform this procedure, and CORBA must be running in order for the NPM to come up.

### Action

Perform the following steps to complete this procedure.

**ATTENTION**

In a two-server configuration, perform the steps that follow on the Active server.

#### *At your workstation*

- 1 Log in to the server by typing  

```
> telnet <server>
```

and pressing the Enter key.  
where  
**server**  
is the IP address or host name of the SSPFS-based server where the NPM server application resides  
**Note:** In a two-server configuration, enter the physical IP address of the Active server (unit 0 or unit 1).
- 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.  
**Note:** In a two-server configuration, ensure you are on the Active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the Inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the

other unit. The response must display ClusterIndicatorACT, which indicates you are on the Active server.

- 5 Verify the status of the NPM server application by typing  
**# servman query -status -group NPM**  
and pressing the Enter key.

<b>If the NPM server application is</b>	<b>Do</b>
not running	step <a href="#">6</a>
running	you have completed this procedure

- 6 Start the NPM server application by typing  
**# servstart NPM**  
and pressing the Enter key.
- 7 Verify the NPM server application is running by typing  
**# servman query -status -group NPM**  
and pressing the Enter key.  
You have completed this procedure.



---

## Performing a full system restore on an SPFS-based server

---

### Application

Use this procedure to perform a full system restore from backup media on a Server Platform Foundation Software (SPFS)-based server (Sun Netra t1400 or Sun Netra 240).

A full system restore consists of reverting to the previous release of SPFS, restoring the file systems, and restoring the oracle data.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway (MG) 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager
- Core Billing Manager (CBM)

**Note:** Restoring the oracle data does not apply to the CBM as it does not use an oracle database.

#### ATTENTION

System logs indicating application and database errors generate until the file systems and oracle data are restored on the system using this procedure and procedure [Restoring the oracle data on an SSPFS-based server on page 767](#). No database errors generate on the CBM as it does not use an oracle database.

### Prerequisites

To complete this procedure you need

- the SPFS Installation CD disk#1 for the release you are reverting to
- the tape or DVD on which you backed up the file systems
- the tape or DVD on which you backed up the oracle data

## Action

Use one of the methods below according to your office configuration.

- [Simplex configuration \(one server\) on page 794](#)
- [High-availability configuration \(two servers\) on page 796](#)

**Note:** Only the [Simplex configuration \(one server\)](#) uses a full system restore from tape on a Sun Netra t1400 server.

### Simplex configuration (one server)

#### At the server console

- 1 Log in to the server through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing  
**# init 0**  
and pressing the Enter key.
- 3 Insert SPFS Installation CD disk#1 into the drive.
- 4 Use the following table to determine your next step.

If restoring from	Do
tape	<a href="#">step 5</a>
DVD	<a href="#">step 6</a>

- 5 Insert the tape with the backed up file systems into the drive.
- 6 At the OK prompt, restore the system by typing  
**OK boot cdrom - restore**  
and pressing the Enter key.
- 7 When prompted, accept the software license restrictions by typing  
**ok**  
and pressing the Enter key.  
The system reboots.

**Note:** If the restore process fails at this point due to one or more disks not being labeled, which is reported as “Bad Magic Number in Disk Label”, refer to procedure [Labelling disks on an SPFS-based server on page 809](#) to label the disks.

If restoring from DVD, you will be prompted to insert Volume 1 of the backup DVD into the drive. Insert the DVD on which you

backed up the file systems. During the restore process, the system will prompt you for additional Volumes if more than one DVD was used during the backup of file systems.

The restore process can take several hours to complete depending on the number and size of the files that are being restored.

**Note:** Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.

**8** Eject the backup DVD from the drive as follows:

**a** Ensure you are at the root directory level by typing

```
# cd /
```

and pressing the Enter key.

**b** Eject the DVD by typing

```
# eject cdrom
```

and pressing the Enter key.

**Note:** If the DVD drive tray does not open (if not busy or being read from or written to), enter the following commands:

```
# /etc/init.d/volmgt stop
```

```
# /etc/init.d/volmgt start
```

Then, press the eject button located on the front of the DVD drive.

**c** Remove the backup DVD from the drive.

**9** Use the following table to determine your next step.

<b>If</b>	<b>Do</b>
this SPFS-based server is hosting the CBM	<a href="#">step 13</a>
otherwise	<a href="#">step 10</a>

**10** List the oracle groups by typing

```
# groups oracle
```

and pressing the Enter key.

---

**If the output is****Do**

---

oinstall data dba or oinstall dbs  
data

[step 11](#)

oinstall dba data

[step 12](#)

---

- 11 Correct the oracle groups by typing  
**# usermod -g oinstall -G data,dba oracle**  
and pressing the Enter key.
- 12 Restore the oracle data using procedure [Restoring the oracle data on an SSPFS-based server on page 767](#). Once the data restore is complete, continue to [step 13](#).
- 13 Reboot the server by typing  
**# init 6**  
and pressing the Enter key.  
You have completed this procedure.

### High-availability configuration (two servers)

#### *At the console connected to the inactive node*

- 1 Log in to the inactive node through the console (port A) using the root user ID and password.
- 2 Bring the system to the OK prompt by typing  
**# init 0**  
and pressing the Enter key.

#### *At the console connected to the active node*

- 3 Log in to the active node through the console (port A) using the root user ID and password.
- 4 Access the OK prompt by typing  
**# init 0**  
and pressing the Enter key.
- 5 Insert SPFS Installation CD disk#1 into the drive.
- 6 At the OK prompt, restore the system by typing  
**OK boot cdrom - restore**  
and pressing the Enter key.

- 7 When prompted, accept the software license restrictions by typing  
**ok**  
and press the Enter key.  
The system reboots.  
**Note:** If the restore process fails at this point due to one or more disks not being labeled, refer to procedure [Labelling disks on an SPFS-based server on page 809](#) to label the disks.
- 8 When prompted, insert Volume 1 of the DVD on which you backed up the file systems, into the drive.  
**Note:** During the restore process, the system will prompt you for additional Volumes if more than one DVD was used during the backup of file systems.  
The restore process can take several hours to complete depending on the number and size of the files that are being restored.  
**Note:** Although it can appear as if the system is hanging at times, please do not interrupt the restore process. If you suspect an issue with the restore process, please contact your next level of support.
- 9 Eject the backup DVD from the drive as follows:
  - a Ensure you are at the root directory level by typing  
**# cd /**  
and pressing the Enter key.
  - b Eject the CD by typing  
**# eject cdrom**  
and pressing the Enter key.  
**Note:** If the DVD drive tray does not open (if not busy or being read from or written to), enter the following commands:  
**# /etc/init.d/volmgt stop**  
**# /etc/init.d/volmgt start**  
Then, press the eject button located on the front of the DVD drive.
  - c Remove the backup DVD from the drive.

- 10 Use the following table to determine your next step.

If	Do
this SPFS-based server is hosting the CBM	<a href="#">step 14</a>
otherwise	<a href="#">step 11</a>

- 11 List the oracle groups by typing

```
# groups oracle
```

and pressing the Enter key.

If the output is	Do
oinstall data dba or oinstall dbs data	<a href="#">step 12</a>
oinstall dba data	<a href="#">step 13</a>

- 12 Correct the oracle groups by typing

```
# usermod -g oinstall -G data,dba oracle
```

and pressing the Enter key.

- 13 Restore the data using procedure [Restoring the oracle data on an SSPFS-based server on page 767](#). Once the data restore is complete, execute [step 14](#) and [step 15](#).

- 14 Reboot the server by typing

```
# init 6
```

and pressing the Enter key.

- 15 Re-image the inactive node using the active node's image. If required, refer to procedure [Cloning the image of one server in a cluster to the other server on page 799](#).

You have completed this procedure.

---

## Cloning the image of one server in a cluster to the other server

---

### Application

Use this procedure to clone the image of the active server in a cluster to the inactive server.

The server can be hosting one or more of the following components:

- CS 2000 Management Tools
- Integrated Element Management System (IEMS)
- Audio Provisioning Server (APS)
- Media Gateway 9000 Manager
- CS 2000 SAM21 Manager
- Network Patch Manager (NPM)
- Core and Billing Manager (CBM)

### Prerequisites

This procedure has the following prerequisites:

- you need the root user ID and password
- you need console access to the inactive server under the following circumstances
  - this is the first time you clone
  - you replaced the inactive server
  - you executed a reverse restore (that is, you switched unit 0 and 1)

**Note:** Under any of the previous circumstances, the inactive server will have a different ethernet address from the one retained in the system. Therefore, console access is required to obtain the ethernet address of the inactive server.

#### **ATTENTION**

Ensure that no provisioning activities are in progress, or are scheduled to take place during this procedure.

## Action

Perform the following steps to complete this procedure.

### ATTENTION

Perform the steps that follow on the active server.

#### *At your workstation*

- 1 Establish a login session to the server, using one of the following methods:

If using	Do
telnet (unsecure)	step <a href="#">2</a>
ssh (secure)	step <a href="#">3</a>

- 2 Log in to the server using telnet (unsecure) as follows:

- a Log in to the server by typing

```
> telnet <server>
```

and pressing the Enter key.

where

**server**

is the physical IP address of the active server

- b When prompted, enter your user ID and password.

- c Change to the root user by typing

```
$ su -
```

and pressing the Enter key.

- d When prompted, enter the root password.

**Note:** Ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

Proceed to step [4](#).

- 3 Log in using ssh (secure) as follows:

- a Log in to the server by typing

```
> ssh -l root <server>
```



and pressing the Enter key.

where

**server**

is the physical IP address of the active server

**Note:** If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

- b** When prompted, enter the root password.

**Note:** Ensure you are on the active server by typing `ubmstat`. If `ClusterIndicatorSTBY` is displayed in the response, which indicates you are on the inactive server, log out of that server and log in to the other server through telnet using the physical IP address of the other unit. The response must display `ClusterIndicatorACT`, which indicates you are on the active server.

**On the active server**

- 4** Access the command line interface to determine the server profile by typing

```
# cli
```

and pressing the Enter key.

- 5** Enter the number next to the View option in the menu.  
**6** Enter the number next to the `sspfs_soft` option in the menu.

Example response

```
=== Executing "sspfs_soft"
```

```
SSPFS version: 09.0 Build: 200508421 Server  
Profile: cbm850
```

```
=== "sspfs_soft" completed successfully
```

- 7** In the system response, note the server profile.  
**8** Exit the CLI by typing `x` until you return to the command prompt.  
**9** Use the following table to determine your next step.

If	Do
the Server Profile is cbm850	step <a href="#">16</a>
otherwise	step <a href="#">10</a>

- 10** Verify that all applications on the server are running by typing  
**# servquery -status all**  
 and pressing the Enter key.

- 11** Use the following table to determine your next step.

<b>If</b>	<b>Do</b>
all applications are running	step <a href="#">14</a>
otherwise	step <a href="#">12</a>

- 12** Start each application that is not running by typing  
**# servstart <app\_name>**  
 and pressing the Enter key.  
 where

**app\_name**

is the name of the application that is not in a RUNNING state, for example, SAM21EM

- 13** Use the following table to determine your next step.

<b>If</b>	<b>Do</b>
all applications started	step <a href="#">14</a>
otherwise	contact your next level of support

- 14** Verify the Patching Server Element (PSE) server application is running by typing  
**# pse status**  
 and pressing the Enter key.

<b>If</b>	<b>Do</b>
PSE is running	step <a href="#">16</a>
otherwise	step <a href="#">15</a>

- 15** Start the PSE server application by typing  
**# pse start**  
 and pressing the Enter key.

<b>If</b>	<b>Do</b>
PSE starts	step <a href="#">16</a>
otherwise	contact your next level of support

- 16** Use the following table to determine your next step.

<b>If</b>	<b>Do</b>
this is the first time you are cloning the server, or you replaced the server, or you executed a reverse restore (that is, switched unit 0 and unit 1)	step <a href="#">17</a>
Under any of the previous circumstances, the inactive server will have a different ethernet address from the one retained in the system. Therefore, console access is required to obtain the ethernet address of the inactive server.	
otherwise	step <a href="#">21</a>

- 17** Use the following table to determine your next step.

<b>If</b>	<b>Do</b>
you do not know the Ethernet address of the inactive server	step <a href="#">18</a>
otherwise	step <a href="#">19</a>

***At the console connected to the inactive server***

- 18** Determine the Ethernet address of the inactive server as follows:

- a** Log in to the inactive server through the console (port A) using the root user ID and password.

Ensure you are on the inactive server by typing `ubmstat`. If `ClusterIndicatorACT` is displayed in the response, which indicates you are on the active server, log out of that server and log in to the other server. The response must display

ClusterIndicatorSTBY, which indicates you are on the inactive server.

- b** Bring the system to the OK prompt by typing

```
# init 0
```

and pressing the Enter key.

- c** At the OK prompt, display the Ethernet address of the inactive server by typing

```
OK banner
```

and pressing the Enter key.

Example response:

```
Sun Fire V240, No keyboard
Copyright 1998-2002 Sun Microsystems, Inc.
All rights reserved. OpenBoot 4.8.0.build_04,
2048 MB memory installed, Serial #52964131.
Ethernet address 0:3:ba:28:2b:23, Host ID:
83282b23.
```

- d** Record the Ethernet address that is displayed.

### ***On the active server***

- 19** Start the cloning process on the active server by typing

```
# startb <Ethernet address>
```

and press the Enter key.

where

**Ethernet address**

is the Ethernet address of the inactive server

- 20** Proceed to step [22](#)

### ***On the active server***

- 21** Start the cloning process on the active server by typing

```
# startb
```

and press the Enter key.

- 22** Use the following table to determine your next step.

<b>If</b>	<b>Do</b>
the system prompts you to enter the command "boot net - image"	step <a href="#">23</a>

	<b>If</b>	<b>Do</b>
	otherwise	step <a href="#">27</a>
<b>23</b>	Connect to the console port of the inactive server.	
	<b>If the console displays the</b>	<b>Do</b>
	login prompt	step <a href="#">24</a>
	OK prompt	step <a href="#">26</a>

***At the console connected to the inactive server***

**24** Log in to the inactive server using the root user ID and password.

**25** Bring the system to the OK prompt by typing

**# init 0**

and pressing the Enter key.

**26** At the OK prompt, boot the inactive server from the image of the active server by typing

**OK boot net - image**

and press the Enter key.

**Note:** There must be a space between the "-" and "image".

Example response

```
SC Alert: Host System has Reset
Sun Fire V240, No Keyboard
Copyright 1998-2002 Sun Microsystems, Inc. All
rights reserved. OpenBoot 4.8.0.build_04, 2048
MB memory installed, Serial #52964131. Ethernet
address 0:3:ba:28:2b:23, Host ID: 83282b23.
Rebooting with command: boot net - image
.
.
.
SC Alert: Host System has Reset
```

***On the active server***

**27** Monitor the progress of the cloning from the active server. Cloning the inactive server takes approximately 40 minutes to

complete, but the time can vary depending on system configuration.

**Example response:**

```
Waiting for network response from
unit1-priv0...
received network response from unit1-priv0...
Waiting for unit1-priv0 to clone data...
waiting...1
waiting...2
waiting...3
unit1-priv0 is cloning: /export/d2
.
.
.
Verifying cluster status of unit1-priv0
waiting for cluster filesystem status to become
normal.
Jun 27 16:01:38 ucary0883c unix: /data: active
up repair - standby reflected (normal)
Deleted snapshot 2.
Deleted snapshot 1.
Deleted snapshot 0.
ucary0883c-unit0(active) :/>
```

- 28** Once cloning is complete, wait approximately 5 minutes before you proceed to the next step.

***On the active server***

- 29** Verify the status of replicated disk volumes on the active server by typing

**# udstat**

and pressing the Enter key.

<b>If</b>	<b>Do</b>
all file systems are ACTIVE normal UP clean	step <a href="#">30</a>
otherwise	contact your next level of support

**At your workstation**

- 30** Establish a login session to the inactive server using one of the following methods:

---

**If using**

telnet (unsecure)

ssh (secure)

**Do**step [31](#)step [36](#)

---

- 31** Log in to the inactive server using telnet (unsecure) by typing  
> **telnet <server>**  
and pressing the Enter key.

where

**server**

is the physical IP address of the inactive server in the cluster

- 32** When prompted, enter your user ID and password.

- 33** Change to the root user by typing

\$ **su -**

and pressing the Enter key.

- 34** When prompted, enter the root password.

- 35** Proceed to step [38](#).

- 36** Log in to the inactive server by typing

> **ssh -l root <server>**

and pressing the Enter key.

where

**server**

is the physical IP address of the inactive server in the cluster

**Note:** If this is the first time you are logging in using ssh, the system will request that you confirm to continue connecting. Enter yes at the prompt.

- 37** When prompted, enter the root password.

***On the inactive server***

- 38** Verify the status of replicated disk volumes on the inactive server by typing

**# udstat**

and pressing the Enter key.

---

**If**

**Do**

---

all file systems are STANDBY  
normal UP clean

step [39](#)

otherwise

contact your next level of support

- 
- 39** You have completed this procedure. If applicable, return to the highlevel task or procedure that directed you to this procedure.



---

## Labelling disks on an SPFS-based server

---

### Application

Use this procedure when, during a full system restore, a failure occurred due to one or more disks not being labeled, which is reported as “Bad Magic Number in Disk Label”. This procedure applies to labeling disks on a Server Platform Foundation Software (SPFS)-based server, Sun Netra t1400 or Sun Netra 240.

### Prerequisites

This procedure has the following prerequisites:

- the system is at the OK prompt
- the SPFS Installation CD disk#1 from which you were attempting a full system restore is still in the drive

### Action

Perform the following steps to complete this procedure.

#### *At the server console*

- 1 At the OK prompt, boot the system by typing  
**OK boot cdrom -s**  
and pressing the Enter key.
- 2 At the shell prompt, access the disk partitioning and maintenance utility by typing  
**\$ format**  
and pressing the Enter key.
- 3 Specify disk 0 by typing  
**\$ 0**  
and pressing the Enter key.
- 4 Use the following table to determine your next step.

---

<b>If</b>	<b>Do</b>
prompted to label the disk (disk 0)	step <a href="#">5</a>
otherwise	step <a href="#">6</a>

---

- 5 Confirm you want to label the disk by typing  
**yes**  
and pressing the Enter key.

6 Specify disk 1 by typing  
**format> disk 1**  
and pressing the Enter key.

7 Use the following table to determine your next step.

<b>If</b>	<b>Do</b>
prompted to label the disk (disk 1)	step <a href="#">8</a>
otherwise	step <a href="#">9</a>

8 Confirm you want to label the disk by typing  
**yes**  
and pressing the Enter key.

9 Use the following table to determine your next step.

<b>If your server is a</b>	<b>Do</b>
Sun Netra t1400	step <a href="#">10</a>
Sun Netra 240	step <a href="#">16</a>

10 Specify disk 2 by typing  
**format> disk 2**  
and pressing the Enter key.

11 Use the following table to determine your next step.

<b>If</b>	<b>Do</b>
prompted to label the disk (disk 2)	step <a href="#">12</a>
otherwise	step <a href="#">13</a>

12 Confirm you want to label the disk by typing  
**yes**  
and pressing the Enter key.

13 Specify disk 3 by typing  
**format> disk 3**  
and pressing the Enter key.

- 14 Use the following table to determine your next step.

---

<b>If</b>	<b>Do</b>
prompted to label the disk (disk 3)	step <a href="#">15</a>
otherwise	step <a href="#">16</a>

---

- 15 Confirm you want to label the disk by typing  
**yes**  
and pressing the Enter key.
- 16 Exit the disk partitioning and maintenance utility by typing  
**format> quit**  
and pressing the Enter key.
- 17 Reboot the server by typing  
**# init 0**  
and pressing the Enter key.
- 18 Return to procedure [Performing a full system restore on an SPFS-based server on page 793](#), and execute again.



---

## Restoring the central security server

---

### Application

Use this procedure to restore the security server from a backup file.

#### **ATTENTION**

SSL uses certificates. Certificates from one server cannot be used on another server. If you want to take a back up file from a server where SSL is implemented and restore to a different server, you must perform the procedure “Replacing HTTPS certificate on security server for SunOne component” in ATM/IP Solution-level Security and Administration, NN10402-600 after the restore is completed. This script is run to set up IS authentication, session, and policy traffic to operate under SSL.

Note that servers in the same high availability cluster can use the same SSL certificate.

Note that if the restored IS SSL certificate has expired, you must perform the procedure in “Replacing HTTPS certificate on security server for SunOne component” in ATM/IP Solution-level Security and Administration, NN10402-600 after the restore is completed.

### Prerequisites

This procedure has the following prerequisites:

- You must have root user privileges.
- You must have a backup tar file created using the procedure for [Backing up the central security server](#).

### Action

Perform the following steps to restore central security server data.

#### ***At your workstation***

- 1 Telnet to the server by typing  
> **telnet <server>**  
and pressing the Enter key.  
where

**server**

is the IP address or host name of the server

**Note:** If you are upgrading the active server, telnet to the active server. If you are upgrading the inactive server, telnet to the inactive server.

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.

If	Do
you are performing this procedure during an upgrade on the inactive server of a two-server configuration	step <a href="#">6</a>
otherwise	step <a href="#">5</a>

5 Stop the security services by doing the following:

a Type:

```
servstop RADSVR
```

and press the Enter key.

b Type:

```
servstop IS
```

and press the Enter key.

c Type:

```
servstop WEBSERVICES
```

and press the Enter key.

6 Change directories by typing:

```
cd
/opt/nortel/applications/security/current_slis
ext/swmgmt/bin
```

and pressing the Enter key.

7 Perform the restore operation by typing:

```
./brr_security.sh -restore /data/bkresmgr/
<date><time>backupSS1.1<host_name>.tar
```

where <date><time>backupSS1.1<host\_name>.tar is the backup file from which you are restoring.

Press the Enter key.

<b>If</b>	<b>Do</b>
you are performing this procedure during an upgrade on the inactive server of a two-server configuration	step <a href="#">9</a>
otherwise	step <a href="#">8</a>

**8** Restart the security services by doing the following:

**a** Type:

**servstart WEBSERVICES**

and press the Enter key.

**b** Type:

**servstart IS**

and press the Enter key.

**c** Type:

**servstart RADSVR**

and press the Enter key.

**9** If the restored image was backed up from a different server with a different certificate or if the restored certificate has expired, follow the procedure in “Replacing HTTPS certificate on security server for SunOne component” in ATM/IP Solution-level Security and Administration, NN10402-600 to replace the invalid or expired certificate on the IEMS Server.

**10** Select your next step.

<b>If you are restoring a server</b>	<b>Do</b>
in a simplex configuration	<a href="#">step 13</a>
in a high-availability configuration	<a href="#">step 11</a>

**11** Select your next step.**If**

---

you are performing this procedure during an upgrade on the inactive server of a two-server configuration

otherwise

**Do**

---

step [13](#)

---

step [12](#)

**12** Clone the active server to the inactive server. For details, see “Cloning the image of one node in a cluster to the other node” in ATM/IP Solution-level Security and Administration, NN10402-600.

**13** You have completed this procedure. If applicable, return to the higher level task flow or procedure that directed you to this procedure.



## Device audits

After a dead office recovery, several data mismatches may be present in the network. An audit must be performed to clear up these data mismatches. The following table lists the audit procedures available for each component and where those procedures are located.

**Table 1 Device audit procedures**

Component	Procedures available	Location
CS 2000 Core Manager or Core and Billing Manager	'Performing a system audit'	CS 2000 Core Manager Fault Management, NN10082-911
GWC	'Perform a GWC line data integrity audit' 'Perform a GWC trunk data integrity audit' 'Perform a CS 2000 data integrity audit' 'Perform a GWC V5.2 data integrity audit'	GWC Fault Management, NN10202-911
MG 9000	'Performing an audit of the MG 9000 provisioning data'	MG 9000 Configuration Management, NN10096-511