NN10190-113

Carrier Voice over IP

Lawful Intercept (NA)

Product and Technology Fundamentals

(I)SN09 and up Standard 07.02 January 2006

NORTEL NETWORKS™

Carrier Voice over IP

Lawful Intercept (NA)

Lawful Intercept (NA) Product and Technology Fundamentals

Publication number: NN10190-113
Product release: (I)SN09
Document release: Standard 07.02
Date: January 2006

Publication history

January 2006

07.02 Standard version - SN09 and up

Enhanced Note at beginning of procedure “Creating a CDC” to support FSK CDC links in hybrid configurations.

September 2005

07.01 Preliminary version - SN09 and up

Added the following feature descriptions of new software functionality to chapter “Lawful Intercept basics”:

- SN09 LI Support of SIP Lines

Additional changed content includes:

- Added SIP-specific information to the following procedures:
  - “Configuring BCT on an MS 2000 Series”
  - Creating call content resources (CCR)
  - “Add a surveillance”
- Updated procedure “Configuring bearer channel tandeming on an MS 2000 Series” to reflect Integrated Element Manager Series (IEMS) use.
- Transferred Private Network Interception (PNI) information from separate chapter to new section “Feature descriptions” in chapter “Lawful Intercept basics”.

Lawful Intercept basics

What's new in Lawful Intercept in SN09

The following table highlights the LI features introduced in this release.

SN09 LI features

Feature changes
LI Support of SIP Lines This feature enables USNBD to support call data and call content monitoring for calls originating or terminating on SIP lines.

Refer to section Feature descriptions in this chapter for details on the listed feature.

Functional description

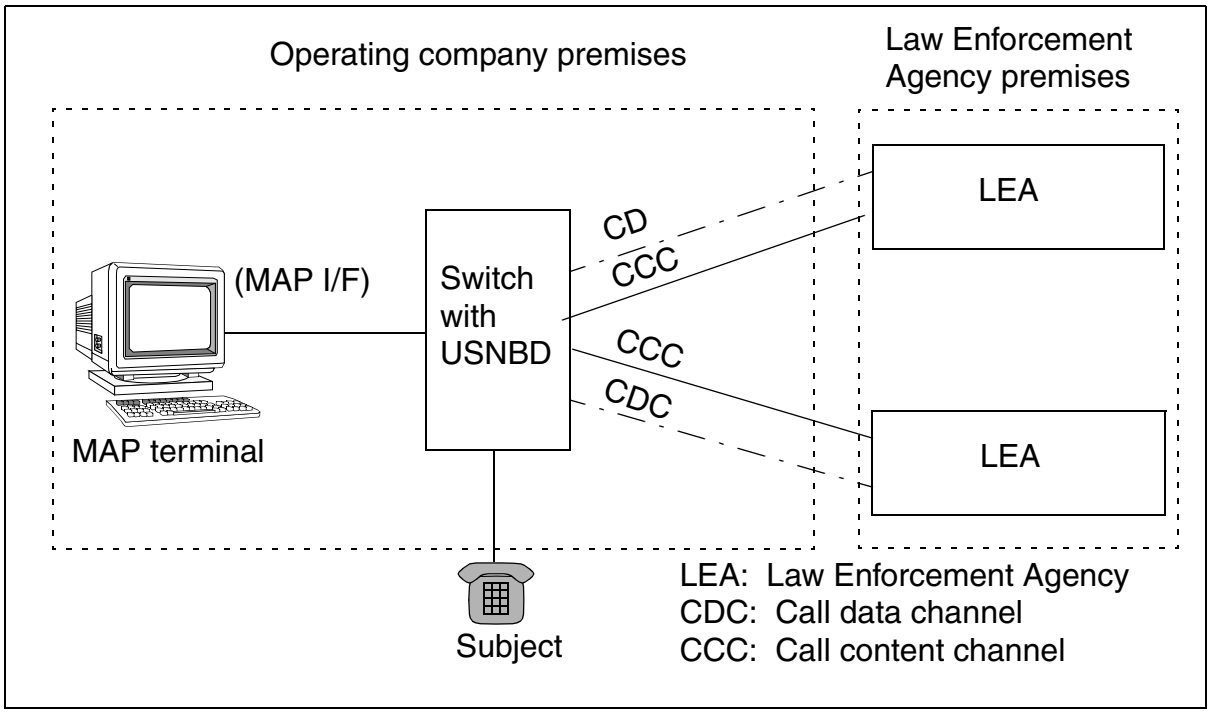
The Communications Assistance for Law Enforcements Act (CALEA) requires that telecommunications equipment manufacturers provide operating companies with the capability to support lawfully authorized electronic surveillance (LAES) activity. Electronic surveillance refers to the mechanism used to access intercepted call content and call data from a switch-based subject, and deliver this information to one or more law enforcement agencies (LEA).

The United States Network Broadcast Delivery (USNBD) feature is Nortel's electronic surveillance product for time division multiplex (TDM) and Voice over IP/Voice over ATM (VoIP/VoATM) networks.

The USNBD feature complies with CALEA requirements, and provides North American Carrier Voice over IP (Carrier VoIP) portfolio with the capability to support lawfully authorized electronic surveillance activity. With the USNBD feature, operating companies have the capability to monitor calls made and received by a switch-based subject and deliver the monitored information to authorized LEAs that require it.

The USNBD feature operates on a switch basis. A subject must be connected to the same switch where the USNBD feature is located for LEAs to have access to the subject's communications.

The following figure illustrates the network overview of USNBD.



Feature descriptions

This section describes software features associated with Lawful Intercept USNBD.

LI Support of SIP Lines

This feature enables USNBD to support call data and call content monitoring for calls originating or terminating on Session Initiation Protocol (SIP) lines.

If call data and call content monitoring are enabled on a SIP surveillance, call data channel (CDC) messages are generated. This result also occurs when call content is not monitored due to an unavailable centralized replicator (CR).

Note: This feature is applicable to the Carrier Hosted Services (CHS) solution.

Call data monitoring

This subsection describes how LI Support of SIP Lines interacts with call data monitoring, particularly the SIP REFER (or Blind Transfer) feature.

REFER support The following scenarios briefly describe the impacts to call data monitoring when transferring a call on a SIP client with the REFER feature.

Note 1: The scenarios are based on Party A call transferring Party B to Party C after A and B have established the call. A disconnects, no longer part of the call.

Note 2: * identifies the monitored party (subject), which varies among scenarios.

Use the following table to identify the parameters listed in the subsequent CDC message tables.

Call data monitoring REFER support legend

Parameter(s)	Description	Examples
A, B, C	Directory numbers (DN) of the agents involved in the call	CalledPartyIdentity - A / Pa
Nx	Sequence number	CallIdentity - SequenceNo: N1
Pa, Pb, Pc	Ports of the agents involved in the call	CalledPartyIdentity - C / Pc

- Call transfer to subject. Two calls are monitored:
  - A – C* (interim call)
  - B – C*

  In this scenario, the following CDC messages are generated as a result of SIP REFER feature.

CDC messages - call transfers to subject

Message	Parameter Attribute Value	Notes
TerminationAttempt	CallIdentity - SequenceNo: N1 CallingPartyIdentity - A / Pa CalledPartyIdentity - C / Pc	A – C* call
Connect	CallIdentity - SequenceNo: N1 ConnectParty Identities - A / Pa, C / Pc	
Answer	CallIdentity - SequenceNo: N1 AnsweringPartyIdentity - C / Pc	
Disconnect	CallIdentity - SequenceNo: N1	
Release	CallIdentity - SequenceNo: N1	

CDC messages - call transfers to subject

Message	Parameter Attribute Value	Notes
TerminationAttempt	CallIdentity - SequenceNo: N2 CallingPartyIdentity - B / Pb CalledPartyIdentity - C / Pc	B – C* call
Connect	CallIdentity - SequenceNo: N2 ConnectPartyIdentities - B / Pc, C / Pc	
Answer	CallIdentity - SequenceNo: N2 AnsweringPartyIdentity - C / Pc	

- Associate call transfers to non-subject. Two calls are monitored:
  - A – B* (initial call)
  - B* – C

In this scenario, the following CDC messages are generated as a result of SIP REFER feature.

CDC messages - associate call transfers to non-subject

Message	Parameter Attribute Value	Notes
Disconnect	CallIdentity - SequenceNo: N1	A – B* call
Origination	CallIdentity - SequenceNo: N2 CallingPartyIdentity - B / Pb CalledPartyIdentity - C / Pc Input - UserInput: <dialed digits>	B* – C call
Connect	CallIdentity - SequenceNo: N2 ConnectPartyIdentities: B / Pb, C / Pc	
Answer	CallIdentity - SequenceNo: N2 AnsweringPartyIdentity - C/ Pc	

- Associate call transfers to subject. Three calls are monitored:
  - A – B* (initial call)
  - A – C* (interim call)
  - B* – C*

In this scenario, the following CDC messages are generated as a result of SIP REFER feature.

CDC messages - associate call transfers to subject

Message	Parameter Attribute Value	Notes
TerminationAttempt	CallIdentity - SequenceNo: N2 CallingPartyIdentity - A / Pa CalledPartyIdentity - C / Pc	A – C* call
Connect	CallIdentity - SequenceNo: N2 ConnectPartyIdentities - A / Pa, C / Pc	
Answer	CallIdentity - SequenceNo: N2 AnsweringPartyIdentity - C / Pc	
Disconnect	CallIdentity - SequenceNo: N1	HOLD A – B* call
Disconnect	CallIdentity - SequenceNo: N2	A – C* call released
Release	CallIdentity - SequenceNo: N2	

CDC messages - associate call transfers to subject

Message	Parameter Attribute Value	Notes
Origination	CallIdentity - SequenceNo: N3 CallingPartyIdentity - B / Pb CalledPartyIdentity - C / Pc Input - UserInput: <dialed digits>	B* – C* call
Connect	CallIdentity - SequenceNo: N3 ConnectPartyIdentities - B / Pb, C / Pc	
TerminationAttempt	CallIdentity - SequenceNo: N3 CallingPartyIdentity - B / Pb CalledPartyIdentity - C / Pc	
Connect	CallIdentity - SequenceNo: N3 ConnectPartyIdentities - B / Pc, C / Pc	
Answer	CallIdentity - SequenceNo: N3 AnsweringPartyIdentity - C / Pc	
Release	CallIdentity - SequenceNo: N1	A – B* call released

- Subject call transfers to non-subject (one original subject). Two calls are monitored:
  - A* – B (initial call)
  - A* – C (interim call, whereby C is the monitored replacement party [MRP] of A)
- Subject call transfers to subject (one original subject). Two calls are monitored:
  - A* – B (initial call)
  - A* – C* (interim call)
  - B – C* (whereby C is the MRP of A)
- Subject call transfers to non-subject (two original subjects). Three calls are monitored:
  - A* – B* (initial call)
  - A* – C (interim call)
  - B* – C (whereby C is the MRP of A)
- Subject call transfers to subject (two original subjects). Three calls are monitored:
  - A* – B* (initial call)
  - A* – C (interim call)
  - B* – C (whereby C is the MRP of A)

Call content monitoring
This subsection describes how LI Support of SIP Lines interacts with call content monitoring.

Multimedia monitoring While SIP lines support multimedia capabilities (such as video and information services), LI Support of SIP Lines supports only the following categories of media monitoring:

- speech
- 3.1 kHz audio
- 64 kbyte restricted and unrestricted data
- 64 kbyte unrestricted data rate adapted from 56 kbyte

Private Network Interception (PNI) Private Network Interception (PNI) provides the ability to intercept the call content of private network calls. The PNI feature supports Internet Transparency (ITRANS), whereby the interception of call content for private network calls can be

enabled or disabled when the media gateways of both call agents are behind the same intra-domain Network Address Translator (NAT).

PNI can be enabled on individual SIP line surveillances. All calls originated by or terminated on a SIP line subject are examined for relevance to call content monitoring. If the call content is not monitored due to PNI not being enabled, CDC message “CCUnavailable” results.

Note: See feature description Private Network Interception (PNI) for details on PNI.

REFER support The following scenarios briefly describe the impacts to call content monitoring when transferring a call on a SIP client using the REFER feature.

Note 1: The scenarios are based on Party A call transferring Party B to Party C after A and B have established the call.

Note 2: * identifies the monitored party (subject), which varies among the scenarios.

- Call transfer to subject. Two calls are monitored:
  - A – C*
  - B – C*

  Only the call with C* must be monitored at a given time. Thus only one call content resource (CCR) is associated with the surveillance on C.
- Associate call transfers to non-subject. Two calls are monitored:
  - A – B* (initial call)
  - B* – C

  Only the call with B* must be monitored at a given time. Thus only one CCR is associated with the surveillance on B*.
- Associate call transfers to subject. Three calls are monitored:
  - A – B* (initial call)
  - A – C* (interim call)
  - B* – C*

  Only one call for each subject must be monitored at a given time. Thus one CCR is associated with surveillances on each B* and C*.

- Subject call transfers to non-subject (one original subject). Two calls are monitored:
  - A* – B (initial call)
  - A* – C (interim call)

  Two calls for A* must be monitored at a given time. Thus two CCRs are associated with the surveillance on A*. Otherwise, the call content for A* – C is not monitored.
- Subject call transfers to subject (one original subject). Three calls are monitored:
  - A* – B (initial call)
  - A* – C* (interim call)
  - B – C*

  Two calls for A* must be monitored at a given time. Thus two CCRs are associated with the surveillance on A*. Otherwise, the call content for A* – C* is not monitored.
- Subject call transfers to non-subject (two original subjects). Three calls are monitored:
  - A* – B* (initial call)
  - A* – C (interim call)
  - B* – C

  Two calls for A* must be monitored at a given time. Thus two CCRs are associated with the surveillance on A*. Otherwise, the call content for A* – C is not monitored.
- Subject call transfers to subject (two original subjects). Three calls are monitored:
  - A* – B* (initial call)
  - A* – C* (interim call)
  - B* – C*

  Two calls for A* must be monitored at a given time. Thus two CCRs are associated with the surveillance on A*. Otherwise, the call content for A* – C* is not monitored.

When a SIP agent under surveillance redirects (using SIP Redirect) or transfer (using SIP REFER) its service to another party, the second set of call content resources (CCR) includes the call content of the originating and monitored replacement parties (MRP). The first set of CCRs rings, but does not include the call content.

SIP impact to LI configuration procedures
The following configuration procedures in this NTP contain SIP-specific information:

- Configuring BCT on an MS 2000 Series – When configuring USNBD on SIP clients, a SIP line surveillance can result in multiple active surveillances, as one SIP line agent supports multiple call appearances. Therefore, provision enough LI ports when configuring BCT for all SIP-related subjects being surveilled. (Procedure Configuring BCT on an MS 2000 Series includes a formula for calculating LI ports on surveillances.)
- Create CCRs – USNBD does not support SIP lines as dedicated CCRs. The CCR must use a single party line with 10 digits.
- Add a surveillance – Surveillances on SIP lines are provisioned against the line DN. When the surveillance is activated, multiple calls originating and terminating on the subject are monitored.

Software dependencies
LI Support of SIP Lines requires the same SIP line dependency as in the CS 2000 Communication Server (CS 2000).

Interactions
LI Support of SIP Lines interacts with non-SIP agents under either or both of the following conditions.

- The SIP line is being surveilled.
- The non-SIP line agent is being surveilled.

LI Support of SIP Lines interacts with MRPs under the following conditions.

- Only the SIP lines are involved in a call.
- The SIP line agents interwork with non-SIP line agents.

See NTP NN10437-111, *CVoIP Session Server Lines - SIP Voice Basics,* for additional information on SIP lines.

Limitations and restrictions
The following limitations and restrictions apply to LI Support of SIP Lines:

- The number of calls monitored for call content is limited by the number of CCRs assigned to the surveillance. Each SIP-line

surveillance can have a maximum of five basic calls monitored for call content.

- The maximum number of active and provisionable SIP-line surveillances is 1024. (If call content is to be monitored, this number can be reduced based on the number of provisioned CCRs.)
- LI Support of SIP Lines does not support multimedia monitoring of video or information services.

Private Network Interception (PNI)

PNI enables interception of the call content of private network calls. The PNI feature supports ITRANS, whereby the interception of call content for private network calls can be enabled or disabled when the media gateways of both call agents are behind the same intra-domain NAT.

Note: For information about ITRANS, refer to NN10205-511, Gateway Controller Configuration Management.

Provisioning PNI

The PNI feature is provisionable on individual surveillances. During configuration of a surveillance order, the LEA requests the service provider to enable or disable PNI. When PNI is enabled, the content of private network calls can be intercepted. When PNI is disabled, the content of private network calls cannot be intercepted.

Note: The LEA must inform the service provider if call content for private network calls is to be intercepted.

A surveillance order is provisioned using the “SURV ADD” command from the USNBD prompt. The PNI field is mandatory and must be datafilled with “Y” or “N.” If “N” is entered, a monitored call behind a private network does not intercept call content nor in-band digit collection.

Note: On a pre-Carrier VoIP switch, the PNI parameter has no effect.

For more information about provisioning PNI, refer to procedure “Adding a surveillance.”

PNI behavior

The following sections briefly describe monitored call behavior in both PNI scenarios.

Monitored calls with PNI disabled If PNI is disabled and both media agents are behind the same NAT, call content for the private

network call is not delivered over the CCR even if a CCR has been provisioned against the monitored call.

Depending on the type of surveillance order provisioned, the following table lists the messaging results that the LEA receives as notification that the call content for the current call is inaccessible (that is, PNI is disabled).

CCR and CDC behavior with PNI disabled

Surveillance order provisioned	Results
CCR only	Call content is not intercepted nor delivered to the LEA. Log UNB303 is generated: "BEARER CHANNEL BEHIND PRIVATE NETWORK" "CALL CONTENT CANNOT BE DELIVERED" ***Note:*** If in-band digit collection (IDC) is provisioned against a surveillance order, and no CDC link is associated with the surveillance, log UNB300 is generated: "BEARER CHANNEL BEHIND PRIVATE NETWORK" "INBAND DIGIT CAPTURE NOT POSSIBLE"
CDC only	CDC messages continue to be generated. However, in-band dialed digits-specific CDC messages are not generated. Post cut-through digits can only be collected when the call traverses the public network. No notification of the absence of digits collection is sent. Log UNB300 is generated: "BEARER CHANNEL BEHIND PRIVATE NETWORK" "INBAND DIGIT CAPTURE NOT POSSIBLE"
CCR and CDC	Call content is not intercepted nor delivered to the LEA. Log UNB303 is generated: "BEARER CHANNEL BEHIND PRIVATE NETWORK" "CALL CONTENT CANNOT BE DELIVERED" All expected CDC messages continue to be generated. However, in-band dialed digits-specific CDC messages are not generated. Post cut-through digits can only be collected when the call traverses the public network. Log UNB300 is generated: "BEARER CHANNEL BEHIND PRIVATE NETWORK" "INBAND DIGIT CAPTURE NOT POSSIBLE"

Monitored calls with PNI enabled If PNI is enabled, content of private network call can be intercepted. Call content is delivered to LEA recording devices. The bearer path of the call is rerouted through the NAT into the public network to media server, similar to inter-NAT LI calls. If a CDC also has been provisioned against the monitoring order, all call data messaging is delivered to the call data decoder of the LEA.

Depending on the type of surveillance order provisioned, the following table lists the messaging results that the LEA receives as notification that the call content for the current call is enabled (that is, PNI is enabled).

CCR and CDC behavior with PNI enabled

Surveillance order provisioned	Results
CCR only	Call content is intercepted and replicated over CCR.
CDC only	CDC messages are generated.
CCR and CDC	Call content and call data are delivered.

Interactions

For LI, call content delivery and in-band digit collections occur when media gateways involved in a monitored call are behind the same NAT. However in some scenarios, call content and in-band digits fail to be intercepted even if PNI is enabled on a monitoring order. If at least two subjects with different PNI settings are involved in a voice conversation, the monitoring order set to “no” overrides the other set values. Therefore, none of the monitoring orders intercept call content and in-band digits when at least two subjects engaged in a call have different PNI settings. The bearer path of the call remains in the private network.

If a call between two monitored subjects is forwarded to a third monitored subject, when the first monitored subject disconnects, call content delivery and in-band digit collection adhere to the settings of the other monitored subjects. If one of the remaining subjects has PNI set to “no,” then call content and in-band digit collection are not intercepted.

However, when multiple surveillances are actively monitoring a single subject at the same time, the disabled PNI value overrides the PNI values of the other surveillances on the subject. Call content and

in-band digit collection are intercepted when one active monitoring order with PNI enabled on the single subject remains.

For the following features, call content is always intercepted regardless of the setting of parameter PNI:

- Three-way calling
- PVG calls
- Multi-service Gateway 4000 (MG 4000) or Interworking Spectrum Peripheral Module (IW-SPM)

Call content monitoring supports PNI on surveillances associated with SIP lines. (See feature description LI Support of SIP Lines for details.)

Limitations and restrictions

The following limitations and restrictions apply to PNI:

- Intra-carrier calls between peer dynamic packet trunking (DPT) gateway controllers (GWC) do not support the PNI functionality.
- In general, call content for intra-carrier calls between peer DPT GWCs is intercepted even if PNI is disabled. However, if the originating DPT-GWC is serving as the slave agent of an intra-carrier call, then call content is not intercepted.

USNBD pre-provisioning requirements

Hardware requirements

Complete table Provisioning data reference for USNBD. Use the entered values to do the calculations described, and complete table Circuit card requirements for Lawful Intercept.

Input data

Enter the values for your switch in table Provisioning data reference for USNBD.

Provisioning data reference for USNBD

CCC variable	Description	Value
Surveillances		
A	Total number of surveillances expected on the switch (maximum 400)	
B	Percentage of surveillances that require call content delivery	
C	Average number of call content resources (CCR) for each surveillance (maximum 5)	
Call content channel (CCC) delivery		
D	Percentage of dedicated lines	

Complete the following calculations to determine the hardware requirements for USNBD. Enter the value beside the correct card in table Circuit card requirements for Lawful Intercept.

Calculate the number of X.25 links

The call data channels (CDC) can communicate with law enforcement agencies (LEA) using X.25 links depending on the hardware type of CM. The X.25 links cannot be used on a Call Server 2000 Compact

(CS2K Compact) CM. A CS2K Compact CM can only use simple control transfer protocol (SCTP) links. The number of X.25 links depends on the following factors:

- A CDC associated with a surveillance can be dedicated to that specific surveillance, or shared by multiple surveillances where all switch surveillances use the same CDC.
- An X.25 facility can support multiple CDCs.
- An X.25 facility can be directly connected to a LEA, or connected to a packet-switched data network where all LEAs share the same facility.
- The multiprotocol controller (MPC) card can support either two 19.2 Kbps low-speed X.25 facilities, or one 56/64 Kbps high-speed facility.

Each switch requires a minimum of two X.25 facilities. The maximum number of facilities is 25.

Note: Nortel Networks recommends provisioning a dedicated X.25 facility for each LEA. Under normal busy-hour traffic patterns, one low-speed 19.2 Kbps X.25 facility can support the delivery of CDC messages for all 400 subjects without any loss of messages.

Calculate the number of SCTP associations (links)

The CDC can communicate with LEAs using SCTP over Internet Protocol (SCTP/IP) links. The number of SCTP associations depends on the following factors:

- A CDC associated with a surveillance can be dedicated to that specific surveillance, or shared by multiple surveillances where all switch surveillances use the same CDC.
- An SCTP/IP facility can support up to eight associations to CDCs.
- An SCTP/IP facility can be directly connected to an LEA, or connected to a packet-switched data network where all LEAs share the same facility.

Note: Nortel Networks recommends provisioning a dedicated SCTP/IP facility for each LEA. Under normal busy-hour traffic patterns, one SCTP/IP facility can support the delivery of CDC messages for all 400 subjects without any loss of messages.

Calculate the number of bearer channel tandeming (BCT) cards

Use the following formula to determine the number of BCT cards in the UAS required for performing Carrier VoIP-based monitoring:

4 × A × B × C = Number of BCT endpoints

Number of BCT cards = (Number of BCT endpoints / BCT endpoints for each card) + 1

Note: For IP, the number of BCT endpoints for each card is 90. For asynchronous transfer mode (ATM), the number of BCT endpoints for each card is 500.

Calculate the number of CCC circuits

To determine the number of dedicated lines required for USNBD, use the following formula:

A × B × C × D × 2 = Number of dedicated lines required

Circuit card requirements for Lawful Intercept

PEC	Function	CM Type
NT1X89BA, NT1X89BB or IOM equivalent	MPC card, or enhanced MPC (EMPC) card for X.25 datalinks	SN series, XA-Core
NTLX03AA	Input/output processor (IOP) card for supporting CDC using SCTP/IP (2 or 4 cards)	SN series, XA-Core
NTLX09AA	Ethernet packlet card for supporting CDC association using SCTP/IP (2 or 4 cards)	SN series, XA-Core, CS2K Compact

Note: Do not configure CCCs behind a NAT that is identified as a limited bandwidth link (LBL). Otherwise, LEA monitoring parties ring but do not receive speech path.

Information required prior to surveillance setup

The LEA and the service provider (SP) must agree upon the following information to establish a surveillance using USNBD:

- What is the case identity to be included in all CDC messages related to the specific surveillance?
- What is the subject's identity? (The SP must translate this information to set up a proper USNBD surveillance.)

- Is call data delivery required? (The SP must verify that the CDC to be associated to this surveillance uses the SCTP or X.25 link of the LEA requesting this surveillance.)
- Is call content delivery required?
  - Specify the delivery method (dedicated or switched)
  - Specify the number of CCRs associated with the surveillance
  - Specify the signalling type of CCR (signalling or non-signalling)
  - Specify the type of CCR (paired or combined)
- Is redirection monitoring provided?
- Is the calling party number delivered in CDC messages?
- Is held conference monitoring provided?
- Is in-band digit collection through CDC messages provided?
- Is Call Content Correlation Tag Delivery provided?

Optional hardware

Refer to the following table for optional LI hardware for ATM systems.

Card	Description	Enables functionality
NT3X68AB	Dual tone multi-frequency (DTMF) sender card	CCC tag delivery
NT2X48AB	DTMF receiver card	In-band digit collection
NTAR02JC	AG4000 card for Universal Audio Server (UAS) announcements and tones	C-tone
NTAR02JE	AG4000 card for UAS rear input/output (I/O) module	C-tone

Refer to the following table for optional LI hardware for IP systems.

Card	Description	Enables functionality
NTAR02JF	CG6000 card for UAS interactive voice response (IVR)	C-tone, in-band digit collection, CCC
NTAR02JG	CG6000 card for UAS rear I/O module	C-tone, in-band digit collection, CCC

Switch provisioning considerations

Service providers should consider the following items:

- pre-provisioning of X.25 interfaces
- low- or high-speed links
- facilities to LEAs

Pre-provisioning of X.25 interfaces

Use MPC cards (NT1X89BB) in the IOC, or upgrade to IOM.

Note: NT1X89BB cards were manufactured discontinued (MD) with a last-time purchase date of 31 March 2000. Currently, IOMs (NTFX4101) with their applicable card (NTFX30AA, NTFX31AA and NTFX34AA) must be purchased.

Low- or high-speed links

Each NT1X89BB card supports two low-speed links, or one high-speed link. In the IOM, each card supports up to 16 links regardless of speed. Under testing of normal busy hour conditions, one 19.2 Kbps link can handle all CDC messages for the maximum 400 surveillances.

Facilities to LEAs

The LEAs can be assigned a dedicated facility. If one facility is used for all LEAs, an external device is required to segregate the data.

Surveillance checklist

This checklist is intended as a tool to:

- identify information required prior to setting up a surveillance
- identify who provides the information
- when applicable, specify where to find information in this document

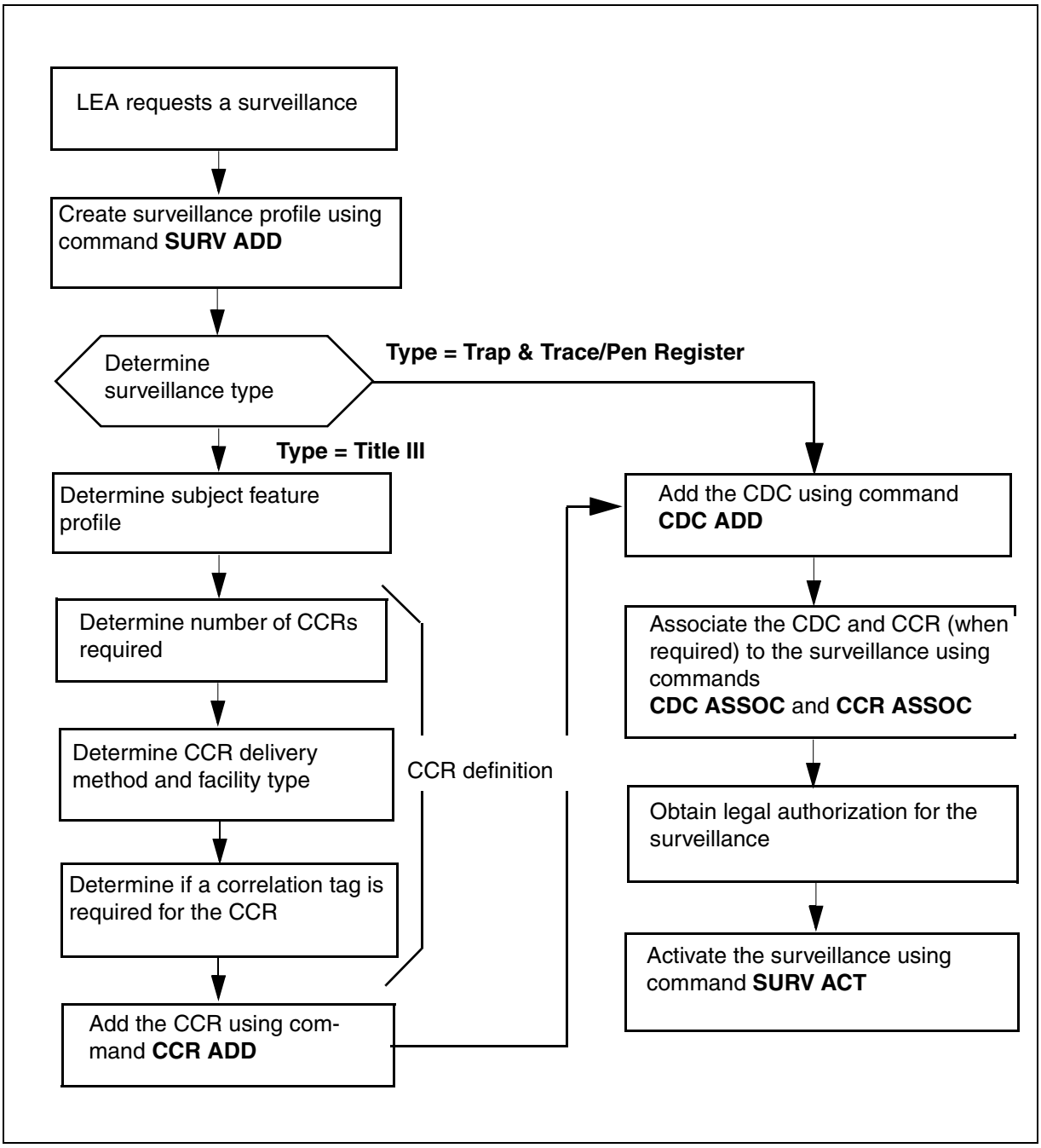
Repeat the following procedures for each agency performing the surveillance. The basic steps in setting up and activating a surveillance are as follows:

- create a surveillance profile using the SURV ADD command (see Adding a surveillance)
- add a CDC using the CDC ADD command (see Creating a CDC)
- add additional CCRs for a surveillance using the CCR ADD command (see Creating CCRs)
- associate a CDC with a specific surveillance using the CDC ASSOC command (see Creating a CDC)
- associate a CCR with a specific surveillance using the CCR ASSOC command (see Associating a CCR with a surveillance)
- activate a surveillance using the SURV ACT command (see Activating a surveillance)

The following figure summarizes the process for communications assistance to law enforcement. Use the instructions in the procedures that follow to implement this process.

Note: The LEA must have provided all information that requires determination in figure Process for communications assistance to law enforcement to the SP.

Process for communications assistance to law enforcement



Surveillance checklist

Create surveillance profile

1 When an LEA requests a surveillance, the LEA must provide the SP with the following information:

- directory number (DN)
- surveillance type (Trap & Trace/Pen Register or Title III)
- case ID (surveillance identity)

2 The SP uses the QDN command to determine the surveillance handle of the subject. The SP also determines if redirection monitoring is to be provided, and if the calling party number is to be included in the CDC message. This information is used as input for the SURV ADD command.

Note: If a subject with an active surveillance on the line is a POTS subscriber and then orders a feature for the line, the line type can change from POTS to RES. This action takes down the surveillance. To re-activate the surveillance, perform the setup procedure again.

3 For LEA's communicating with the SP using X.25, the LEA provides the SP with the CDC X.25 address where surveillance data is to be sent. The SP uses the CDC address and MPC card location for the CDC ADD command.

For LEA's communicating with the SP using SCTP/IP, the LEA provides the SP with the CDC SCTP/IP association (address) where surveillance data is to be sent. The SP uses the CDC SCTP/IP association for the CDC ADD command.

4 Identify the type of surveillance required

If the surveillance type is	Do
Title III	step 5
Trap & Trace/Pen Register	step 9

Note: The above types are LEA titles. Trap &Trace/Pen Register is CDC surveillance, and Title III is both CDC and CCR surveillance.

5 The SP determines the subject's feature profile using the QDN command.

6 The SP and LEA determine the number of CCRs depending on the subject's feature profile. For example, if the subject has redirection features, such as the following, then an additional CCR is required to increase the probability of delivering all call

content. If held conference monitoring is enabled on the switch, one additional CCR is required to deliver all call content.

- call forward busy (CFB)
- call forward don't answer (CFDA)
- call forward universal (CFU)
- call transfer (CXR)
- universal 3-way calling (U3WC)

7 The LEA and SP determine the delivery method and the facility type. (See the following tables for brief descriptions.)

CCR definition - delivery method

Method	Equipment required for each CCR
Paired	2 lines
Combined	1 line ***Note:*** Combined uses one line plus one conference circuit port.

Facility type	Signalling option
Dedicated lines	Y or N
Switched lines	N/A

8 The SP enters the command CCR ADD using information from steps 5 through 8.

9 The SP enters the command CDC ASSOC and if required, the command CCR ASSOC.

10 The SP receives legal authorization for the surveillance.

11 The SP activates the surveillance using the command SURV ACT.

Configuration management

List of procedures

The USNBD administrators and USNBD users can perform the following procedures:

- Configuring a Universal Audio Server (UAS) for bearer channel tandeming (BCT)
- Configuring bearer channel tandeming on an MS 2000 series
- Activating software optionality control (SOC) option NBD00003
- Activating software optionality control (SOC) option NBD00004
- Activating bearer channel tandeming (BCT)
- Activating USNBD office-wide parameters
- Adding an agency
- Adding USNBD users
- Creating call content resources (CCR)
- Creating a call data channel (CDC)
- Listing a surveillance
- Adding a surveillance
- Associating a call data channel (CDC) with a surveillance
- Associating a call content resources (CCR) with a surveillance
- Activating a surveillance
- Deactivating a surveillance
- Taking down a surveillance
- Deleting a call content resource (CCR)
- Deleting a call data channel (CDC)
- Deleting USNBD agencies
- Deleting USNBD users
- Deactivating bearer channel tandeming (BCT)

- Deactivating software optionality control (SOC) option NBD00003
- Deactivating software optionality control (SOC) option NBD00004
- Accessing LI-specific operational measurements

Configuring bearer channel tandeming on a UAS

This procedure enables you to configure a previously-installed Universal Audio Server (UAS) for bearer channel tandeming (BCT). Use this procedure to configure an ATM-AAL2 or Internet Protocol (IP) system for BCT functionality.

Note 1: This procedure applies to a UAS in either an IP network or an ATM-AAL2 network. If you have an ATM-AAL1 network, this procedure does not apply. The UAS comes pre-configured for BCT on an ATM-AAL1 network.

Note 2: The UAS on which this procedure is performed must have already been installed with release UAS07, or greater, software. The UAS must also have the appropriate hardware configuration to support BCT functionality.

Note 3: The user performing this procedure must have USNBD administrative privileges.

Note 4: This procedure assumes that only some of the CG6000 cards provisioned in the UAS node are to be used for BCT. If all of the CG6000 cards are to be used for BCT, IVR and Conferencing Service functionality for the node must not be enabled.

Configuring BCT on a UAS

At the Network Element Status pane 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 Select the entry for the node in the Node States window. Then lock the node by clicking button **Lock Graceful** at the bottom of the Node States pane.

At the Windows interface for the network element

6 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.

Note: Leave the Services window open for use later in this procedure.

7 Launch the Local Configuration Interface GUI by performing the following step:

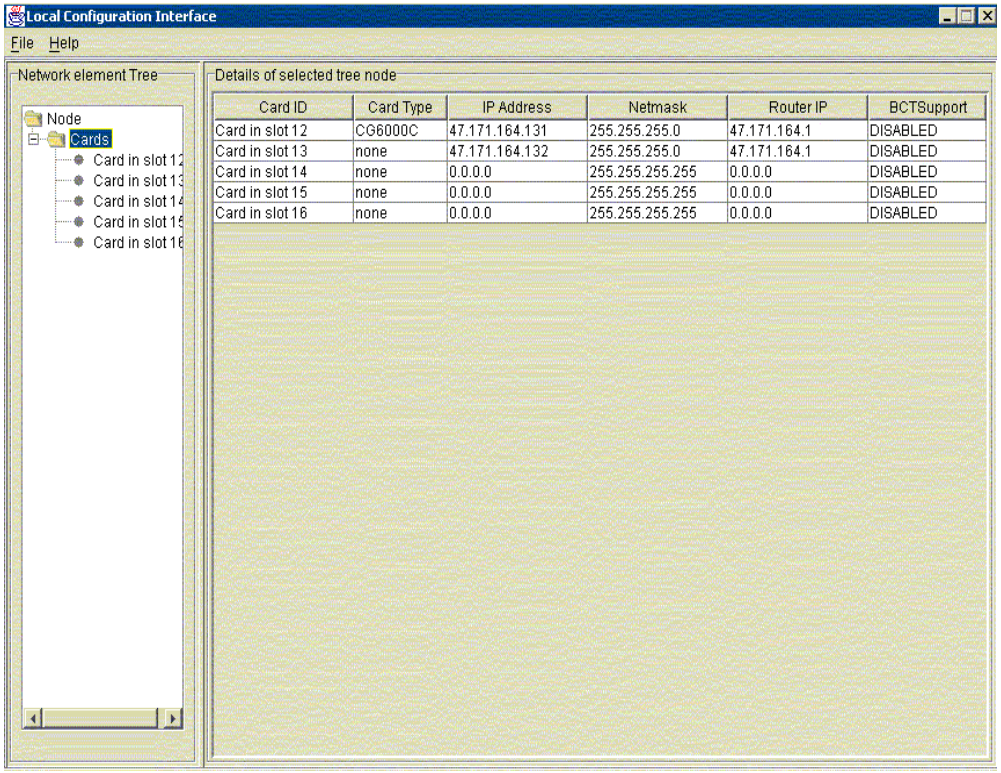
a Open a command window by selecting **Start -> Run**

b Type **lci** in the window that displays.

Note: The first letter in the lci command is an "l," as in the word "local."

c Click **OK** or press Enter.

The main Local Configuration Interface GUI screen displays.



8 Determine the appropriate bearer type for your node.

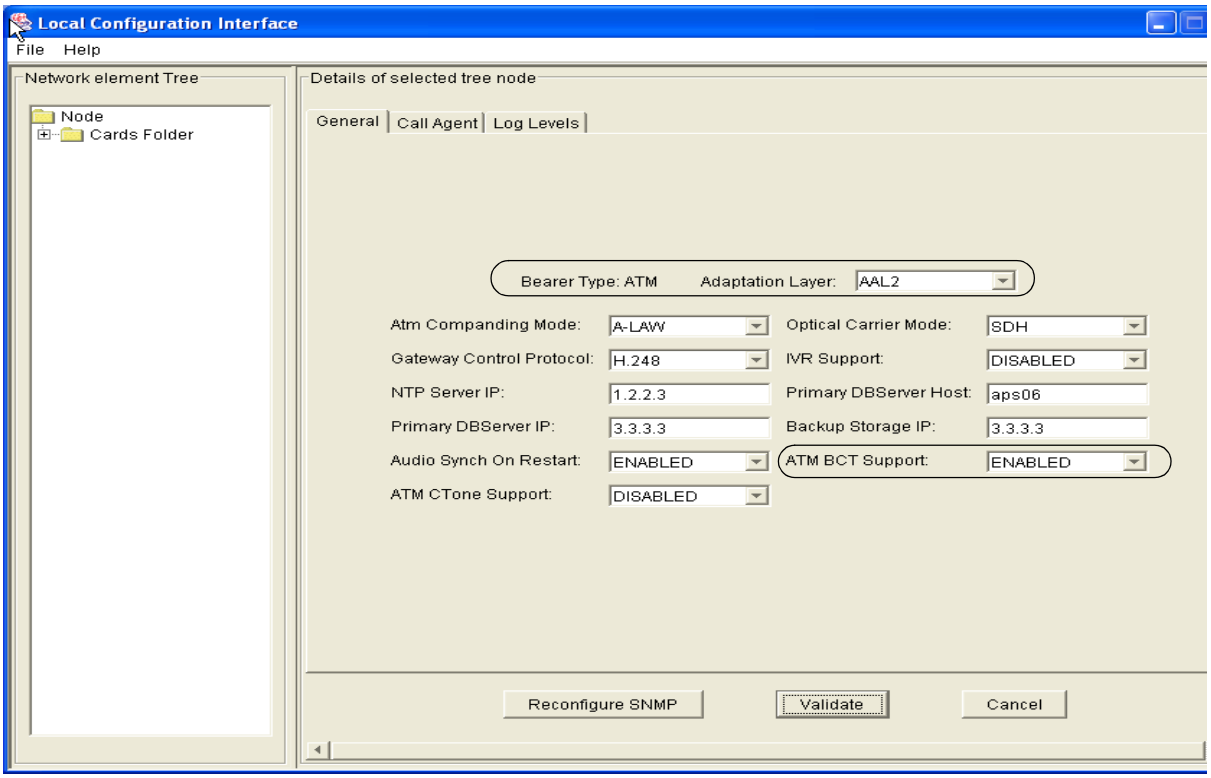
If the UAS bearer fabric type is	Do
ATM-AAL2	step 9
IP	step 16

9 Examine the Adaptation Layer heading on the screen and ensure that the ATM-AAL2 bearer fabric screen is displaying.

If the ATM-AAL2 bearer fabric screen is	Do
not displaying	step 10
displaying	step 11

10 Pull down the Adaptation Layer menu and select the ATM-AAL2 bearer fabric type.

An ATM Local Configuration Interface GUI screen for the ATM-AAL2 fabric type displays.



11 Ensure that field ATM BCT Support is Enabled.

12 Click **Validate**.

13 Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save.” Click **OK** when the confirmation screen displays.

14 Close the Local Configuration Interface GUI by selecting **File -> Exit.**

15 Go to step 21.

16 In the pull-down list in the box labeled “Please select,” select Configuration.

17 In the Configuration Tree pane, select Node.

18 Select the next step as follows.

If the configuration	Do
supports Real Time Protocol (RTP) for dual-tone multifrequency (DTMF)	step 19
does not support RTP for DTMF	step 20

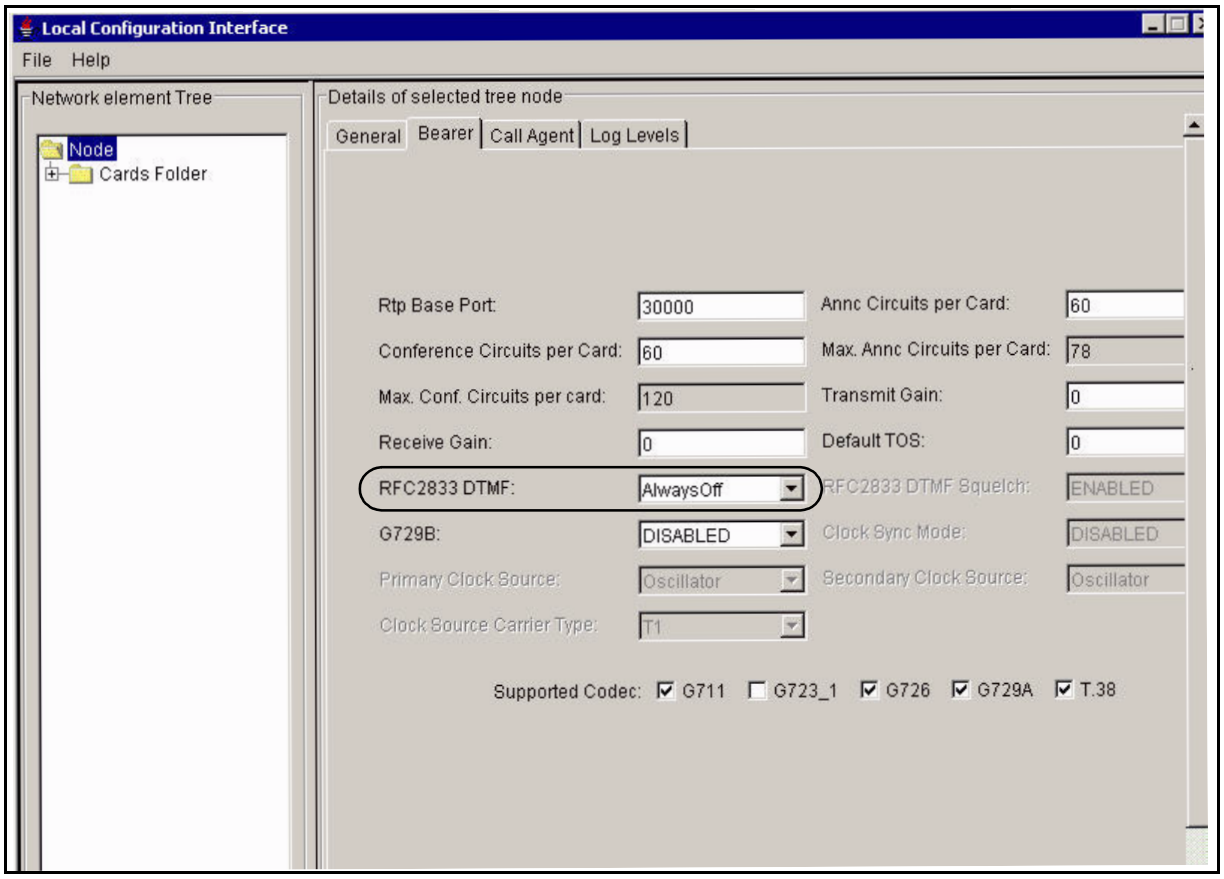
19 Select the Bearer tab.

Field RFC2833 DTMF indicates how the UAS determines if RFC2833 is enabled for each RTP connection. Negotiated is the default setting for field, which applies when all gateway controller nodes (GWC) nodes support RFC2833. Set this field to AlwaysOff if all line GWC nodes have RFC2833 disabled.

Note: See the following NTPs for details on the RFC2833 setting:

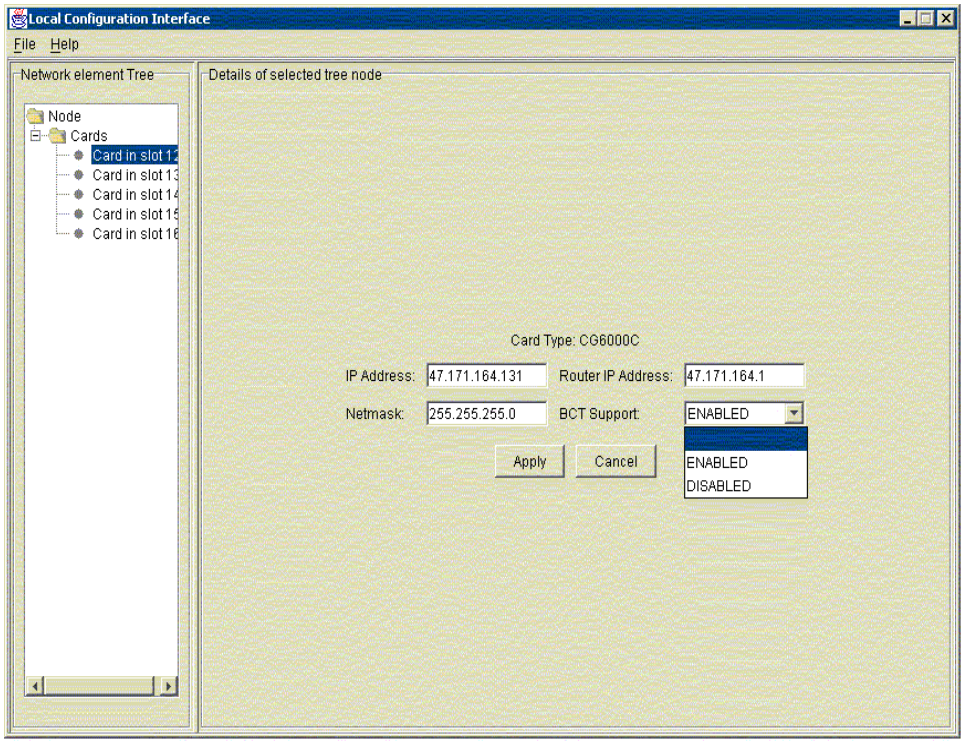
- procedure “Modifying configuration parameters through the UAS Manager,” *UAS Configuration Management*, NN10095-511
- procedure “Add a network codec profile,” *Gateway Controller Configuration Management*, NN10205-511

The following figure shows field RFC2833 DTMF set to AlwaysOff.



20 In the Topology pane of the Local Configuration Interface GUI screen, first select the Nodes folder. Within the Nodes folder, select the Cards folder.

The Local Configuration Interface GUI cards screen displays.



a Review the card list that displays. Field Card Type is set automatically to “CG6000C” if a card is present. Field Card Type is set to “none” and the information detail field labels are colored grey if no card is present. Double click the Cards folder. From the list of cards that displays below the Cards folder, click the bullet associated with the card to be dedicated to BCT. Ensure that field BCT Support is Enabled.

b Click **Validate**.

c Pull down the menu under File (located at the top left-hand corner of the Local Configuration Interface GUI screen) and select “Save.” Click **OK** when the confirmation screen displays.

d Close the Local Configuration Interface GUI by selecting **File -> Exit.**

21 Restart the network element by performing the following steps:

a If the Services window is not already open, access it as follows:

Start -> Programs -> Administrative Tools -> Services

b Right-click **PMGRdaemon service** and select Start. Wait approximately 2 or 3 minutes before performing the next step to ensure that the UAS has restarted.

At the Network Element Status pane of the Universal Audio Server Manager

22 After the network element has restarted (that is, the network element appears in the Network Elements pane), set the administrative state for this UAS node to “unlocked” by performing the following steps.

a In the Network Elements pane, select the appropriate UAS node.

Information about the node displays in the System Identification pane.

b In the pull-down list in the box labeled “Please select,” select Maintenance.

c In the Maintenance Tree pane, select “Node.”

d Click the node entry that displays in the table shown in the Node States pane.

e Unlock the node by clicking **Unlock** at the bottom of the Node States pane.

23 You have completed this procedure.

Configuring bearer channel tandeming on an MS 2000 Series

Purpose of this procedure

This procedure enables you to configure the Lawful Intercept parameter in support of enabling bearer channel tandeming (BCT) on one of the following Nortel Networks media servers (MS 2000 Series):

- MS 2010 for an IP network
- MS 2020 for an ATM network

The MS 2000 Series is sold in different configurations based on the availability of the total number of ports. The MS 2010 is available in 120- and 240-port configurations. The MS 2020 is available in 240- and 480-port configurations. The Lawful Intercept parameter is configured on all MS 2000 Series boxes based upon software feature keying and hardware requirements. As long as the feature key of the MS 2000 Series is set to support BCT, from 0 to the maximum number of ports available in its configuration type can be allocated to LI.

Note 1: For the remainder of this procedure, the term “MS 2000 Series” refers to either an MS 2010 or an MS 2020.

Note 2: For details on configuration parameters for the MS 2000 Series, refer to NN10340-511, *MS 2000 Series Configuration Management*.

When to use this procedure

Configuring parameters is executed during an installation or upgrade of the MS 2000 Series. Lawful Intercept is one of the parameters configurable through the MS 2000 Maintenance and Configuration tool.

The MS 2000 Maintenance and Configuration tool is accessible through the Integrated Element Management System (IEMS).

Refer to the following Integrated IEMS NTPs for additional details, as directed, when using this procedure:

- NN10329-111, *IEMS Basics*
- NN10330-511, *IEMS Configuration Management*

Additional information

One Session Initiation Protocol (SIP) line agent supports multiple call appearances. When configuring LI on SIP clients, a SIP line surveillance can result in multiple active surveillances. Therefore, provision enough LI ports when configuring BCT for all SIP-related targets under a surveillance.

See feature description LI Support of SIP Lines in chapter Lawful Intercept basics for details.

Calculating LI ports

Use the following formula to calculate the number of LI ports for BCT configuration:

2 * (A + B + C)

where:

A = the maximum number of simultaneous monitored calls with call content or IDC, or both

B = the number of CCRs required to monitor the calls in A

C = the number of calls in that require IDC

Example

Assume that 100 simultaneous calls are to be monitored.

Out of these 100 calls:

a. 20 calls have one CCR

b. 20 calls have two CCRs

c. 20 calls have IDC only

d. 20 calls have one CCR and IDC

e. 20 calls are call data only

The following values result for A, B, and C.

A = 80 calls (sum of a. through d.)

B = 80 calls (sum of a., two b.'s, and d.)

C = 40 calls (sum of c. and d.)

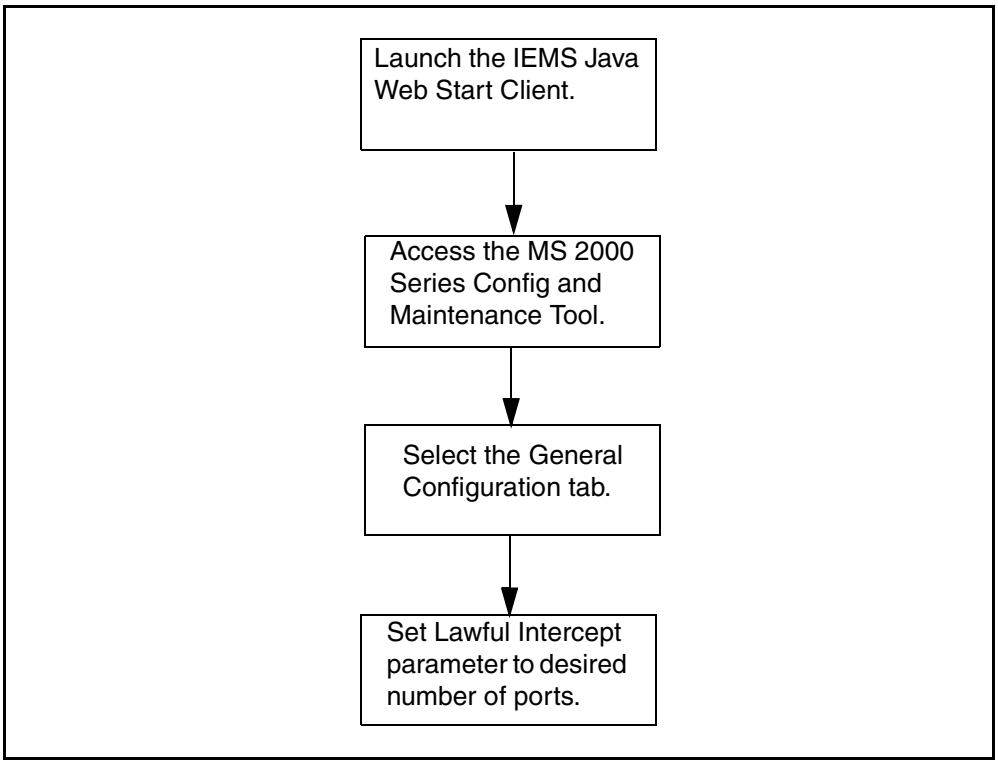
The number of LI ports to be configured for BCT in this example is 400:

2 * (80 + 80 +40) = 2 * 200 = 400

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow to perform the procedure.

Summary of configuring an MS 2000 Series for BCT



Configuring BCT on an MS 2000 Series

At the IEMS workstation

1 Launch the IEMS Java Web Start Client.

Note: Refer to procedure “Launching IEMS Java Web Start Client.” See NTP NN10329-111, *IEMS Basics*.

2 Select the Networks Element topology node in the IEMS tree.

3 Select an MS 2000 map symbol in the IEMS display panel.

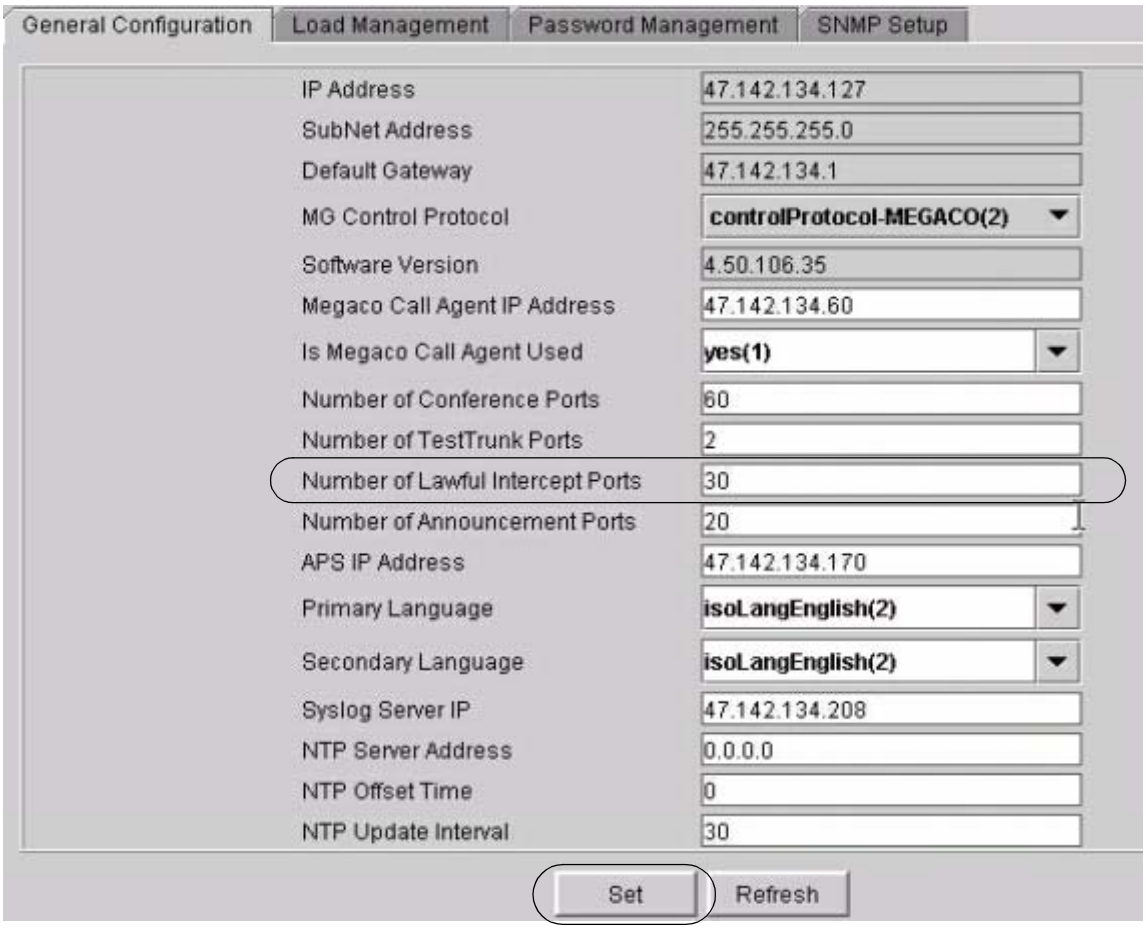
4 Right click the map symbol and select “Config and Maintenance Tool” menu item.

The Configuration and Maintenance tool launches.

5 Click the General Configuration tab in the right side of the Maintenance and Configuration tool.

The following menu displays.

IEMS General Configuration menu



6 Enter the number of ports in field Number of Lawful Intercept Ports.

7 If needed, populate any remaining fields in this menu.

8 Click the Set button to save all configuration data.

Valid data entry prompts you to save the configuration data by backing up the INI file.

The following error message displays if invalid data was entered.

```
Error occurred while setting the data on the
node.
```

> ***Note:*** *Refer to procedure "Configuring general parameters for MS 2000 NEs." See NTP NN10330-511, IEMS Configuration Management, for details on saving the configuration data.*

9 You have completed this procedure.

Activating SOC option NBD00003

Purpose of this procedure

The purpose of this procedure is to activate USNBD in an office. This procedure is performed by a user who has been designated as a USNBD administrator.

When to use this procedure

Use this procedure once the software load that includes the USNBD feature is added to the switch, and it is required to activate USNBD.

Prerequisites and Restrictions

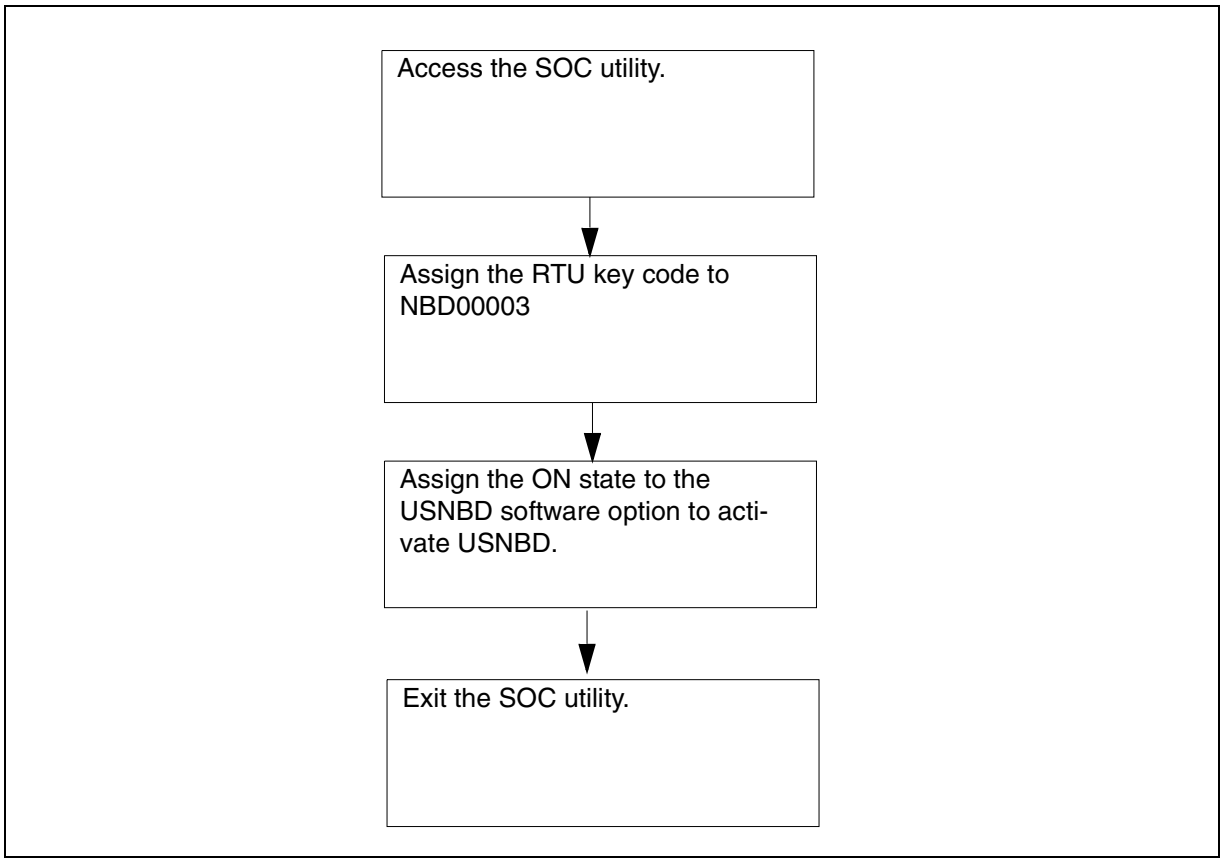
The user performing this procedure must have access to the USER command of USNBD and to the appropriate software optionality control (SOC) commands. Therefore, adhere to the following recommendations *before* performing this procedure.

- Create a privilege class specific to USNBD using the PRIVCLAS command, and assign the USNBD privilege class to authorized users using the PERMIT command.
- Obtain the right-to-use (RTU) key code (password) from your Nortel Networks representative to activate SOC option NBD00003.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of Activating SOC option NBD00003



Activate SOC option NBD00003

At the CI level of the MAP

1 Access the SOC utility by typing:

SOC

and pressing the **Enter** key.

Example Response:

```
SOC :
```

2 Display the status of the USNBD software option by typing:

select option nbd00003

and pressing the **Enter** key.

Example Response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00003 USNBD     N  IDLE   -     -       -     02/05/10
```

3 Assign the RTU key code to the USNBD software option by typing:

assign rtu <key_code> to nbd00003

and pressing the **Enter** key.

where

key_code
is the password obtained from your Nortel Networks representative

Example Response:

```
Done.
```

Note: For security reasons, Nortel Networks strongly recommends assigning the ON state to the USNBD software option immediately after assigning the RTU key code to SOC option NBD00003.

4 Verify the RTU status change of the USNBD software option by typing:

select option nbd00003

and pressing the **Enter** key.

Example Response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00003 USNBD     Y  IDLE   -     -       -     02/05/10
```

5 Assign the ON state to the USNBD software option by typing:

assign state on to nbd00003

and pressing the **Enter** key.

Example Response:

```
Done.
```

You are defined as the initial USNBD administrator.

6 Verify the state change of the USNBD software option by typing:

select option nbd00003

and pressing the **Enter** key.

Example Response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00003 USNBD     Y  ON    -     -       -     02/05/10
```

7 Use the following table to determine your next step.

If	Do
TRIG log generation and Frequency Shift Keying (FSK) CDC functionality is required by the LEA	Refer to section Activating SOC option NBD00004 in this document.
TRIG log generation and FSK CDC functionality is NOT required by the LEA	step 8

8 Exit the SOC utility by typing:

quit

and pressing the **Enter** key.

9 You have completed this procedure.

Activating SOC option NBD00004

Purpose of this procedure

The purpose of this procedure is to activate USNBD FSK Line CDC functionality in an office. This procedure is performed by a user who has been designated as a USNBD administrator.

When to use this procedure

Use this procedure once the software load that includes the USNBD feature is added to the switch through NBD00003, and it is required to activate USNBD FSK Line CDC functionality.

Prerequisites and Restrictions

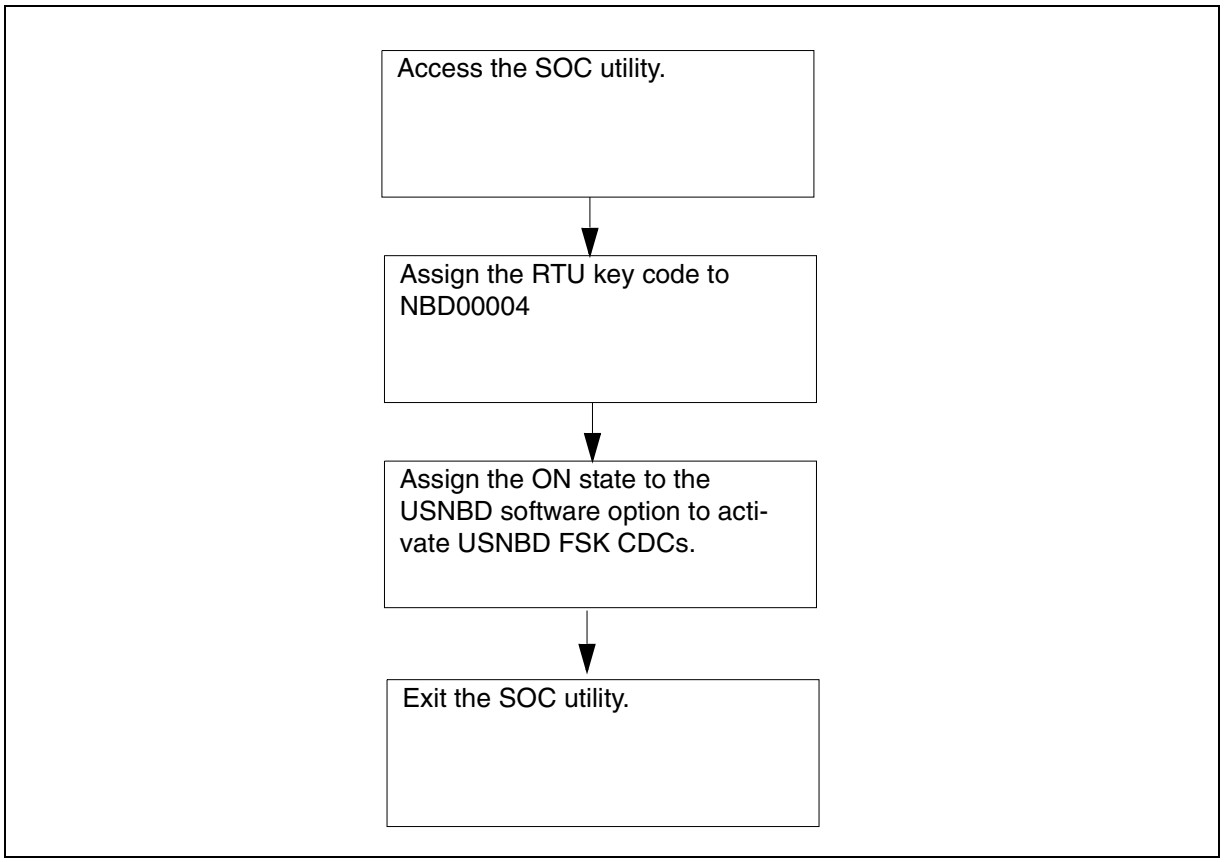
The user performing this procedure must have access to the USER command of USNBD and to the appropriate software optionality control (SOC) commands. Therefore, adhere to the following recommendations *before* performing this procedure.

- Ensure the user is part of the same priv class that was used for USNBD.
- Obtain the right-to-use (RTU) key code (password) from your Nortel Networks representative to activate SOC option NBD00004.
- Ensure SOC option NDB00003 is ON.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of Activating SOC option NBD00004



Activate SOC option NBD00004

At the CI level of the MAP

1 Access the SOC utility by typing:

SOC

and pressing the **Enter** key.

Example Response:

```
SOC :
```

2 Display the status of the USNBD software option by typing:

select option nbd00004

and pressing the **Enter** key.

Example Response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00004 USNBD     N  IDLE   -     -       -     02/05/10
```

3 Assign the RTU key code to the USNBD software option by typing:

assign rtu <key_code> to nbd00004

and pressing the **Enter** key.

where

key_code
is the password obtained from your Nortel Networks representative

Example Response:

```
Done.
```

Note: For security reasons, Nortel Networks strongly recommends assigning the ON state to the USNBD software option immediately after assigning the RTU key code to SOC option NBD00004.

4 Verify the RTU status change of the USNBD software option by typing:

select option nbd00004

and pressing the **Enter** key.

Example Response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00004 USNBD     Y  IDLE   -     -       -     02/05/10
```

5 Assign the ON state to the USNBD software option by typing:

assign state on to nbd00004

and pressing the **Enter** key.

Example Response:

```
Done.
```

6 Verify the state change of the USNBD software option by typing:

select option nbd00004

and pressing the **Enter** key.

Example Response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00004 USNBD     Y  ON    -     -       -     02/05/10
```

7 Exit the SOC utility by typing:

quit

and pressing the **Enter** key.

8 You have completed this procedure.

Activating bearer channel tandeming

Purpose of this procedure

The purpose of this procedure is to activate bearer channel tandeming (BCT) functionality provided by a Universal Audio Server (UAS) subtended from a Communication Server. This procedure is performed by a USNBD user (with or without administrator privileges).

When to use this procedure

Use this procedure only once, the first time an LEA requests that a surveillance be activated on this Communication Server. Subsequent surveillance requests do not require executing this procedure.

For additional assistance with the **BCT** command, type **bct help** at the USNBD: prompt.

Prerequisites

The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights.

When adding a BCT tuple in table SERVSINV, an AUD tuple must be present in the table pointing to the same gateway controller (GWC) as the BCT tuple, even if the UAS associated with that GWC is not intended to play announcements or conferencing.

CAUTION

Partial service disruption

If the AUD tuple is not present and that UAS is taken out of service, the CORE is NOT informed, the BCT “node” is not busied, and calls attempt to be tandemed on a UAS that is out of service.

CAUTION

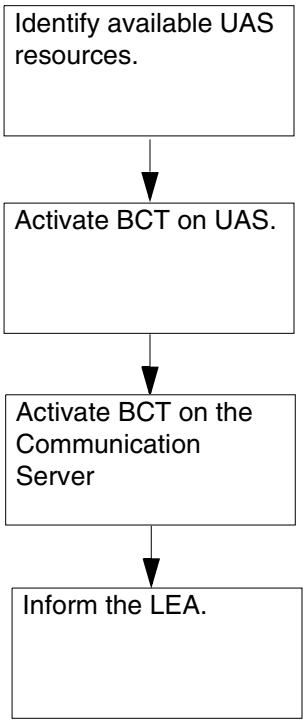
Partial service disruption

If a GWC hosting UAS(es) undergoes a cold Swact maintenance action, all calls going through the UAS(es), including LI calls will be dropped immediately. Always ensure disruptive maintenance procedures are performed during approved maintenance time periods.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of activating BCT on a Carrier VoIP Network



Activate bearer channel tandeming

At the CI level of the MAP

1 Access table SERVSINV of the MAP by typing:

```
table servsinv
```

and pressing the **Enter** key.

2 Allocate BCT resources by typing

```
add BCT x GWC y 1024 ALTTERMS z
```

and pressing the **Enter** key.

where

x
is the BCT tuple number

y
is the identity of the GWC you wish to use to manage the UAS resources.

Note: Use the CS2000 Management Element Manger to acquire the correct identity of the GWC controlling the UAS resources.

z
is the total number of *altterms* or BCT endpoints that the subtending GWC (**y**) of the UAS can use. In an IP network, the recommended default is 90 endpoints for each BCT-configured CG6000 card for each UAS. In a ATM network, the recommended default is 500 endpoints.

Example Response:

```
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
```

3 Ensure that an AUD tuple is present in table SERVSINV and that it points to the same GWC as the BCT tuple you are datafilling.

Note: You can still add the BCT tuple without the AUD tuple. However, a warning displays when the tuple is added.

4 Continue adding the tuple by typing

```
y
```

and pressing the **Enter** key.

Example Response:

```
TUPLE TO BE ADDED:
BCT 0 GWC 3 1024 ALTTERMS 90
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

5 Confirm that you want to add the tuple by typing:

y

and pressing the **Enter** key.

Example Response:

```
TUPLE ADDED

JOURNAL FILE ACTIVE
```

6 If you receive the following message:

WARNING: No AUD node detected on this GWC. AUD node is required to ensure proper BCT node status

Return to step 3 and check your AUD tuple entry. Otherwise, continue with the next step.

7 Access the USNBD level of the MAP by typing:

usnbd

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

8 Display the current status of BCT by typing:

bct status

and pressing the **Enter** key.

Example Response:

```
BCT STATUS: INACTIVE
```

9 Use the following table to determine your next step.

If	Do
BCT status is active	step 11
BCT status is inactive	step 10

10 Activate the BCT functionality by typing

bct activate

and pressing the **Enter** key.

Example Response:

```
BCT ACTIVATE: BCT FUNCTIONALITY ACTIVATED.
RESERVED RESOURCES SET TO 0
```

11 Inform the LEA that BCT has been activated.

12 You have completed this procedure.

Activating USNBD office-wide parameters

Purpose of this procedure

The purpose of this procedure is to activate specific USNBD functional capability on an office-wide basis. This procedure is performed by a USNBD administrator.

This procedure contains the following three sections:

- Activating the Held Conference monitoring (HELDMON) office-wide parameter
- Activating the Trig Log generation (TRIG_LOGS) office-wide parameter
- Setting the Test call billing number (TEST_CALL_BILLNO) office-wide parameter

When to use this procedure

Use this procedure when specific office-wide functionality for USNBD is required, and that functionality is controlled by an office-wide parameter.

The supported parameters are Held Conference monitoring, Trig log generation, and Test call billing number.

Prerequisites

The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights.

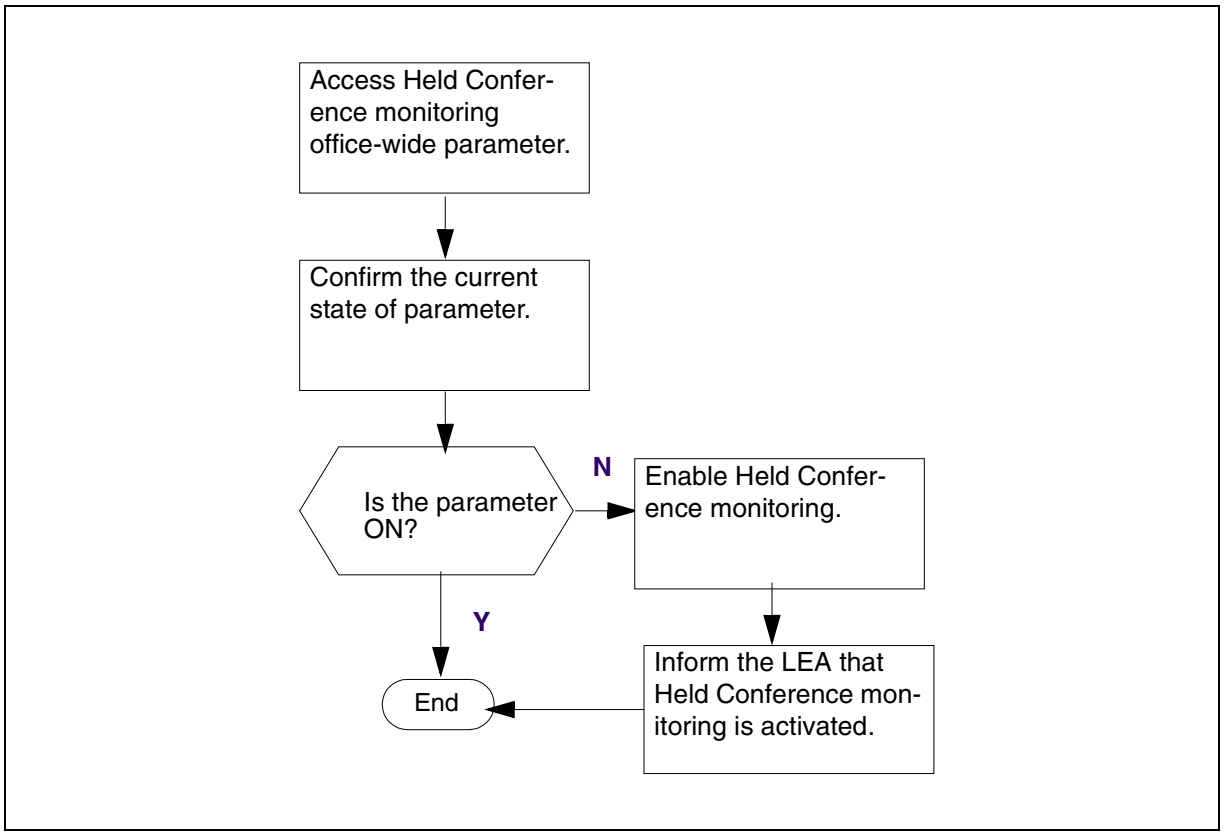
Action

The following sections contain flowchart summaries of the three parts of this procedure. Use the step-action instructions that follow each flowchart to perform the procedure.

Held Conference monitoring

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of setting the HELDMON office-wide parameter



Activate Held Conference monitoring

At the CI level of the MAP

1 From the USNBD prompt level, access the Held Conference monitoring office-wide parameter by typing:

```
unb_ofcwide heldmon
```

and pressing the **Enter** key.

A list of three options is presented: ON, OFF, and STATUS.

2 Confirm the current state of this parameter by typing:

`status`

and pressing the **Enter** key.

The response is either ON or OFF.

3 Refer to the following table to determine the next step.

If the response is	Do
ON	step 6
OFF	step 4

4 Enable Held Conference monitoring by typing:

`unb_ofcwide heldmon on`

and pressing the **Enter** key.

Example Response:

```
HELDMON ON DONE.
```

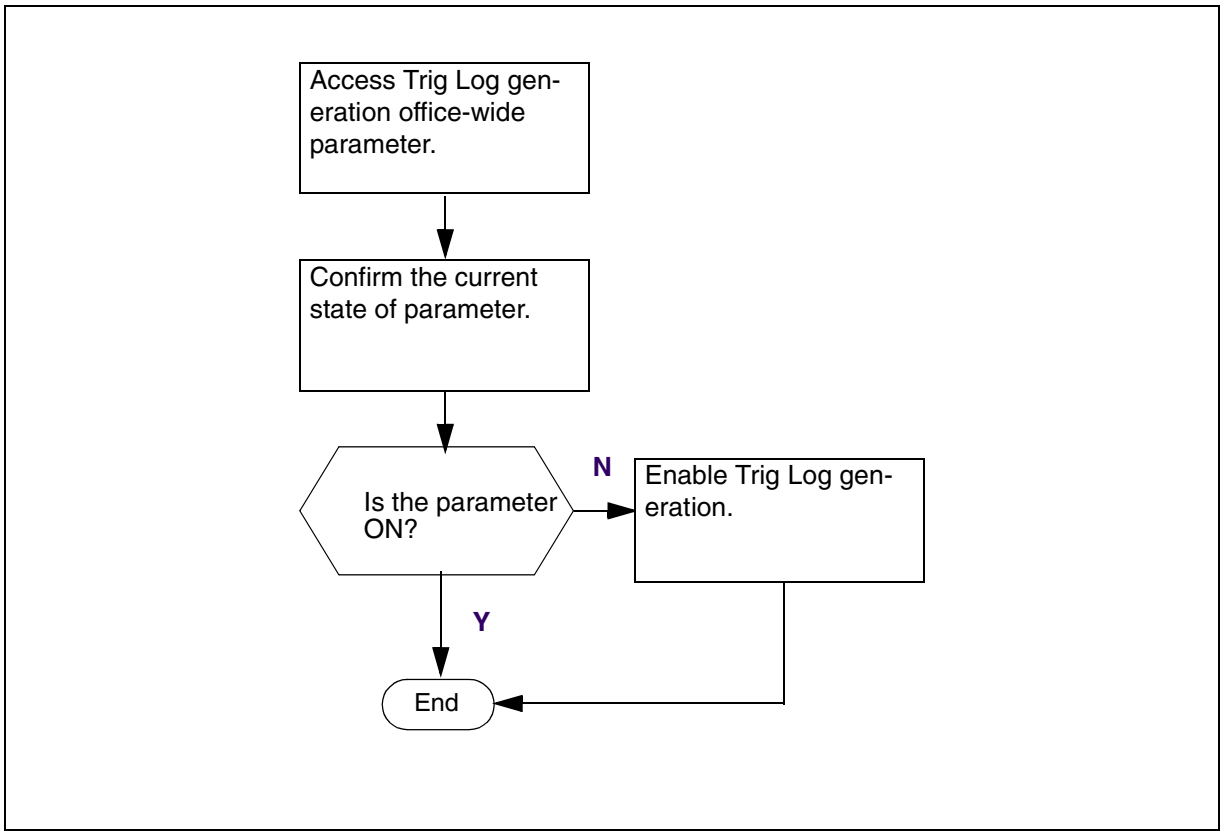
5 Inform the LEA that conference monitoring has been activated.

6 You have completed this procedure.

Trig Log generation

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of setting the TRIG_LOGS office-wide parameter



Activate Trig Log generation

At the CI level of the MAP

1 From the USNBD prompt level, access the Trig Log generation office-wide parameter by typing:

```
unb_ofcwide trig_logs
```

and pressing the **Enter** key.

A list of three options is presented: ON, OFF, and STATUS.

2 Confirm the current state of this parameter by typing:

`status`

and pressing the **Enter** key.

The response is either ON or OFF.

3 Refer to the following table to determine the next step.

If the response is	Do
ON	step 5
OFF	step 4

4 Enable Trig Log generation monitoring by typing:

`unb_ofcwide trig_logs on`

and pressing the **Enter** key.

Example Response:

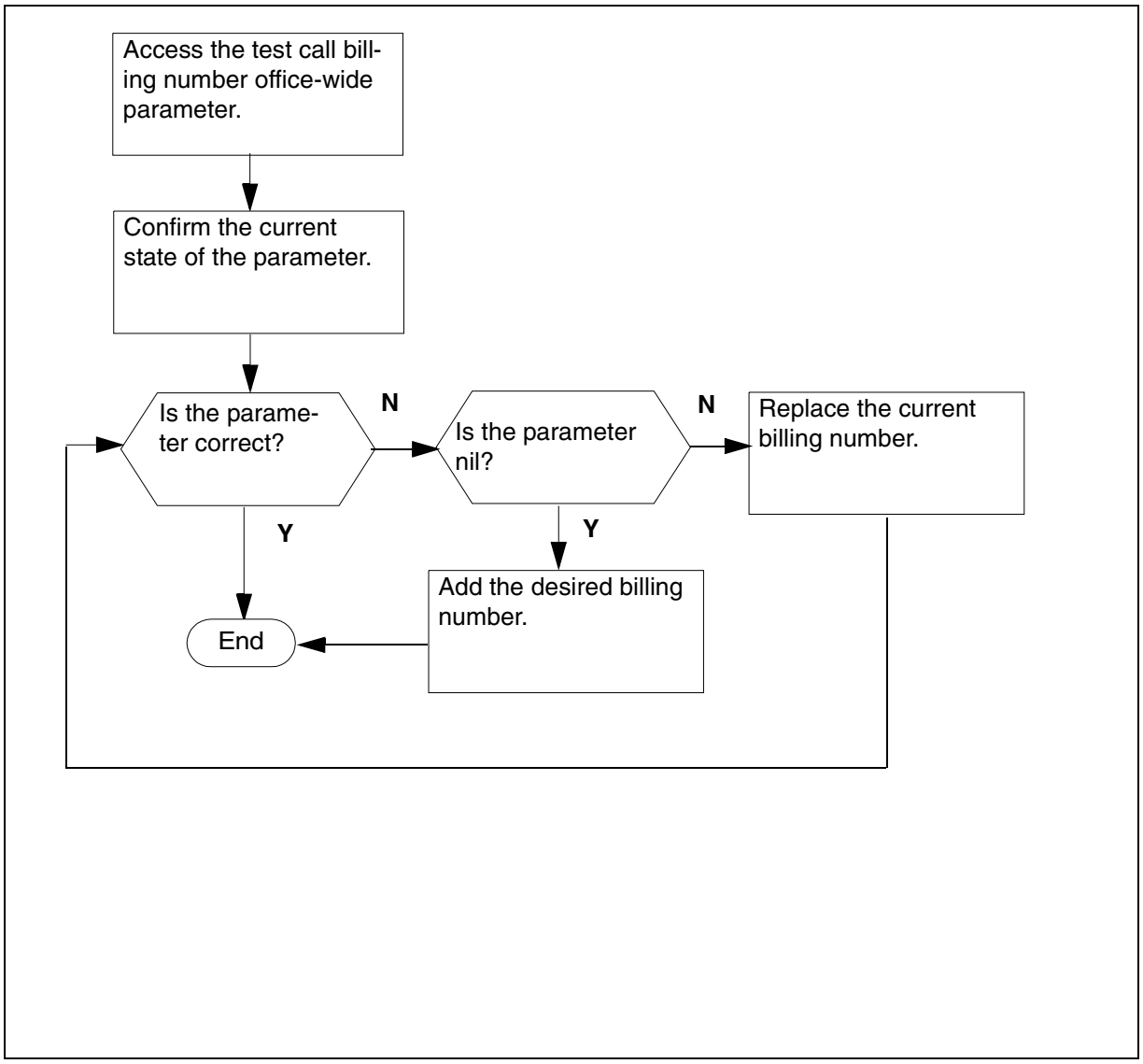
```
TRIG_LOGS ON DONE.
```

5 You have completed this procedure.

Test call billing number

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of setting the TEST_CALL_BILLNO office-wide parameter



Setting the test call billing number

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

usnbd

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Access the test call billing number office-wide parameter by typing:

unb_ofcwide test_call_billno

and pressing the **Enter** key.

A list of options is presented: ADD, REP, DEL, LIST.

3 Confirm the current state of this parameter by typing:

list

and pressing the **Enter** key.

The response is either NIL or a 10-digit DN.

Example
Example response:

```
PARNAME                    PARVAL
-------------------------------------------
TEST_CALL_BILLNO           NIL
TEST_CALL_BILLNO LIST DONE.
```

4 Refer to the following table to determine the next step:

If the response is	Do
NIL	step 5
NOT the desired billing number	step 6
the desired billing number	step 7

5 Add the desired billing number by typing:

unb_ofcwide test_call_billno add <10 digit DN>

and pressing the **Enter** key.

Example
Example response:

```
TEST_CALL_BILLNO ADD DONE.
```

Go to step 7.

6 Replace the desired billing number by typing:

`unb_ofcwide test_call_billno rep <10 digit DN>`

and pressing the **Enter** key.

Example
Example response:

```
TEST_CALL_BILLNO REP DONE.
```

7 You have completed this procedure.

Adding USNBD users

Purpose of this procedure

The purpose of this procedure is to add new USNBD users or administrators. This procedure is performed by a USNBD user with USNBD administrator privileges.

When to use this procedure

Use this procedure when a new USNBD administrator or user needs to be added.

A maximum of 20 USNBD users, including USNBD administrators, can be added. Nortel Networks recommends having at least two USNBD users with administrator privileges at all times.

For additional assistance with the **USER** command, type **user help** at the USNBD: prompt.

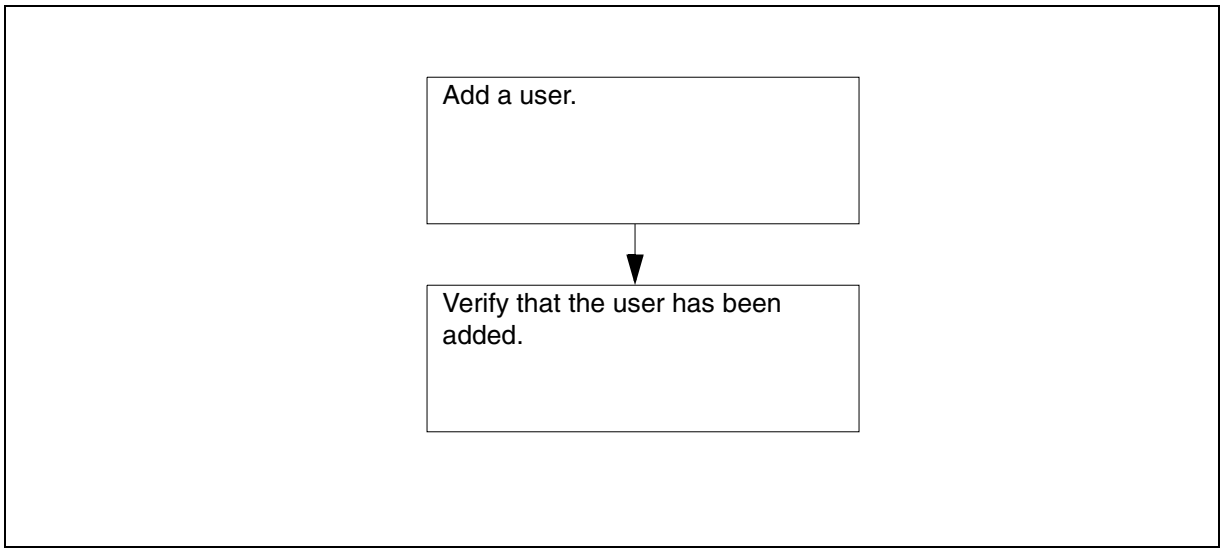
Prerequisites

The administrator or user to be added must have a valid CI user ID.

Actions

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of adding USNBD users



Add USNBD users

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example response:

```
USNBD:
```

At the USNBD level of the MAP

2 Add a user by typing:

`user add <user_id> <admin> <agency>`

and pressing the **Enter** key.

where

where	is
user_id	the user ID of the user to be added
admin	Y to indicate the user has administration privileges, or N to indicate the user does not have administration privileges. This parameter is required.
agency	the agency of the user. This parameter is prompted for only if the added user is not ADMIN, meaning that the admin field is set to N.

Example

`user add user1 n agency1`

Example response:

```
USER ADD DONE:
```

3 Repeat step 2 to add the next user if required.

4 Ensure the users have been added by typing:

`user list`

and pressing the **Enter** key.

Example response:

```
USER   ADMIN AGENCY
-----------------------------
USER1    N      agency1
USER2    Y
USER3    Y
USER LIST DONE.
```

Note: A maximum of 20 USNBD users, including USNBD administrators, can be added.

5 You have completed this procedure.

Adding an agency

Purpose of this procedure

The purpose of this procedure is to add USNBD agency information for those agencies using switched remote access. This procedure is performed by a USNBD user with USNBD administrator privileges.

When to use this procedure

Use this procedure to add agency information to USNBD for agencies using switched remote access. Agency information is required before setting up switched call content resources (CCR).

For additional assistance with the **agency** command, type **agency help** at the USNBD: prompt.

Prerequisites

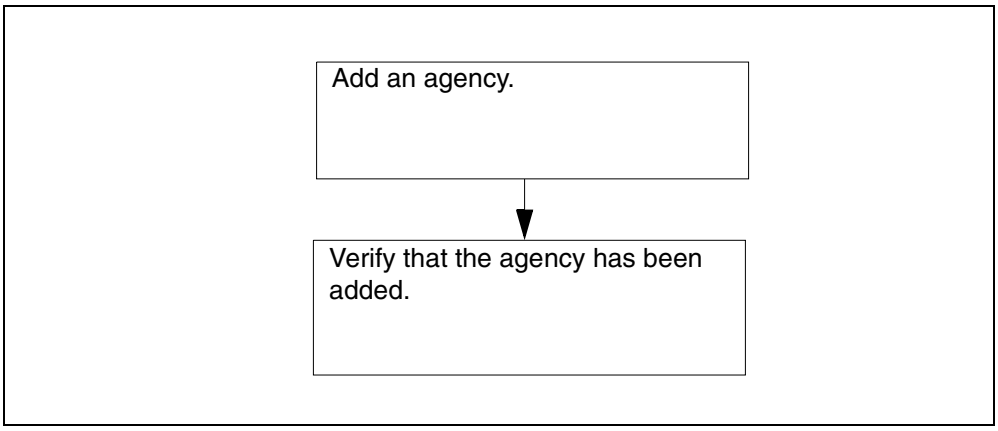
To add an agency, the user must have the following information:

- agency name to be used in USNBD (1 to 16 characters)
- Serving Translation Scheme (STS)
- pretranslator name
- Local Calling Area Screening name (LCA)
- For switched CCCs, or Feature Shift Keying (FSK) switched remote CDCs using Equal Access trunks, the 10-digit billing number that generates billing records for the switched ISUP call content channel (CCC) call pertaining to the specified agency.
- Primary InterLata Carrier (PIC) - used for switched CCRs or FSK SR CDCs using Equal Access dialing
- Local Access and Transport Area (LATA) - used for switched CCRs or FSK SR CDCs using Equal Access dialing

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of adding USNBD agencies



Add an agency

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Add an agency by typing:

`agency add <agency_name> <STS> <pretranslator> <lca> <billno> <PIC> <LATA>`

and pressing the **Enter** key.

where	is
agency_name	the agency having access to switched ISUP CCCs to their remote recording device
STS	the Serving Translation Scheme
pretranslator	the PRETRANSLATOR Name
lca	the local calling area screening name
billno	the 10-digit billing number that generates billing records for the SWITCHED ISUP CCC or FSK SR CDCs call pertaining to the specified agency
PIC	the carrier to be used for switched CCRs or FSK SR CDCs using Equal Access dialing
LATA	the LATA to be used for switched CCRs or FSK SR CDCs using Equal Access dialing

Note: PIC and LATA fields should be NIL (NILC and NILLATA) if Equal Access dialing is not required. A valid PIC and LATA are required if Equal Access dialing is being used.

Example

`agency add agency1 613 p621 1667 1234567890 ITT LATA1`

Example Response:

```
AGENCY ADD DONE:
```

3 Repeat step 2 to add the next agency if required.

4 Ensure the agencies have been added by typing:

`agency list`

and pressing the **Enter** key.

Example Response:

```
AGENCY-NAME       STS PRETRANSLATOR LCANAME BILLNO
                  PIC                 LATA
-------------------------------------------------------
AGENCY1           613 P621            L667    1234567890
                  ITT                 LATA1
AGENCY2           416 P463            L467    0987654321
                  NILC                NILLATA
AGENCY LIST DONE.
```

Note: A maximum of eight USNBD agencies with switched ISUP CCC access can be added.

5 You have completed this procedure.

Creating CCRs

Purpose of this procedure

The purpose of this procedure is to create call content resources (CCR). This procedure is performed by a USNBD user (with or without administrator privileges). A user without administrative rights can only add a CCR for the user's agency.

When to use this procedure

Use this procedure when an LEA requests to have a CCR created.

For additional assistance with the **ccr** command, type **ccr help** at the USNBD: prompt.

Prerequisites

The USNBD user performing this procedure requires the following information:

- the preferred delivery method of the LEA
- the directory number (DN) of each line to be used as a call content channel (CCC) circuit

The USNBD user performing this procedure also must be associated with the same agency as the CCR or have USNBD administrative rights.

Ensure the line(s) to be used as CCC(s) for the CCR exist, and the datafill is correct.

To use a line as a dedicated CCC circuit, the line must have a non-ambiguous, 10-digit DN associated with it. This DN must meet the following requirements:

- must be of type "single party line"

  Note: LI does not support Session Initiation Protocol (SIP) lines as dedicated CCRs. The CCR must use a line with a single party line with 10 digits.

  See feature description LI Support of SIP Lines in chapter Lawful Intercept basics for details.

- must have a line class code (LCC) of 1FR, 1MR, or RES

- only can be assigned the following options:
  - COD
  - DGT
  - NAME
- cannot be assigned any RES options
- can make use of office options, but not all are supported

To use a line as a switched CCC circuit:

- the DN should be *remote* from the host switch
- routing from the host switch must be across an ISUP trunk or an SIP-T trunk

Note: If a *local* DN is used, routing from the host switch must be across an ISUP trunk or an SIP-T trunk.

Verify the line(s) belong to the LEA requesting the creation of the CCR(s).

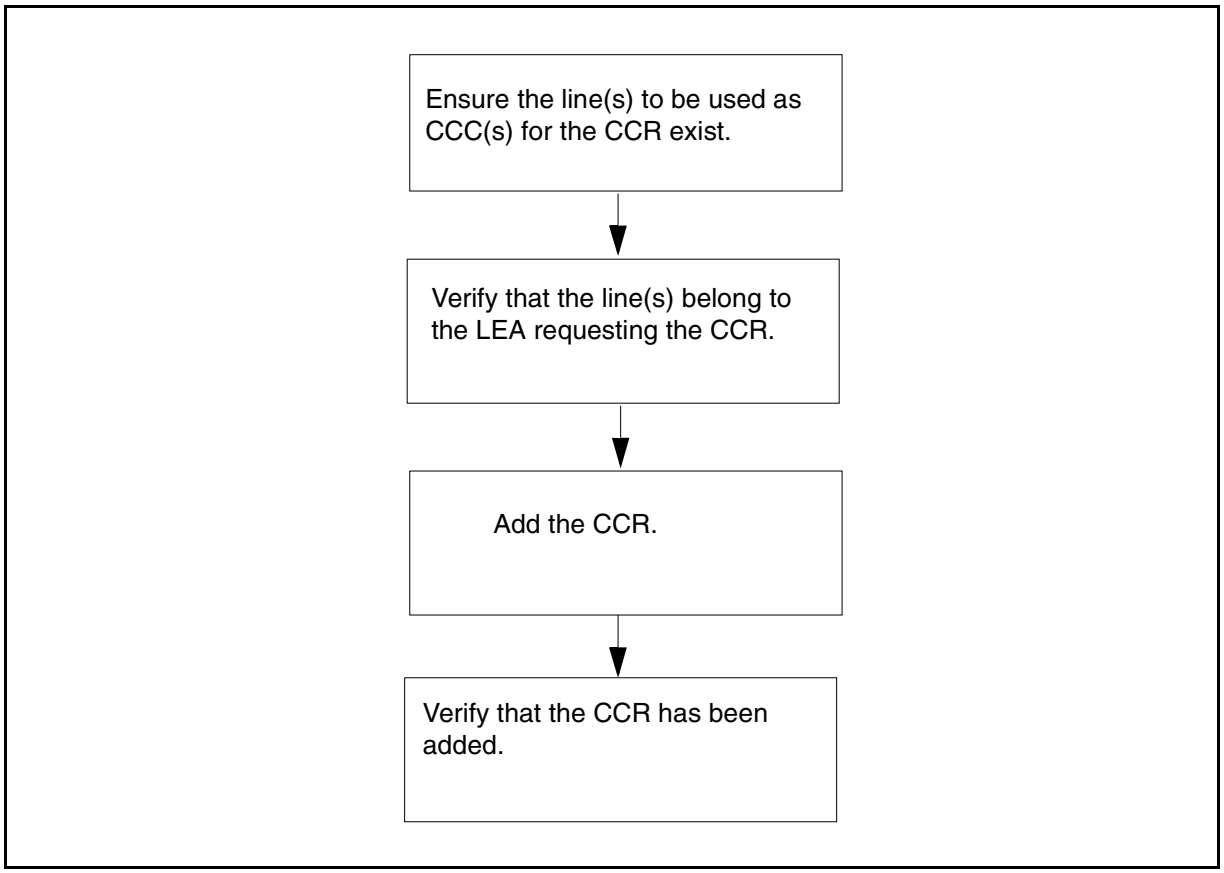
Verify the CCR type selected meets possible data call requirements:

- SW CCRs default to 64K DATA capability. If the terminating lines do not support 64K DATA, the CCRs are set up as speech, unless the monitored call is a 64K DATA call, in which case the CCRs fail.
- SW CCRs over SIP-T default to the same bearer capability as the monitored call. If the terminating lines do not support 64K data, the CCRs fail for any 64K monitored calls.
- SW CCRs use the AGENCY PIC and LATA fields to terminate to SS7 ATC IT type trunks with Equal Access. If the PIC and LATA are set to NILC and NILLATA, SW CCRs can terminate to SS7 IT, TO, or T2 trunks.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of creating CCRs



Create CCRs

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

usnbd

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Display a list of unused CCR index numbers by typing:

```
ccr list free
```

and pressing the **Enter** key.

Example Response:

```
10-500
CCR LIST DONE.
```

3 For administrative users, add the requested CCR by typing:

```
ccr add <index> <ccr_content> <ccr_definition>
<ccr_id> <access> <DN> <DN> <signaling>
<ccc_tag> <agency>
```

and pressing the **Enter** key.

For non-administrative users, add the requested CCR by typing:

```
ccr add <index> <ccr_content> <ccr_definition>
<ccr_id> <access> <DN> <DN> <signaling>
<ccc_tag>
```

and pressing the **Enter** key.

where	is
index	the CCR index number (1 through 500) obtained in step 3 that identifies the CCR
ccr_content	VOICE
ccr_definition	PAIRED, COMBINED
ccr_id	LINE
access	the access type of the CCR. For switched access, type SW. For dedicated access, type DE.
DN	the two 10-digit DNs of the CCC circuits
signaling	Y to indicate signaling is enabled on the CCC(s) or N to indicate signaling is not enabled on the CCC(s). This parameter is inapplicable to SW access CCRs.
ccc_tag	Y to indicate the correlation tag is to be sent. N to indicate the correlation tag is not to be sent. The correlation tag matches the CallID of the CCClose CDC message.
agency	the agency of the CCR. This parameter is prompted only when the user has ADMIN access. When a non-ADMIN user types the command, the user agency is taken as the CCR agency. The user is not prompted for this parameter.

Unsupported CCR parameter values

Parameter	Unsupported value
ccr_content	packet
ccr_id	trunk

Example
Administrative user

```
ccr add 10 voice paired line de 4188326520
4183427653 Y N agency2
```

Example
Non-administrative user

```
ccr add 11 voice paired line de 4188326520
4183427653 Y N
```

Example Response:

```
CCR ADD DONE.
```

4 If a switched CCR is used, perform a test using the TEST command:

- For lines over a SIP-T trunk, the translations are verified.
- For lines over an ISUP trunk, the translations are verified and signalling messages are sent to make the phones ring.
- If the lines cannot support 64K data, a warning is displayed.

```
>ccr list all
```

Example Response:

```
150 VOICE PAIRED LINE SW 14164631621
14164631321 N N NIL
CCR LIST DONE.
```

>test ccr 150

Example Response 1:

```
SUCCESSFUL TEST CALL FOR CCC DN 14164631621.
SUCCESSFUL TEST CALL FOR CCC DN 14164631321.
```

Example Response 2:

```
SUCCESSFUL TEST CALL FOR CCC DN 14164631621.
WARNING: CCR DOES NOT SUPPORT 64K.
RECOMMENDED FOR MONITORING SPEECH ONLY CALLS.
SUCCESSFUL TEST CALL FOR CCC DN 14164631321.
WARNING: CCR DOES NOT SUPPORT 64K.
RECOMMENDED FOR MONITORING SPEECH ONLY CALLS.
```

Note: If the test call terminates to lines capable of 64K data, response 1 will be generated. Otherwise, response 2 will be generated. Verify the capability of the CCR is what Law Enforcement expects it to be.

> ccr list all

Example Response:

```
28 VOICE PAIRED LINE SW 16009632281
16009632282 N N NIL      CCR LIST DONE.
```

test ccr 28

Example Response:

```
NOTE: ONLY TRANSLATIONS AND ROUTING TESTED DUE
TO TEST CALL CANNOT BE DONE WHEN ROUTING OUT
OVER A DPT TRUNK.
SUCCESSFUL TEST CALL FOR CCC DN 16009632281.
NOTE: ONLY TRANSLATIONS AND ROUTING TESTED DUE
TO TEST CALL CANNOT BE DONE WHEN ROUTING OVER A
DPT TRUNK.
SUCCESSFUL TEST CALL FOR CCC DN 16009632282.
TEST CALL DONE.
```

Once a CCR has been added, it can be associated with a surveillance. See procedure “Associating a CCR with a surveillance.”

5 You have completed this procedure.

Creating a CDC

Purpose of this procedure

The purpose of this procedure is to add a call data channel (CDC). This procedure is performed by a USNBD user (with or without administrator privileges). A user without administrative rights can only add a CDC for the user's agency.

When to use this procedure

Use this procedure when a CDC is required to deliver monitoring information to the law enforcement agencies (LEA).

For additional assistance with the **cdc** command, type **cdc help** at the USNBD: prompt.

Prerequisites

The USNBD user performing this procedure requires the following information:

- the index number of the multiprocessor controller card (MPC) or enhanced MPC (EMPC) from table MPC
- the MPC link number from table MPCLINK
- if using X.25 links for CDCs, the address and protocol of the X.25 node. X.25 is not supported for 3PC platform; see section "Executing pre-provisioning requirements for USNBD"
- if using SCTP/IP (simple control transfer protocol over internet protocol) links for CDCs, the IP address and port address of the SCTP/IP link
- if using Frequency Shift Keying (FSK) links for CDCs, the access type (Switched Remote [SR], Switched Local [SL] or Dedicated [DE]) and the 10-digit directory number

  Note: A TDM or a hybrid configuration (that is, both TDM and IP/ATM fabrics residing on the same switch) supports access type SR for FSK CDC links. However, the configuration must have one in-service CMR card hosted in the same XPM.

The USNBD user performing this procedure must also be associated with the same agency as the CDC will be or have USNBD administrative rights.

To use a line as an FSK SL or DE CDC circuit, the line must have a non-ambiguous, 10-digit DN associated with it. The DN must meet the following requirements:

- must be of type “single party line”
- must have line class code (LCC) of 1FR, 1MR, or RES
- can be assigned only the following options:
  - COD
  - DGT
  - NAME
- cannot be assigned any RES options
- can make use of any office options
- must have an in-service CMR card hosted in the same XPM

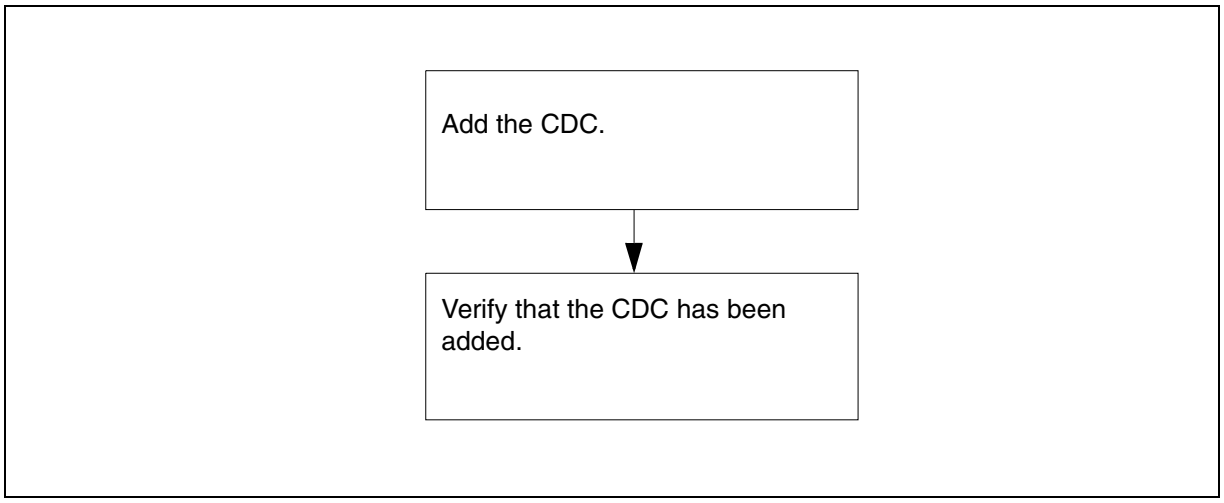
To create an FSK SR CDC circuit, the following requirements must be met:

- The 10- or 11-digit string must terminate to an SS7 trunk of the following types:
  - ATC with EA dialing
  - IT with or without EA dialing
  - TO
  - T2
- The 10- or 11-digit string must not reside on the same switch as the surveillance.
- There must be at least one LGC/LTC XPM (running QLI17AY1 load or higher) with an inservice CMR card.
- The terminating line (which is connected to the modem and PC performing the decoding of the CDC messages) must have a cutoff or disconnect feature (COD for Nortel equipment), which will allow the line to be idled if the trunk is released. Otherwise, the modem will remain offhook, putting the line in a busy or lockout state, which will require manually releasing the modem.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of creating a CDC



Create a CDC

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Ensure the link to be used as a CDC exists and the datafill is correct.

3 Display a list of unused CDC index numbers by typing:

`cdc list free`

and pressing the **Enter** key.

Example Response:

```
1-200
CDC LIST DONE.
```

4 Refer to the following table to determine your next step:

If	Do
you are configuring your CDCs to communicate with the LEA using SCTP/IP association	step 5
you are configuring your CDCs to communicate with the LEA using X.25 links	step 7
you are configuring your CDCs to communicate with the LEA using FSK over local lines or trunks	step 9

Note: FSK CDCs are available only if SOC NBD00004 has been activated.

5 For administrative users, add the requested CDC by typing:

```
cdc add <CDCindex> IP <ip1> <ip2> <ip3> <ip4>
<port> <agency>
```

and pressing the **Enter** key.

For non-administrative users, add the requested CDC by typing:

```
cdc add <CDCindex> IP <ip1> <ip2> <ip3> <ip4>
<port>
```

and pressing the **Enter** key.

(Sheet 1 of 2)

where	is
CDCindex	the CDC index number (1 through 200) obtained in step 2 that identifies the CDC
IP	indicates that the CDC is using SCTP/IP association for its connection
IP1, IP2, IP3, IP4	the first, second, third and fourth address block of an IP subnet address, separated by spaces
port	the port address (1025 to 65534)

(Sheet 2 of 2)

where	is
agency	the agency of the CDC. This parameter is prompted for only when the user executing the command has ADMIN access. When a non-ADMIN user types the command, the user agency is taken as the CDC agency. The user is not prompted for this parameter.

Example
Example for an administrative user:

```
cdc add 1 IP 10 56 16 32 12347 agency1
```

Example
Example response for a non-administrative user:

```
cdc add 1 IP 10 56 16 32 12347
```

Example Response:

```
CDC ADD DONE.
```

6 Go to step 13.

7 For administrative users, add the requested CDC by typing:

```
cdc add <CDCindex> X25 <MPCIndex>
<MPCLinkNumber> <address> <protocol1>
<protocol2> <protocol3> <protocol4> <agency>
```

and pressing the **Enter** key.

For non-administrative users, add the requested CDC by typing:

```
cdc add <CDCindex> X25 <MPCIndex>
<MPCLinkNumber> <address> <protocol1>
<protocol2> <protocol3> <protocol4>
```

and pressing the **Enter** key.

(Sheet 1 of 2)

where	is
CDCindex	the CDC index number (1 through 200) obtained in step 2 that identifies the CDC
X25	indicates that the CDC is using an X.25 link for its connection

(Sheet 2 of 2)

MPCIndex	the index number of the EMPC or MPC card specified in table MPC
MPCLinkNumber	the number of the MPC link specified in table MPCLINK
protocol1, protocol2, protocol3, protocol4	the protocol to use for the CDC
agency	the agency of the CDC. This parameter is prompted for only when the user executing the command has ADMIN access. When a non-ADMIN user types the command, the user agency is taken as the CDC agency and the user is not prompted for this parameter.

Example
Example for an administrative user:

```
cdc add 1 X25 0 3 11111111 3 1 128 0 agency1
```

Example
Example response for a non-administrative user:

```
cdc add 1 X25 7 2 22222222 3 1 128 0
```

Example Response:

```
CDC ADD DONE.
```

8 Go to step 13.

9 Ensure the line to be used as the FSK SL or DE CDC exists and the datafill is correct. If you are creating an FSK SR CDC, ensure the translations are set up to correctly terminate to a trunk. See the “Prerequisites” section of this document.

10 For administrative users, add the requested CDC by typing:

```
cdc add <CDCindex> FSK <access> <10-digit-dn>
<agency>
```

and pressing the **Enter** key.

For non-administrative users, add the requested CDC by typing:

```
cdc add <CDCindex> FSK <access> <10-digit-dn>
```

and pressing the **Enter** key.

where	is
CDCindex	the CDC index number (1 through 200) obtained in step 2 that identifies the CDC
FSK	indicates the CDC is using an FSK association for its connection
access	the type of access the LEA requires for its FSK CDC, switched remote (SR), switched local (SL), or dedicated (DE)
DN	the 10-digit DN of the FSK SL/DE CDC circuit. For FSK SRs, a 10- or 11-digit string translating to a trunk.
agency	the agency of the CDC. This parameter is prompted for only when the user executing the command has ADMIN access. When a non-ADMIN user types the command, the user agency is taken as the CDC agency and the user is not prompted for this parameter.

Example
Example response for an administrative user:

```
cdc add 1 FSK DE 9197633101 agency1
cdc add 2 FSK SL 9199763000 agency2
cdc add 3 FSK SR 13458881212 agency3
```

Example
Example response for a non-administrative user:

```
cdc add 1 FSK DE 9197633101
cdc add 2 FSK SL 9199763000
cdc add 3 FSK SR 13458881212
```

Example Response:

```
CDC ADD DONE.
```

11 Use the USNBD test command to verify a call can be made to the SL or SR CDC prior to association to a surveillance by typing:

```
cdc list all
```

and pressing the **Enter** key.

Example
Example response for an administrative user:

```
cdc add 1 FSK DE 9197633101 agency1
cdc add 2 FSK SL 9199763000 agency2
cdc add 3 FSK SR 13458881212 agency3
```

Example
Example response for a non-administrative user:

```
cdc add 1 FSK DE 9197633101
cdc add 2 FSK SL 9199763000
cdc add 3 FSK SR 13458881212
```

12 Type:

```
test cdc 2 or test cdc 3
```

and press the **Enter** key.

Example
Example response:

```
SUCCESSFUL TEST CALL FOR CDC DN 9197631234
SUCCESSFUL TEST CALL FOR CDC DN 13458881212
```

13 You have completed this procedure.

Listing a surveillance

Purpose of this procedure

The purpose of this procedure is to list a surveillance on a subject.

When to use this procedure

Use this procedure to list all datafilled surveillance orders.

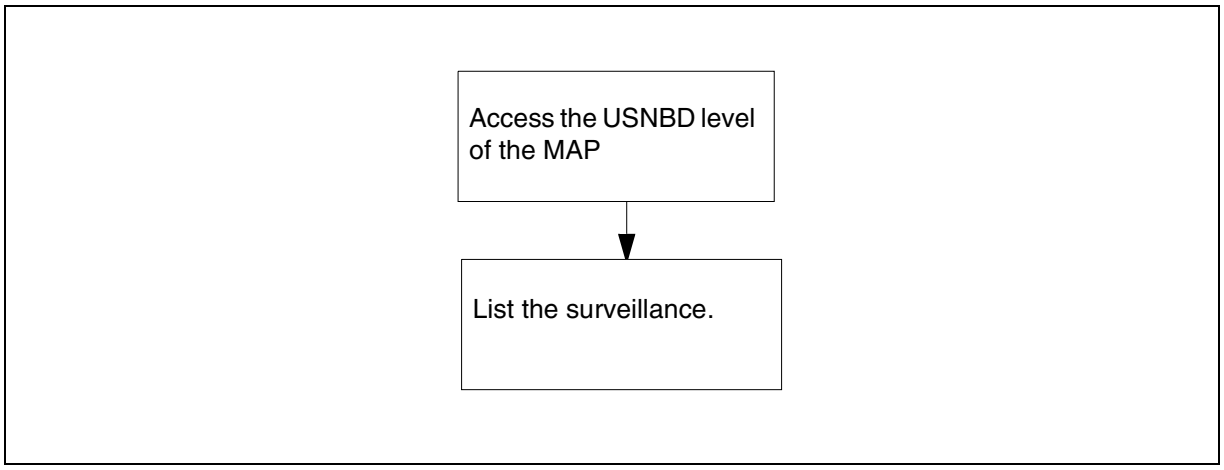
Prerequisites

There are no prerequisites for this procedure.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of listing a surveillance



List a surveillance

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
usnbd
```

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Using the appropriate LIST command parameter, list the monitoring orders by typing:

```
surv list {ALL, ACT, INACT, SIN, DN, KEY, LEN,
LTID, PNI, AGENCY}
```

and pressing the **Enter** key.

where	is
<LIST>	to list a surveillance on a subject
Parameters and variables	description
ALL	to display all provisioned surveillance orders
ACT	to display activated surveillance order only
INACT	to display all the surveillances that are deactivated
SIN	to display the surveillance with the specified surveillance identification number (SIN)
DN	to display the surveillance on the specified directory number (DN)
KEY	to display the surveillance on the specified key
LEN	to display the surveillance on the specified line equipment number (LEN)
LTID	to display the surveillance on the specified LTID
PNI	to indicate whether Private Network Interception (PNI) is activated or deactivated.
agency	the agency of the user

Example

To list the specific monitoring order of SIN "SIN_SUBJECTC" type the following:

surv list sin SIN_SUBJECTC

Example response:

```
Subject          CaseID SIN MRP Clg_dlvry Inband_dlvry
                (Feat_status Interval) (Surv_status Interval) PNI Agency
                 Status {Associated_CDC} {Associated_CCRs}
-------------------------------------------------------------------------
DN 6043210281    CASEID_AUTO SIN_SUBJECTC Y Y N
                 (N 0) (N 0) N AUTO_AGENCY
                 ACTIVE { 42 } { 442 }
```

3 You have completed this procedure.

Adding a surveillance

Purpose of this procedure

The purpose of this procedure is to add a surveillance on a subject.

When to use this procedure

Use this procedure when an LEA requests to have a surveillance set up on a subject.

For additional assistance with the **surv** command, type **surv help** at the USNBD: prompt.

Prerequisites

The USNBD user performing this procedure requires the following information:

- the directory number (DN), line equipment number (LEN), KEY, or logical terminal ID (LTID) of the subject to be monitored
- the case ID of the surveillance provided by the LEA
- the surveillance identification number (SIN) for the surveillance
- an indication on whether a monitored replacement party (MRP) can be provided for a monitored call
- an indication of whether in-band digits should be delivered for a monitored call
- an indication of whether the feature status message should be delivered and how often
- an indication of whether the surveillance status should be delivered and how often
- an indication of whether Private Network Interception (PNI) is activated or deactivated

The USNBD user performing this procedure also must be associated with the same agency as the surveillance will be or have USNBD administrative rights.

Additional information

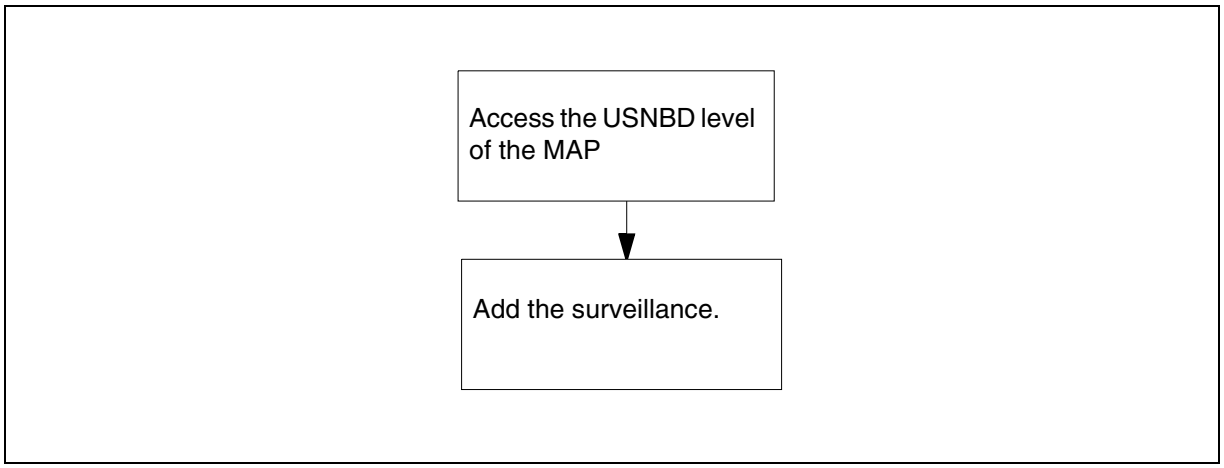
Surveillances on Session Initiation Protocol (SIP) lines are provisioned against the line DN. When the surveillance is activated, multiple calls originating and terminating on the target are monitored.

See feature description LI Support of SIP Lines in chapter Lawful Intercept basics for details.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of adding a surveillance



Add a surveillance

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 For administrative users, add the requested surveillance by typing:

`surv add <handle> <caseid> <SIN> <MRP> <calling_party_num_delivery> <inband_delivery> <feature_status_periodic> <surveillance_status_periodic> <PNI> <agency>`

and pressing the **Enter** key.

For non-administrative users, add the requested surveillance by typing:

```
surv add <handle> <caseid> <SIN> <MRP>
<calling_party_num_delivery> <inband_delivery>
<feature_status_periodic>
<surveillance_status_periodic> <PNI>
```

and pressing the **Enter** key.

(Sheet 1 of 2)

where	is
handle	one of the following: • DN with <subject_dn> • LEN with <subject_len> • KEY with <subject_key> • LTID with <subject_ltid>
case_id	the identification of the surveillance provided by the LEA (1 through 16 alphanumeric characters)
sin	the surveillance identification number, which uniquely identifies the surveillance (1 through 25 alphanumeric characters)
mrp	Y or N to indicate whether an MRP can be provided for a monitored call
calling_party_ num_delivery	Y or N to indicate whether the calling party DN can be delivered to the LEA
inband_delivery	Y or N to indicate whether digits captured inband should be delivered to the LEA through a CDC link ***Note:*** If the surveillance has inband_dlvry set to Y, then CDC monitoring is required.
feature_status_ periodic	Y or N to indicate whether a feature status periodic message should be generated for the surveillance
feature_status_ interval	a time parameter in minutes (15 to 1440 in increments of 15) to indicate the amount of time between periodic messages
surveillance_ status_periodic	Y or N to indicate whether a surveillance status periodic message should be generated for the surveillance
surveillance_ status_interval	a time parameter in minutes (60 to 1440 in increments of 15) to indicate the amount of time between periodic messages

(Sheet 2 of 2)

where	is
<PNI>	Y or N to indicate whether Private Network Interception (PNI) is activated or deactivated. <BOOLEAN> (Y,N) If the boolean is set to “Y,” call content and in-band digits of private network calls can be intercepted. If the boolean is set to “N,” call content and in-band digits of private network calls cannot be intercepted. ***Note:*** In-band digits are affected only if in-band digit collection is enabled and a CDC has been provisioned.
agency	the agency of the surveillance. This parameter is prompted for only when the user executing the command has ADMIN access. When a non-ADMIN user types the SURV ADD command, the user agency is taken as the surveillance agency and the user is not prompted for this parameter.

Example
(for administrative users)

```
surv add dn 6137213456 case1 sin1 y n n n n
agency1
```

Example
(for non-administrative users)

```
surv add dn 6137213456 case1 sin1 y n n n n
```

Example Response:

```
SURV ADD DONE.
```

3 You have completed this procedure.

Associating a CDC with a surveillance

Purpose of this procedure

The purpose of this procedure is to associate the requested call data channel (CDC) with the surveillance if monitoring information is required for the surveillance. (If the requested CDC is not already created, refer to procedure Creating a CDC.)

When to use this procedure

Use this procedure when a law enforcement agency (LEA) requests to set up a surveillance on a subject.

For additional assistance with the **cdc** command, type **cdc help** at the USNBD: prompt.

Prerequisites

The USNBD user performing this procedure requires the following information:

- the index number of the CDC to be associated with the surveillance if the a CDC is required.
- monitoring information, if required

> ***Note:*** If the surveillance has Inband_dlvry set to Y, then CDC monitoring is required.

The CDC and the surveillance must have the same agency to be associated.

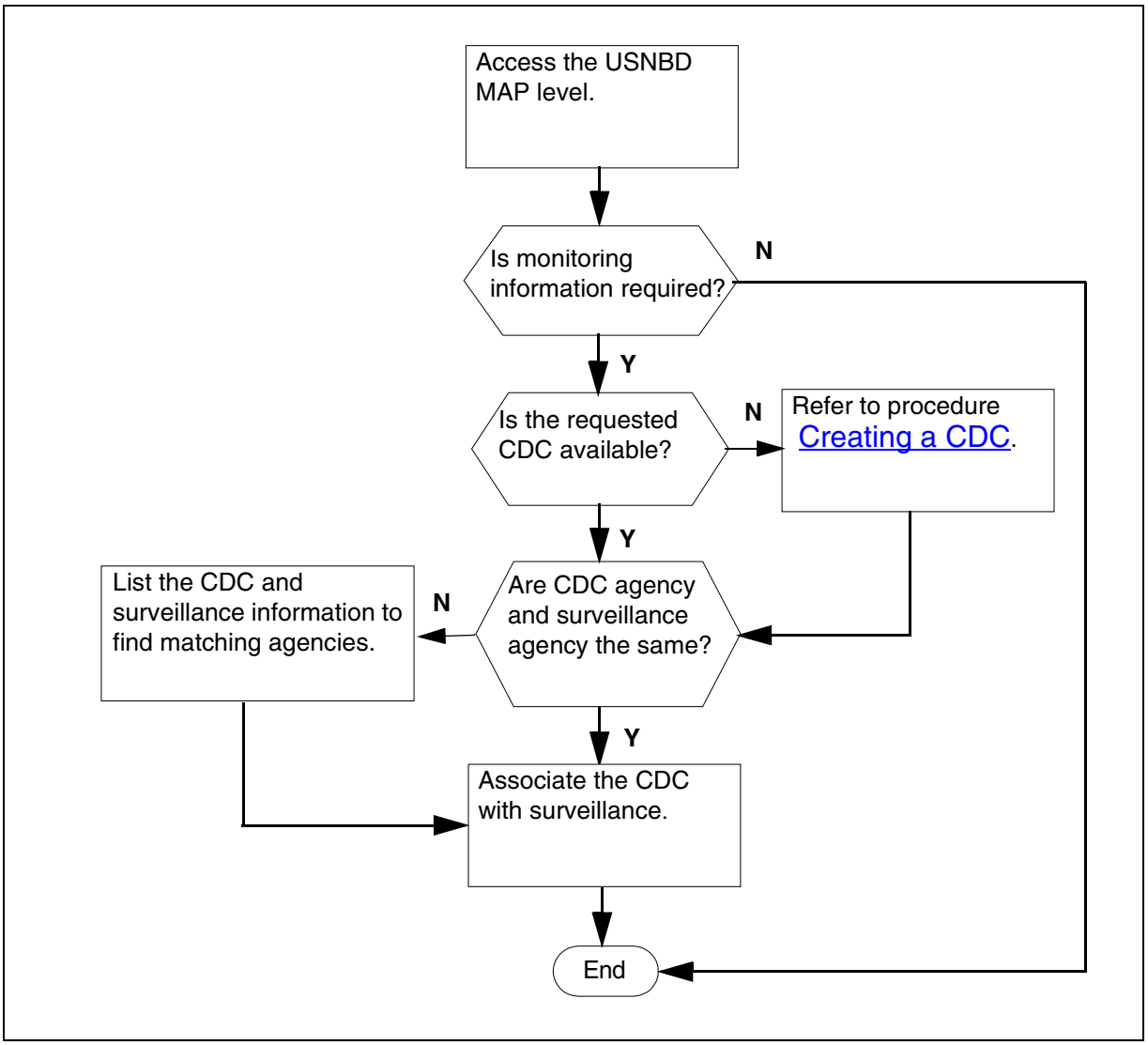
The USNBD user performing this procedure also must be associated with the same agency as the CDC or have USNBD administrative rights.

Agency data must be datafilled before Switched Remote FSK CDCs can be associated to a surveillance.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of Associating a CDC with a surveillance



Associate a CDC with a surveillance

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

usnbd

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

2 Use the following table to determine your next step:

the LEA	go to
requires monitoring information for the surveillance	step 3
does not require monitoring information for the surveillance	step 6

At the USNBD level of the MAP

3 Display a list of CDCs to determine whether the requested CDC is available for the surveillance. If the user does not have administrative rights, only CDCs for the user's agency are shown. If the user has administrative rights, agency information is shown for all CDCs. Display the list by typing:

`cdc list all`

and pressing the **Enter** key.

Example Response:

```
Index Type  MPClink Address      Protocol     Agency
      [Associated SINs]
------------------------------------------------------------
   2 X25   1 3 12345          2   2   2   2   AGENCY3
Index Type  IP Address     IP Port       Agency
      [Associated SINs]
------------------------------------------------------------
   1 IP  10  66  34  16    12347         AGENCY1
CDC LIST DONE.
```

Note: Look for the requested CDC using its index number. In the example above, the index number of the IP CDC is 1.

the requested CDC is	go to
not available	step 3
available	step 4

4 Create the requested CDC using procedure Creating a CDC. Then return to step 4 in this procedure.

5 Associate the requested CDC with the surveillance by typing:

`cdc assoc <index> <sin>`

and pressing the **Enter** key.

where	is
index	the index number (1 through 200) of the CDC to be associated with the surveillance
sin	the surveillance identification number of the surveillance to which the CDC is being associated

Note: Different surveillances for the same LEA can share the same CDC.

Once a CDC is associated with the first surveillance for an LEA, a switched virtual circuit (SVC) is created. All monitoring information for the surveillances with which the CDC is associated, is delivered to the LEA using the CDC over a point-to-point facility.

Example

```
cdc assoc 1 sin1
```

and pressing the **Enter** key.

```
CDC ASSOC DONE.
```

6 You have completed this procedure.

Associating a CCR with a surveillance

Purpose of this procedure

The purpose of this procedure is to associate the requested call content resources (CCR) with the surveillance if call content is required for the surveillance.

When to use this procedure

Use this procedure when a law enforcement agency (LEA) requests to set up a surveillance on a subject.

For additional assistance with the **ccr** command, type **ccr help** at the USNBD: prompt.

Prerequisites

The USNBD user performing this procedure must know if call content delivery is required.

The CCR and the surveillance must have the same agency to be associated.

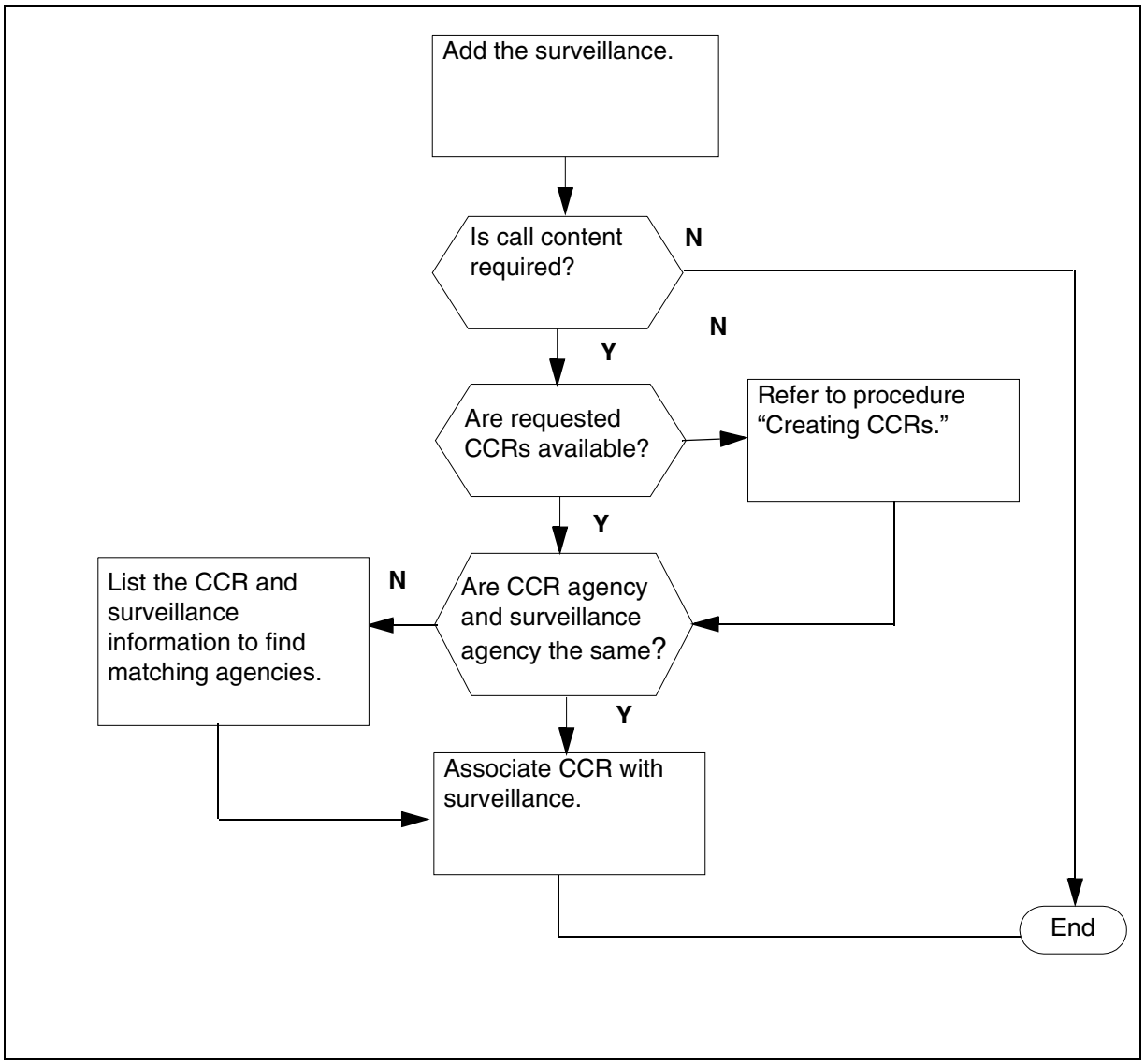
The USNBD user performing this procedure also must be associated with the same agency as the CCR or have USNBD administrative rights.

Agency data must be datafilled before switched ISUP call content channels (CCC) can be associated to a surveillance.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of associating a CCR with a surveillance



Associate a CCR with a surveillance

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Determine if call content delivery is required.

If call content is:	Do
not required	step 7
required	step 3

3 Display a list of CCRs to determine whether the requested CCR(s) are available for the surveillance by typing:

`ccr list all`

and pressing the **Enter** key.

Example response for an administrative user:

```
Index Content CCRtype  Acc CCRid CCC1  [CCC2]
[Sig] [Tag]       [SIN] [Agency]
-------------------------------------------------------
1 VOICE   PAIRED  LINE  SW 19006671021 19006671024
N     N                          AGENCY3
2 VOICE   PAIRED  LINE  DE 6136631001 6136631234
N     N                          AGENCY1

CCR LIST DONE
```

Note 1: An administrative user sees CCR information for all agencies.

Note 2: A non-administrative user sees information only for those CCRs associated with the user's agency.

4 Look for the requested CCR(s) using their index number. (In the previous example, the index number of the CCR is 2.)

If the CCRs are	Do
not available	step 5
available	step 6

5 Create one or more CCRs using procedure Creating CCRs, then return to step 4 in this procedure.

6 Associate the requested CCR(s) with the surveillance by typing:

`ccr assoc <index> <sin>`

and pressing the **Enter** key.

where **index** is the index number (1 through 500) of the CCR to be associated with the surveillance and **sin** is the surveillance identification number of the surveillance to which the CCR is being associated

Example
ccr assoc 2 sin1

Example Response:

CCR ASSOC DONE.

Once the CCR ASSOC command is entered for dedicated CCRs, a call is made to the CCC circuit(s) using standard translations and routing. If the signalling parameter for the CCRs was set to 'Y' in the CCR ADD command, phone sets ring if they are at the end of the CCC circuit(s). If the signalling parameter is set to 'N,' the CCC phones do not ring.

When call setup is complete (for example, if phone sets at the end of the CCC are answered), C-tone is applied on the CCC circuit(s).

Note: When one of the CCCs of a separated CCR cannot be established, the CCR is not associated.

Each call to a CCC requires one USNBD extension block. If no extension block is available, CCR association fails. The EXTOVFL register of key FBSEXT in the EXT operational measurement (OM) group increments.

7 You have completed this procedure.

Activating a surveillance

Purpose of this procedure

The purpose of this procedure is to activate a surveillance on a subject. This procedure is performed by a USNBD user (with or without administrator privileges).

When to use this procedure

Use this procedure when a law enforcement agency (LEA) requests that a surveillance be activated on a subject.

For additional assistance with the **surv** command, type **surv help** at the USNBD: prompt.

Prerequisites

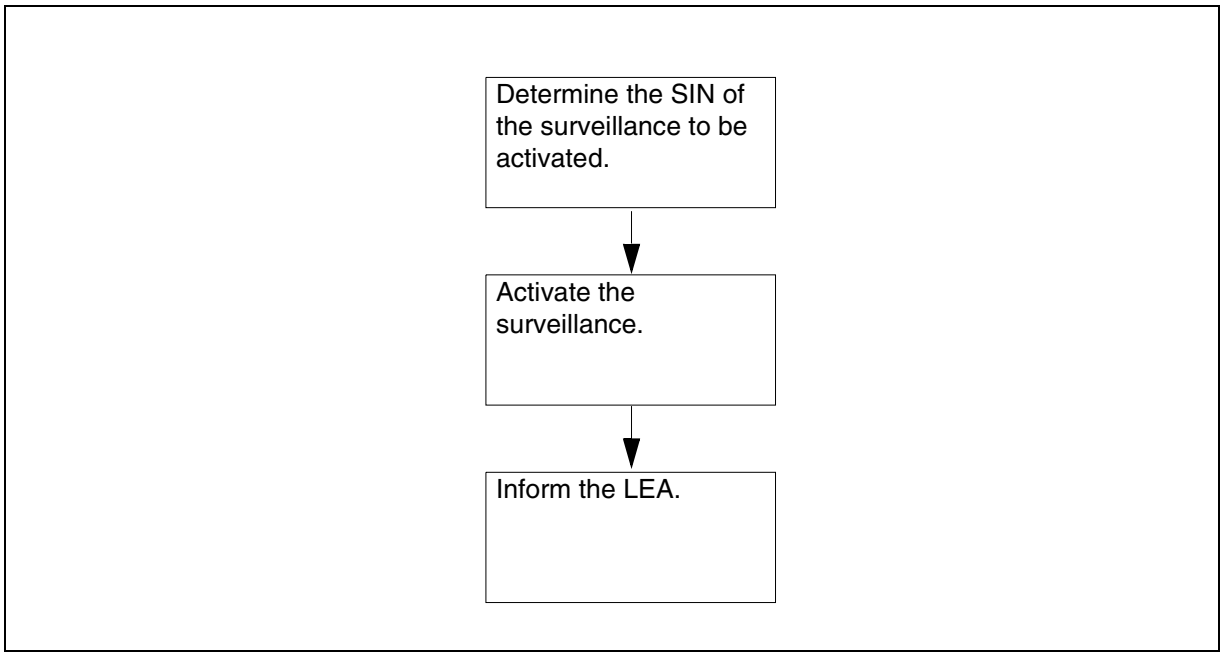
The USNBD user performing this procedure requires the surveillance identification number (SIN) of the surveillance to be activated.

The USNBD user performing this procedure must be associated with the same agency as the surveillance, and have USNBD administrative rights.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of activating a surveillance



Activate surveillance

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

usnbd

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2

CAUTION

Risk of service disruption

If any of the settings of office parameter RES_SO_SIMPLIFICATION are changed during a surveillance, the surveillance of a subject can be disconnected.

Activate the surveillance by typing:

```
surv act <sin>
```

and pressing the **Enter** key.

where **sin** is the surveillance identification number of the surveillance to be activated

Example
surv act sin1

Example Response:

```
SURV ACT DONE.
```

Once a surveillance is active, calls made or received by the subject are monitored, provided the type of call is capable of being monitored.

3 Inform the LEA that the surveillance has been activated.

4 You have completed this procedure.

Deactivating a surveillance

Purpose of this procedure

The purpose of this procedure is to deactivate a surveillance. This procedure is performed by a USNBD user (with or without administrator privileges).

When to use this procedure

Use this procedure when a law enforcement agency (LEA) requests that a surveillance on a subject be deactivated.

For additional assistance with the **surv** command, type **surv help** at the USNBD: prompt.

Prerequisites

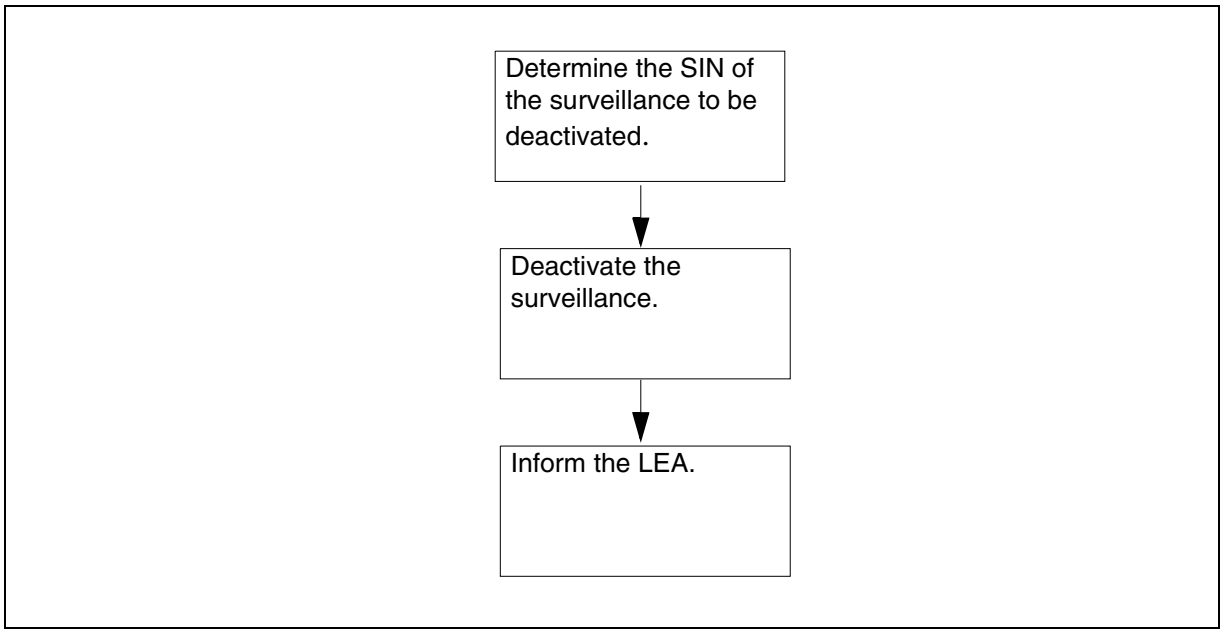
The USNBD user performing this procedure requires the case ID of the surveillance to be deactivated.

The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of deactivating a surveillance



Deactivate surveillance

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Deactivate the surveillance by typing:

```
surv deact <sin>
```

and pressing the **Enter** key.

where **sin** is the surveillance identification number of the surveillance to be deactivated

Example
surv deact sin1

Example Response:

```
SURV DEACT DONE.
```

Note: If a surveillance is deactivated while calls to or from the subject are in progress and being monitored, monitoring on those calls stops immediately.

3 Inform the LEA that the surveillance has been deactivated.

4 You have completed this procedure.

Taking down a surveillance

Purpose of this procedure

The purpose of this procedure is to take down a surveillance. This procedure is performed by a USNBD user (with or without administrator privileges) and includes

- disassociating any call content resources (CCRs) from the surveillance
- disassociating the call data channel (CDC) from the surveillance if any
- deleting the surveillance

When to use this procedure

Use this procedure when a law enforcement agency (LEA) requests that a surveillance on a subject be taken down.

Prerequisites

The surveillance must first be deactivated using the “Deactivating a surveillance” procedure.

The USNBD user performing this procedure requires the following information:

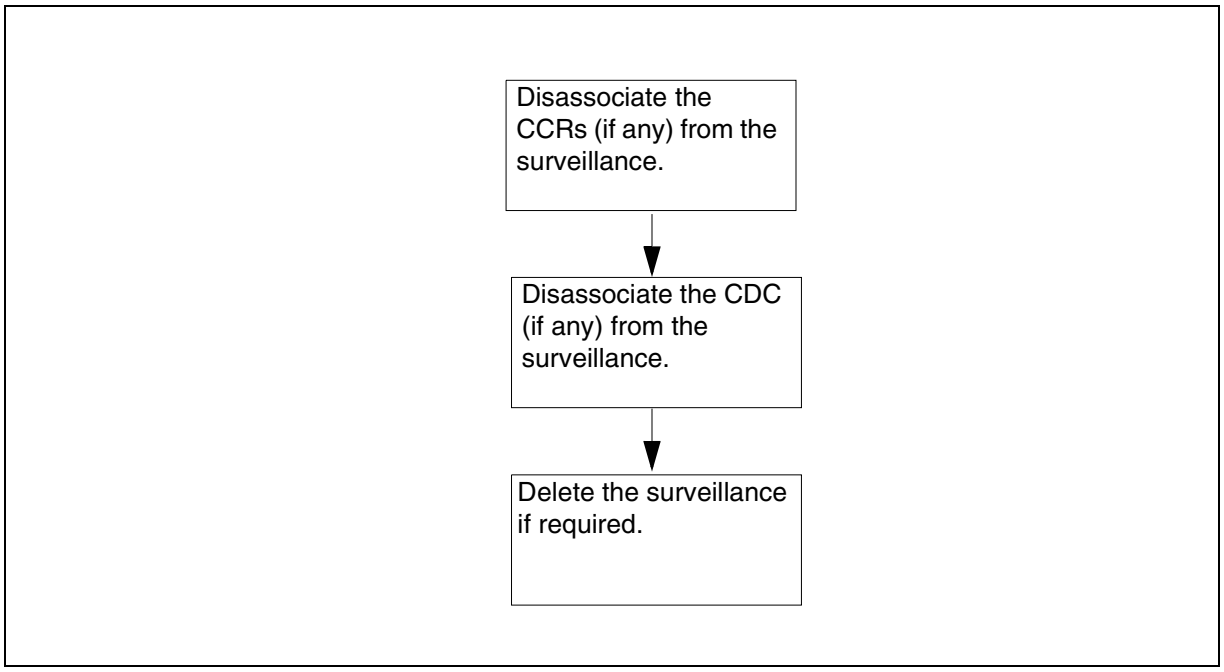
- the surveillance identification number (SIN) of the surveillance to be taken down
- the index number of any CCR(s) to be disassociated from the surveillance
- the index number of the CDC (if any) to be disassociated from the surveillance

The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of taking down a surveillance



Take down a surveillance

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Determine whether a CDC is associated with the surveillance. (In the example above, CDC 1 is associated with the surveillance.)

If a CDC is	Do
associated with the surveillance	step 3
not associated with the surveillance	step 4

3 Disassociate the CDC from the surveillance by typing:

cdc disassoc <sin>

and pressing the **Enter** key.

where **sin** is the surveillance identification number of the surveillance to be disassociated from the CDC

Example
cdc disassoc sin1

Example Response:

```
CDC DISASSOC DONE.
```

4 Determine whether one or more CCRs are associated with the surveillance. (In the previous example, CCR 10 is associated with the surveillance.)

If one or more CCRs are	Do
associated with the surveillance	step 5
not associated with the surveillance	step 6

5 Disassociate the CCR(s) from the surveillance by typing:

ccr disassoc <index>

and pressing the **Enter** key.

where **index** is the surveillance index number (1 through 500) of the CCR to be disassociated from surveillance

Example
ccr disassoc 8

Example Response:

```
CCR DISASSOC DONE.
```

Once a CCR is disassociated from its surveillance, the call to the call content channel (CCC) circuit(s) ends, and the CCC circuits are idle.

6 If required, delete the surveillance by typing:

surv del <sin>

and pressing the **Enter** key.

where **sin** is the surveillance identification number of the surveillance to be deleted

Example
surv del sin1

Example Response:

```
SURV DEL DONE.
```

7 Complete this procedure as follows:

If it is necessary to delete the	Do
CCRs	procedure Deleting a CCR
CDC	procedure Deleting a CDC

8 You have completed this procedure.

Deleting a CCR

Purpose of this procedure

The purpose of this procedure is to delete a call content resource (CCR). This procedure is performed by a USNBD user (with or without administrator privileges).

When to use this procedure

Use this procedure to delete all CCRs prior to deactivating USNBD, or when a particular CCR is no longer required.

Note: A CCR can be saved for reuse for other surveillances. Therefore, confirm with the law enforcement agency (LEA) that the CCR needs to be deleted.

Prerequisites

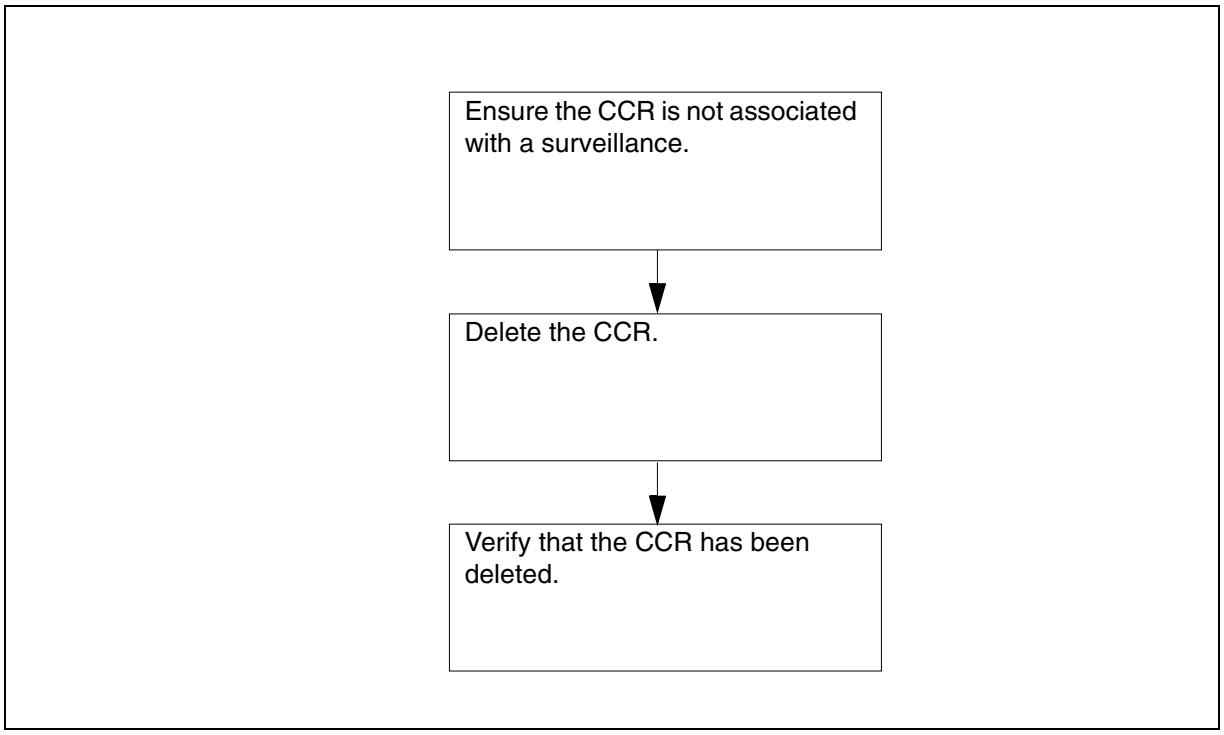
A CCR can only be deleted if it is disassociated from its surveillance.

The USNBD user who disassociates the CCR from its surveillance must be associated with the same agency as the CCR or have USNBD administrative rights.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of deleting a CCR



Delete a CCR

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

usnbd

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Display a list of all CCRs (as an administrative user) to ensure the CCR to be deleted is not associated with a surveillance by typing:

ccr list all

and pressing the **Enter** key.

Example Response:

```
CIndex Content CCRtype  CCRid Acc CCC1            [CCC2]
       [Sig]  [Tag]   Agency              [SIN]
-------------------------------------------------------
    10 VOICE   PAIRED   LINE  DE  9059632091      9059632101
       Y       N        AGENCY4                  SIN2

CCR LIST DONE.
```

Note 1: A non-administrative user can only view CCR information for the user's agency. The AGENCY parameter does not appear.

Note 2: The CCR is not associated with a surveillance if no entry appears under field SIN.

If the CCR is	Do
associated with a surveillance	step 3
not associated with a surveillance	step 4

3 Disassociate the CCR from the surveillance by typing:

`ccr disassoc <index>`

and pressing the **Enter** key.

where **index** is the surveillance index number (1 through 500) of the CCR to be disassociated from surveillance

Example
ccr disassoc 10

Example Response:

```
CCR DISASSOC DONE.
```

Note: The user disassociating this CCR must have the same agency as the CCR or have USNBD administrative rights.

4 Delete the CCR by typing:

`ccr del <index>`

and pressing the **Enter** key.

where **index** is the surveillance index number (1 through 500) of the CCR to be deleted.

Example
ccr del 10

Example Response:

```
CCR DEL DONE.
```

Note: The user deleting this CCR must have the same agency as the CCR or have USNBD administrative rights.

5 Ensure that the CCR has been deleted by typing:

`ccr list all`

and pressing the **Enter** key. You should not see a CCR entry with the index that was specified in the delete command.

Example Response:

```
CCR LIST: NO MATCHING CCRS
```

6 You have completed this procedure.

Deleting a CDC

Purpose of this procedure

The purpose of this procedure is to delete a call data channel (CDC). This procedure is performed by a USNBD user (with or without administrator privileges).

When to use this procedure

Use this procedure to delete a CDC prior to deactivating USNBD, or when a CDC is no longer required.

Note: A CDC can be saved and reused for other surveillances. Therefore, confirm with the law enforcement agency (LEA) that the CDC needs to be deleted.

Prerequisites

A CDC can only be deleted if

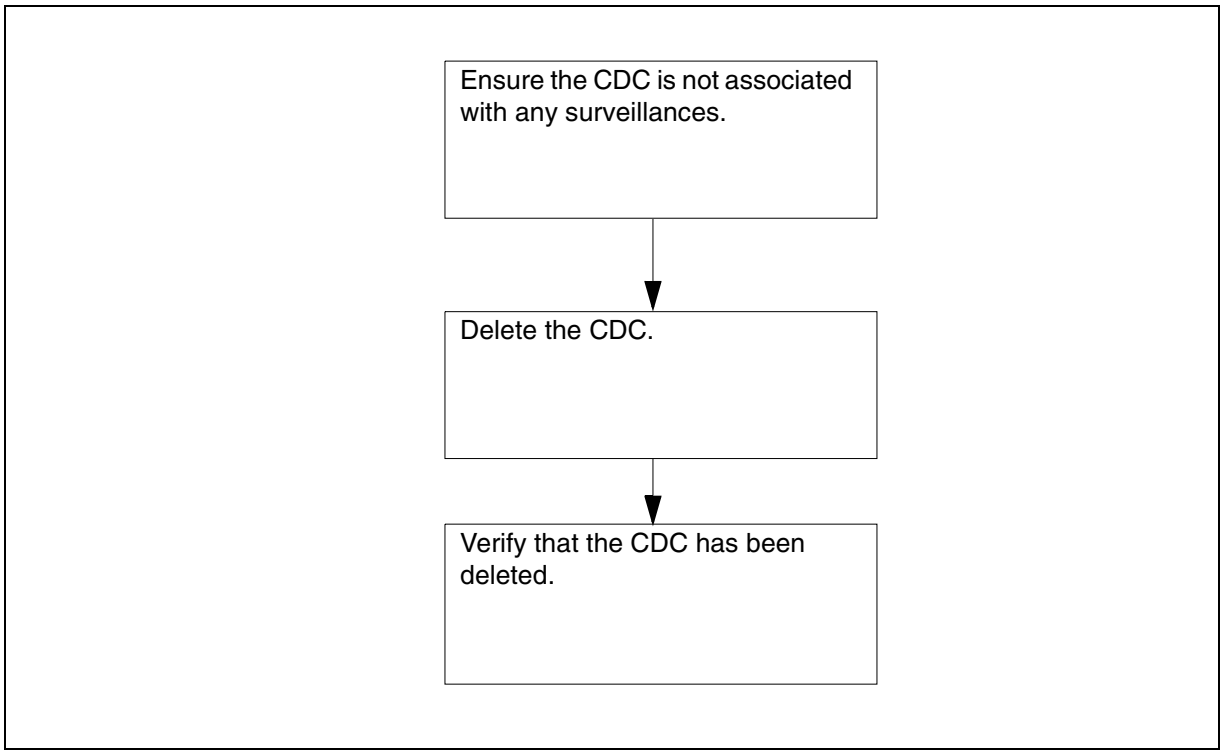
- the CDC is disassociated from all its surveillances
- all CDC messages have been sent and none are left in the CDC message queue

The USNBD user who disassociates the CDC from its surveillance must be associated with the same agency as the CDC or have USNBD administrative rights.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of deleting a CDC



Delete a CDC

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Display a list of all CDCs (as an administrative user) to ensure the CDC to be deleted is not associated with any surveillances by typing:

`cdc list all`

and pressing the **Enter** key.

Example Response:

```
Index Type MPClink Address     Protocol    Agency
      [Associated SINs]
-------------------------------------------------------------
   2 X25   1 3 12345          2   2   2   2   AGENCY3
Index Type  IP Address     IP Port       Agency
      [Associated SINs]
-------------------------------------------------------------
   1 IP  10  66  34  16    12347         AGENCY2
CDC LIST DONE.
```

Note 1: A non-administrative user can only view CDC information for the user's agency. The AGENCY parameter does not appear.

Note 2: The CDC is not associated with any surveillances if no entries appear under field Associated SINs.

If the CDC is	Do
associated with a surveillance	step 3
not associated with a surveillance	step 4

3 Disassociate the CDC from the surveillance by typing:

`cdc disassoc <sin>`

and pressing the **Enter** key.

where **sin** is the surveillance identification number (SIN) of the surveillance from which the CDC is to be disassociated

Example
cdc disassoc sin1

Example Response:

```
CDC DISASSOC DONE.
```

Note: The user disassociating this CDC must have the same agency as the CDC or have USNBD administrative rights.

4 Delete the CDC by typing:

`cdc del <index>`

and pressing the **Enter** key.

where **index** is the index number (1 through 200) of the CDC to be deleted.

Note: The user deleting this CDC must have the same agency as the CDC or have USNBD administrative rights.

5 Ensure the CDC has been deleted by typing:

cdc list all

and pressing the **Enter** key. You should not see a CDC entry with the index that was specified in the delete command.

Example Response:

```
CDC LIST: NO MATCHING CDCS
```

6 You have completed this procedure.

Deleting USNBD agencies

Purpose of this procedure

The purpose of this procedure is to delete existing USNBD agencies. This procedure is performed by a USNBD user (with or without USNBD administrator privileges).

When to use this procedure

Use this procedure to delete a USNBD agency with switched ISUP call content channel (CCC) or FSK SR CDC that is no longer required. Once a USNBD agency has been deleted, associated call content resources (CCR), call data channels (CDC), surveillances, and users lose the agency information.

Prerequisites

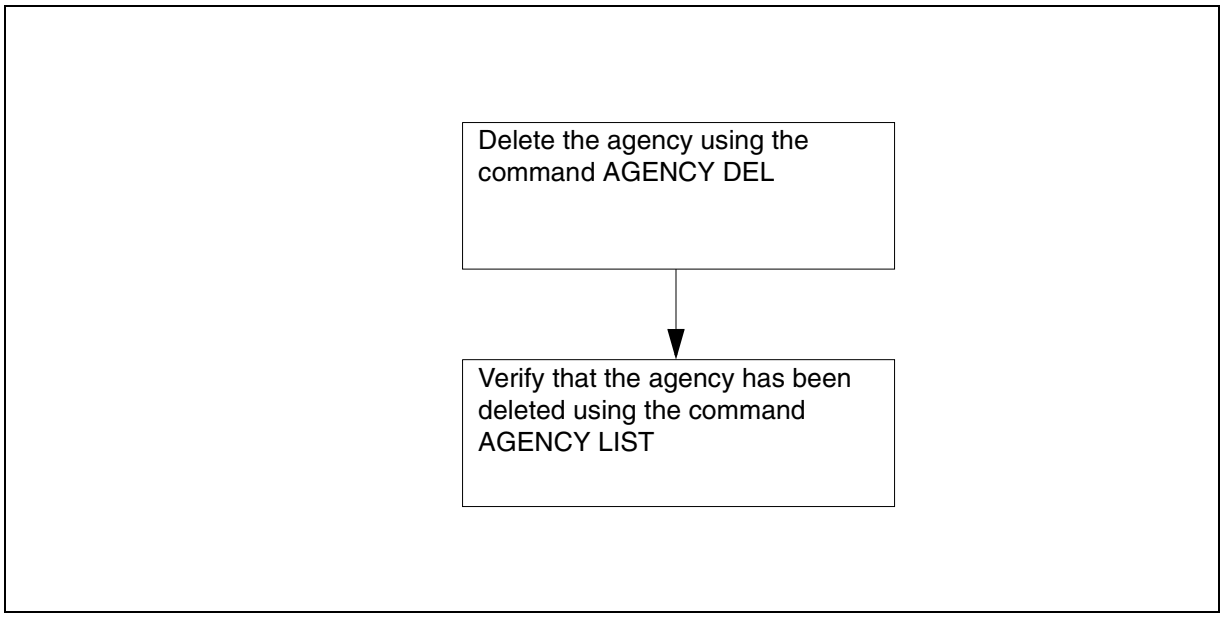
The following requirements must be met before deleting an agency:

- The user must have the agency name to perform this procedure.
- Switched ISUP CCRs corresponding to the agency are disassociated from all surveillances.
- FSK SR CDCs corresponding to the agency are disassociated from all surveillances.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of deleting USNBD agencies



Delete USNBD agencies

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Delete an agency by typing:

`agency del <agency_name>`

and pressing the **Enter** key.

where **agency_name** is the agency having access to switched ISUP CCCs or FSK SR CDCs to their remote recording device.

Example
agency del agency3

Example Response:

```
AGENCY DEL DONE.
```

3 Ensure the agency has been deleted by typing:

`agency list`

and pressing the **Enter** key.

Example Response:

```
AGENCY-NAME       STS PRETRANSLATOR LCANAME BILLNO
                  PIC                 LATA
-------------------------------------------------------
AGENCY1           613 P621            L667    1234567890
                  ITT                 LATA1
AGENCY2           416 P463            L467    0987654321
                  NILC                NILLATA
AGENCY LIST DONE.
```

4 You have completed this procedure.

Deleting USNBD users

Purpose of this procedure

The purpose of this procedure is to delete existing USNBD users. This procedure is performed by a USNBD user who has USNBD administrator privileges.

When to use this procedure

Use this procedure to delete a USNBD administrator or user who is no longer required. Once a USNBD administrator or user has been deleted, the user can no longer execute USNBD commands.

Note: At least one USNBD user with administrator privileges must be defined at all times. If you try to delete the only remaining administrator, the following message displays:

```
CANNOT DELETE THE ONLY REMAINING ADMINISTRATOR
```

Therefore, Nortel Networks recommends having at least two USNBD users with administrator privileges at all times.

For additional assistance with the **USER** command, type **user help** at the USNBD: prompt.

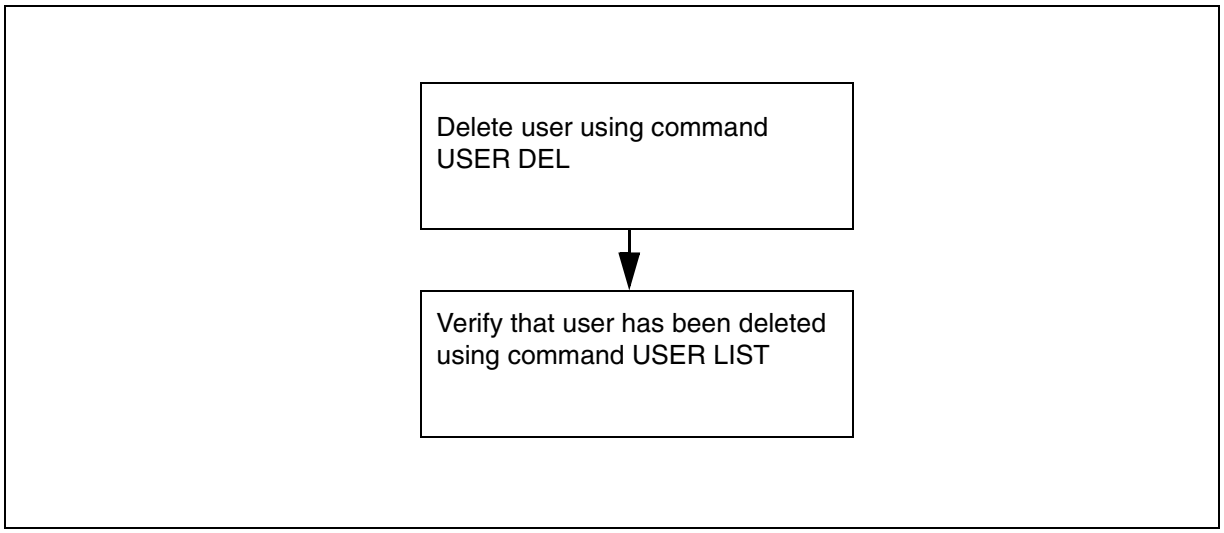
Prerequisites

None

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of deleting USNBD users



Delete USNBD users

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

`usnbd`

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Delete a user by typing:

`user del <user_id>`

and pressing the **Enter** key.

where **user_id** is the user id of the user to be deleted.

Example
user del user1

Example Response:

```
USER DEL DONE.
```

3 Ensure the user has been deleted by typing:

user list

and pressing the **Enter** key.

Example Response:

```
USERS   ADMIN
--------------------
USER2   Y
USER3   Y

USER LIST DONE.
```

4 You have completed this procedure.

Deactivating bearer channel tandeming

Purpose of this procedure

The purpose of this procedure is to deactivate bearer channel tandeming (BCT) functionality. This procedure is performed by a USNBD user (with or without administrator privileges).

When to use this procedure

Use this procedure when a law enforcement agency (LEA) requests that a surveillance on a subject be deactivated, and this is the last surveillance on the Communication Server.

For additional assistance with the **BCT** command, type **bct help** at the USNBD: prompt.

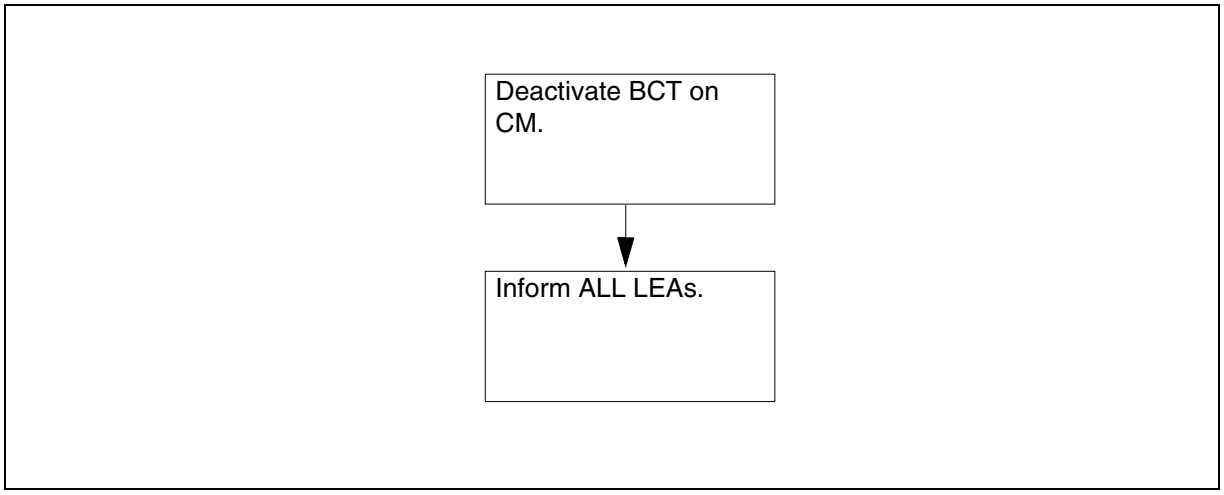
Prerequisites

Before deactivating BCT, ensure that there are no surveillances with associated call content resources (CCR).

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of deactivating BCT on a Carrier VoIP network



Deactivate bearer channel tandeming

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

usnbd

and pressing the **Enter** key.

Example Response:

```
USNBD:
```

At the USNBD level of the MAP

2 Deactivate the BCT for the tuple by typing:

bct deactivate

and pressing the **Enter** key.

Example Response:

```
BCT DEACTIVATE: BCT FUNCTIONALITY DEACTIVATED
```

3 If you do not want to change or delete a BCT tuple in table SERVSINV, go to step 9.

At the CI level of the MAP

4 Access table SERVSINV of the MAP by typing:

table servsinv

and press the **Enter** key.

5 Access the BCT tuple you want to remove for the specified gateway controller (GWC) by typing:

pos bct x

where x is the number associated with the BCT tuple in question. There can be multiple BCT tuples.

and press the **Enter** key.

6 Delete the BCT tuple typing:

del

and press the **Enter** key.

Example Response:

```
ENTER Y TO CONTINUE PROCESSING OR N TO QUIT
```

7 Continue processing by typing:

y

and press the **Enter** key.

Example Response (in an IP system):

```
TUPLE TO BE DELETED:
BCT 0 GWC 3 1024 (ALTTERMS 90)$
ENTER Y TO CONFIRM, N TO REJECT OR E TO EDIT.
```

8 Confirm the tuple deletion by typing:

y

and press the **Enter** key.

Example Response:

```
Static data update for GWC 3 UNIT 0 submitted.
Static data update for GWC 3 UNIT 1 submitted.
Static data updates completed.
TUPLE DELETED
```

9 You have completed this procedure.

Deactivating SOC option NBD00003

Purpose of this procedure

The purpose of this procedure is to deactivate USNBD in an office. This procedure is performed by a USNBD user who has USNBD administrator privileges.

When to use this procedure

Use this procedure when USNBD functionality is no longer required.

Prerequisites

Perform the following procedures before deactivating USNBD:

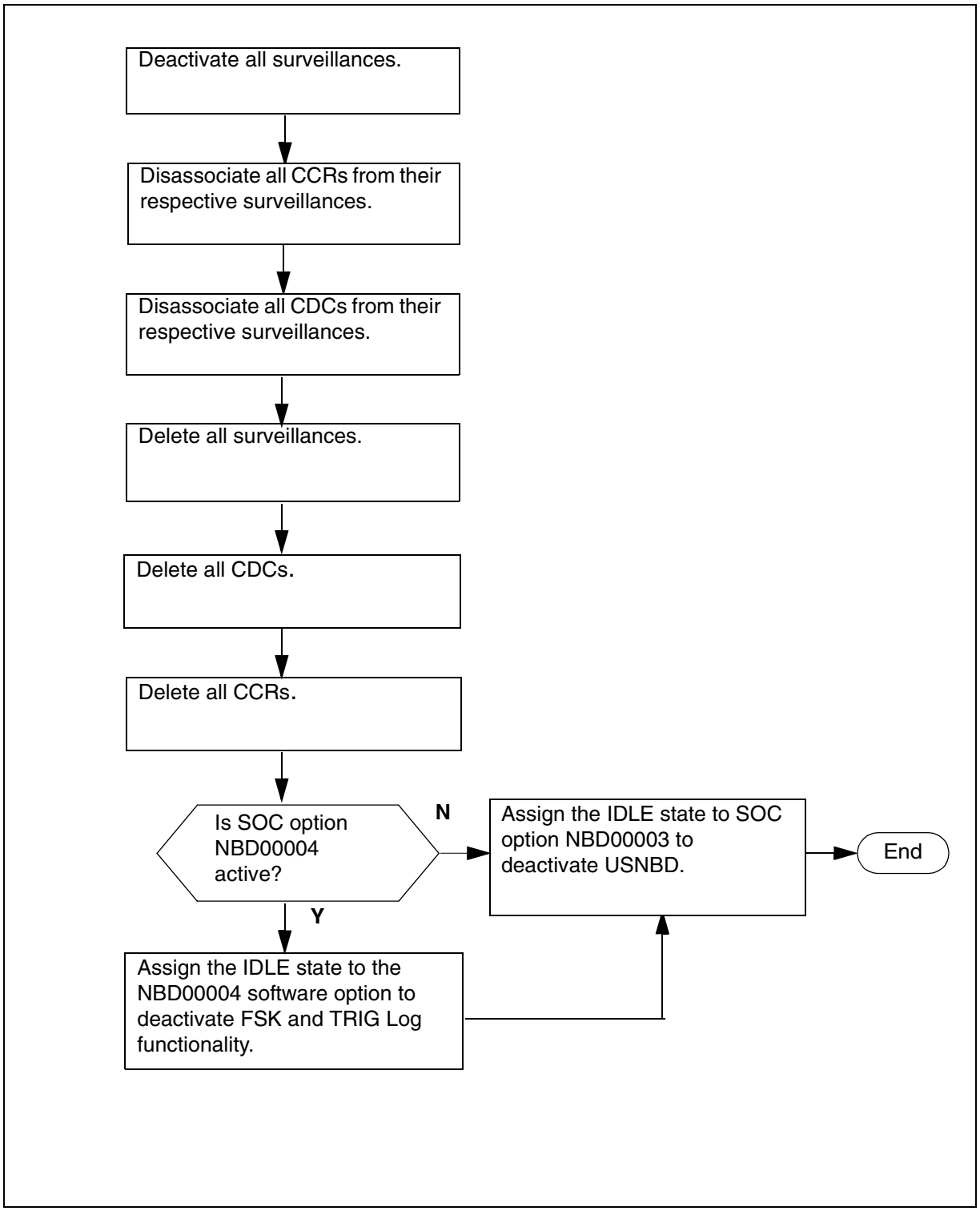
- deactivate all surveillances
- disassociate all call content resources (CCR) from their respective surveillances
- disassociate any call data channels (CDC) from their respective surveillances
- delete all surveillances
- delete all CDCs
- delete all CCRs
- deactivate trig log generation
- deactivate Line FSK CDC functionality (if needed)

Note: For information about deactivating Line FSK CDC functionality, refer to section Deactivating SOC option NBD00004 in this document.

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of deactivating USNBD in an office



Deactivate the SOC option NBD00003

At the CI level of the MAP

1 Display a list of all the active surveillances by typing:

```
surv list act
```

and pressing the **Enter** key.

2 Note the surveillance identification number (SIN) of each surveillance in the list.

3 Deactivate each surveillance in the list by typing:

```
surv deact <sin>
```

and pressing the **Enter** key.

where **sin** is the surveillance identification number of the surveillance to be deactivated.

Example
surv deact sin1

Example Response:

```
SURV DEACT DONE.
```

4 Repeat step 3 for each surveillance to be deactivated.

5 Display a list of all associated CCRs by typing:

```
ccr list assoc
```

and pressing the **Enter** key.

6 Note the index of each CCR in the list.

7 Disassociate each CCR in the list from its respective surveillance by typing:

```
ccr disassoc <index>
```

and pressing the **Enter** key.

where **index** is the number (1 through 500) that identifies the CCR.

Example
Example Response:

ccr disassoc
10

```
CCR DISASSOC DONE.
```

8 Repeat step 7 for each CCR to be disassociated.

9 Display a list of all associated CDCs by typing:

```
cdc list assoc
```

and pressing the **Enter** key.

10 Note the SIN of the surveillances with which each CDC is associated.

11 Disassociate each CDC in the list from its respective surveillances by typing:

```
cdc disassoc <sin>
```

where **sin** is the surveillance identification number of the surveillance with which the CDC is associated.

Example
cdc disassoc sin1

Example Response:

CDC DISASSOC DONE.

12 Repeat step 11 for each CDC to be disassociated.

13 Display a list of all surveillances by typing:

```
surv list all
```

14 Note the SIN of each surveillance in the list.

15 Delete each surveillance in the list by typing:

```
surv del <sin>
```

where **sin** is the surveillance identification number of the surveillance to be deleted.

Example
surv del sin1

Example Response:

SURV DEL DONE.

16 Repeat step 15 for every surveillance until a **surv list all** command shows no surveillance left.

17 Display a list of all CCRs by typing:

```
ccr list all
```

18 Note the index of each CCR in the list.

19 Delete each CCR in the list by typing:

```
ccr del <index>
```

where **index** is the number (1 through 500) that identifies the CCR.

Example
ccr del 1

Example Response:

CCR DEL DONE.

20 Repeat step 19 for every CCR until a **ccr list all** command shows no CCRs left.

21 Display a list of all CDCs by typing:

```
cdc list all
```

22 Note the index of each CDC in the list.

23 Delete each CDC in the list by typing:

```
cdc del <index>
```

where **index** is the number (1 through 500) that identifies the CDC.

Example
cdc del 10

Example Response:

CDC DEL DONE.

24 Repeat step 23 for every CDC until a **cdc list all** command shows no CDCs left.

25 Assign the IDLE state to the USNBD software option by typing:

```
assign state idle to nbd00003
```

Example Response:

```
Confirm state change of option NBD00003 to state
IDLE by entering the textual option name.
```

Confirm by typing:

```
usnbd
```

Example Response:

```
Done.
```

26 Choose the next step as follows:

If the right-to-use code for NBD00003	Do
needs to be removed	step 27
does NOT need to be removed	step 28

27 Remove the RTU key code from NBD00003 by typing:

`remove rtu <key_code> from nbd00003`

Example Response:

```
Done.
```

28 Exit the SOC utility by typing:

`quit`

29 You have completed this procedure.

Deactivating SOC option NBD00004

Purpose of this procedure

The purpose of this procedure is to deactivate USNBD FSK Line CDC functionality in an office. This procedure is performed by a USNBD user who has USNBD administrator privileges.

When to use this procedure

Use this procedure when USNBD FSK Line CDC functionality is no longer required.

Prerequisites

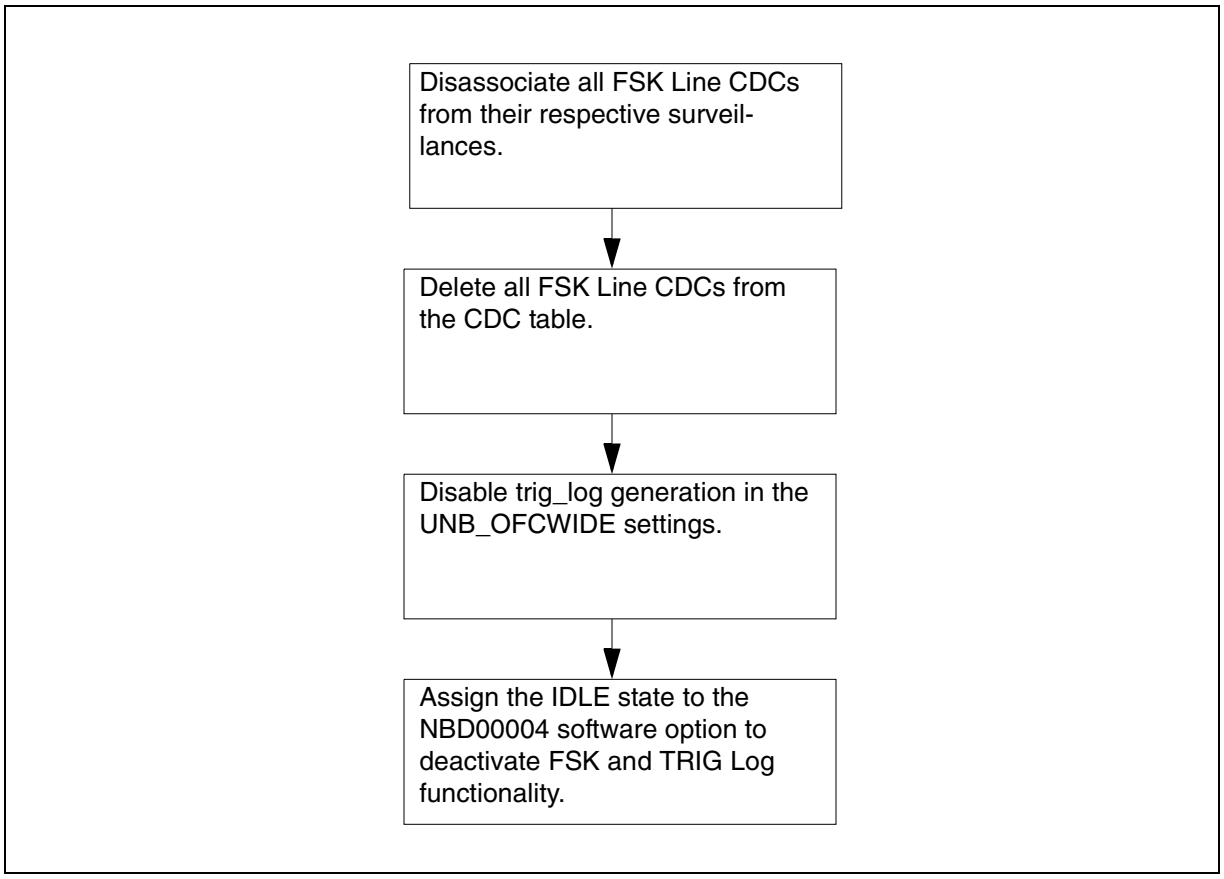
Perform the following procedures before deactivating USNBD FSK Line CDC functionality:

- disassociate all FSK call data channels (CDC) from their respective surveillances
- delete all FSK CDCs
- deactivate trig log generation

Action

The following flowchart is a summary of this procedure. Use the step-action instructions that follow the flowchart to perform the procedure.

Summary of deactivating USNBD FSK Line CDC functionality in an office



Deactivate SOC option NBD00004

At the CI level of the MAP

1 Display a list of all associated CDCs by typing:

```
cdc list assoc
```

and pressing the **Enter** key.

2 Note the SIN of the surveillances with which each FSK Line CDC is associated.

3 Disassociate each FSK Line CDC in the list from its respective surveillances by typing:

```
cdc disassoc <sin>
```

where **sin** is the surveillance identification number of the surveillance with which the CDC is associated.

Example
cdc disassoc sin1

Example Response:

CDC DISASSOC DONE.

4 Repeat step 3 for each FSK Line CDC to be disassociated.

5 Display a list of all CDCs by typing:

cdc list all

6 Note the index of each FSK Line CDC in the list.

7 Delete each FSK Line CDC in the list by typing:

cdc del <index>

where **index** is the number (1 through 500) that identifies the FSK Line CDC.

Example
cdc del 10

Example Response:

CDC DEL DONE.

8 Repeat step 7 for every FDK Line CDC until a **cdc list all** command shows no FSK Line CDCs are left.

9 Deactivate trig_log generation by typing:

unb_ofcwide trig_logs off

Example Response:

```
TRIG_LOGS OFF DONE.
```

10 Access the software optionality control (SOC) utility by typing:

soc

Example Response:

```
SOC:
```

11 Assign the IDLE state to the Line CDC software option by typing:

assign state idle to nbd00004

Example Response:

```
This transition will disable provisioning of FSK
CDCs and the generation of TRIG logs. Refer to
UNSBD NTPs and contact you next level of support
before proceeding. Confirm state change of
option NBD00004 to state IDLE by entering the
textual option name.
```

Confirm by typing:

Line CDC

Example Response:

```
Done.
```

12 Choose the next step as follows:

If the right-to-use code for NBD00004	Do
needs to be removed	step 13
does NOT need to be removed	step 14

13 Remove the RTU key code from NBD00004 by typing:

`remove rtu <key_code> from nbd00004`

Example Response:

```
Done.
```

14 Exit the SOC utility by typing:

`quit`

15 You have completed this procedure.

Accessing LI-specific operational measurements

Purpose of this procedure

This procedure shows the correct syntax to use when accessing Lawful Intercept operational measurements (OM).

When to use this procedure

Use this procedure when it is necessary to access Lawful Intercept OMs.

Prerequisites

This procedure has no prerequisites.

Action

At the CS2000 MAPCI

1 Log in as the USNBD administrator.

2 At the prompt type

omshow *omgroup*

where

omgroup is one of the following:

- UNBCDC
- UNBMISC

3 Use the following table to review the details for OM group UNBCDC.

Lawful Intercept OMs for group UNBCDC

OM group	Registers	Description	Register Type	Notes
UNBCDC		Records measurements on USNBD call data channels (CDC).		
	CDCGEN	Register CDCGEN counts the number of CDC messages that USNBD generates. During a given period, CDCGEN can exceed CDCSNT even though no messages are lost. This condition occurs because the messages can be sent during the next OM collection period. CDCGEN can also be smaller than CDCSNT, which can occur when messages generated during an earlier OM collection period were successfully sent during the current OM collection.	peg-type	
	CDCSNT	Register CDCSNT counts the number of USNBD CDC messages successfully sent over the X.25 link.	peg-type	

4 Use the following table to review the details for OM group UNBMISC.

Lawful Intercept OMs for group UNBMISC

OM group	Registers	Description	Register Type	Notes
UNBMISC		Records miscellaneous USNBD data, including the number of monitored calls and the number of monitored calls for which monitoring was stopped because USNBD capacity is exceeded, or because of non-monitored features.		
	RELCPCTY	Register RELCPCTY counts the number of monitored calls for which monitoring was stopped because USNBD-defined capacity is exceeded.	peg-type	
	RELNMON	Register RELNMON counts the number of calls for which monitoring was stopped because of non-monitorable features, including the following: • the subject uses a feature not monitored by USNBD • the call is redirected and USNBD does not support this type of redirection, and cannot follow the call • the subject is on a 2FR line, and is currently talking to the mate 2FR subscriber ***Note:*** During a given period, RELNMON can exceed UNBMCALL. This condition occurs because monitoring could be stopped in the next OM collection period.	peg-type	
	UNBMCALL	Register UNBMCALL counts the number of calls monitored by USNBD. Register UNBMCALL determines the real-time impact monitored calls make on the DMS switch.	peg-type	

5 You have completed this procedure.

USNBD log reports

USNBD log reports

This section describes the following USNBD logs:

- BCT100
- BCT101
- BCT200
- BCT300
- BCT400
- BCT401
- UNB300
- UNB301
- UNB302
- UNB303
- UNB304
- UNB305
- UNB306
- TRIG600
- TRIG700

Only USNBD users (with or without administrator privileges) can access USNBD logs through the LOGUTIL; OPENSECRET UNB command. No password is required.

When to use this procedure

Use this procedure to view the USNBD logs.

Prerequisites

None

Log procedures

Viewing logs

At the CI level of the MAP

1 Access the LOGUTIL directory of the MAP by typing:

LOGUTIL

and pressing the **Enter** key.

Example Response:

```
LOGUTIL:
```

Access the UNB log buffer by typing: **opensecret UNB**

and pressing the **Enter** key.

Example:

```
UNB 300 JUN05 15:33:23 7300 INFO
CONFERENCE CIRCUIT HAS BEEN MADE BUSY
CALL CANNOT BE MONITORED
SIN:111
```

Log TRIG600

Field	Value	Action
INFO	300, 301, 302, 303, or 304	Indication that a UNB service impact log (300 to 304) has been generated

Log TRIG700

Field	Value	Action
INFO	305 or 306	Indication that a UNB information log (305 or 306) has been generated

Log UNB300 (Sheet 1 of 3)

Field	Value	Action
problem	This field indicates the problem USNBD encountered with a shared resource. Can be any of the following: • Conference circuit has been made busy	Inform the law enforcement agency (LEA), if required.

Log UNB300 (Sheet 2 of 3)

Field	Value	Action
	• Conference circuit unavailable	Inform the LEA, if required. Also install more conference circuits if this log is generated frequently.
	• DTMF receiver is unavailable	Inform the LEA, if required. Also consider installing more conference circuits.
	• DTMF receiver is lost	Inform the LEA, if necessary, and contact your Nortel Networks representative to determine further action.
	• Feature data block unavailable	Inform the LEA, if required. Also contact your Nortel Networks representative to determine further action.
	• FTRQ16WPERMS block unavailable	Inform the LEA, if required. Also contact your Nortel Networks representative to determine further action.
	• Bearer channel behind private network	Inform the LEA, if required. The voice communication between parties traverses a private network (e.g., enterprise network).

Log UNB300 (Sheet 3 of 3)

Field	Value	Action
result	• Call cannot be monitored • Call content cannot be delivered • Inband digits can have been lost • Inband digits have not been captured • Surveillance cannot be activated • CCC tag was not delivered • Inband digits capture not possible	
sin	alphanumeric	This field indicates the surveillance identification number (SIN) of the affected surveillance. When surveillance information is not available, this field is not present.

Log UNB301 (Sheet 1 of 6)

Field	Value	Action
cdc_problem	This field indicates the problem encountered with the call data channel (CDC). Can be any of the following:	
	CDC audit queue full	Use the QUERY PROCESS NBAUDIT command to determine if the NBAUDIT process is running. If the process is not running, recreate it by performing a warm or cold maintenance SWACT. If the process is running, verify all links (x.25, IP, and FSK) of the USNBD CDCs. If all links (x.25, IP, and FSK) are functional, contact your Nortel Networks representative to determine further action.

Log UNB301 (Sheet 2 of 6)

Field	Value	Action
	CDC has become invalid	If the CDC is X.25 then verify the multiprotocol controller (MPC) link information in tables MPC and MPCLINK. If the CDC is FSK then verify which changes have been made to the FSK CDC datafill, also ensure that the Class Modem Resource Card on the XPM hosting the FSK DN is in service. If required, contact the affected LEA. Correct the problem and re-add the CDC. Check log UNB304 to determine which surveillances the CDC was associated. Reactivate those surveillances.
	CDC queue full	Use the QUERY PROCESS FBSX25 command to determine if the FBSX25 process is running. If the process is not running, recreate it by performing warm or cold SWACT. If the process is running, contact your Nortel Networks representative.
	Maximum number of transmission attempts reached	Verify the datalink of the specified CDC. Inform the LEA.
	SVC failed	Verify the X25 datalink of the specified CDC. If required, contact the LEA to discuss further action.
	SCTP/IP failed	Verify the IP datalink of the specified CDC. If required, contact the LEA to discuss further action.
	Cannot route to CDC	

Log UNB301 (Sheet 3 of 6)

Field	Value	Action
	CDC down	Verify the FSK CDC line state. If required, contact the LEA. Disassociate the FSK CDC and reassociate it.
	CDC has become invalid	Verify which changes have been made to the CCR datafill. If required, contact the LEA to determine the problem. Correct the problem and recreate the CCR. Check log UNB304 to determine which surveillances the CCR was associated with and reactivate the surveillance(s).
	CDC in bad state	Verify the FSK CDC line state. If required, contact the LEA. Disassociate the FSK CDC and reassociate it.
	Lost integrity on CDC	Inform your next level of support.
	No answer from CDC	Verify the FSK CDC line state. If required, contact the LEA.
	Unsupported line class for CDC	Verify which changes have been made to the FSK CDC datafill. If required, contact the LEA to determine the problem. Correct the problem and recreate the FSK CDC. Check log UNB304 to determine which surveillances the FSK CDC was associated with and reactivate the surveillance(s).

Log UNB301 (Sheet 4 of 6)

Field	Value	Action
	Unsupported line format for CDC	Verify which changes have been made to the FSK CDC datafill. If required, contact the LEA to determine the problem. Correct the problem and recreate the FSK CDC. Check log UNB304 to determine which surveillances the CCR was associated with and reactivate the surveillance(s).
result	This field indicates the consequence of the problem, including any of the following: • CDC has been deleted • CDC message has been lost • CDC message has been put in the CDC audit queue • CDC message cannot be sent on this CDC • CDC messages have been lost	
cdc_index	1 through 200	This field indicates the index number of the CDC with the problem.
mpc	0 through 255	This field indicates the MPC index number defined for the CDC that was deleted. The MPC index number is only provided when the result field is “CDC has been deleted.”
link	0 through 3	This field indicates the MPC link number defined for the CDC that was deleted. The MPC link number is only provided when the result field is “CDC has been deleted.”

Log UNB301 (Sheet 5 of 6)

Field	Value	Action
address	1 through 15 decimal digits	This field indicates the MPC address defined for the X.25 CDC that was deleted. The MPC address is provided only when the result field is “CDC has been deleted” and the CDC deleted was an X.25 CDC.
protocol	4 decimal digits of 0 through 255	This field indicates the protocol defined for the X.25 CDC that was deleted. The protocol is provided only when the result field is “CDC has been deleted” and the CDC deleted was an X.25 CDC.
IP address	4 decimal digits of 0 through 255	This field indicates the IP address defined for the IP CDC that was deleted. The IP address is provided only when the result field is “CDC has been deleted” and the CDC deleted was an IP CDC.
port	0 through 32767	This field indicates the port defined for the IP CDC that was deleted. The port is provided only when the result field is “CDC has been deleted” and the CDC deleted was an IP CDC.

Log UNB301 (Sheet 6 of 6)

Field	Value	Action
access	SL or DE	This field indicates the access (switched local or dedicated) defined for the FSK CDC that was deleted. The access is provided only when the result field is “CDC has been deleted” and the CDC deleted was an FSK CDC.
DN	10-digit DN	This field indicates the 10-digit directory number defined for the FSK CDC that was deleted. The access is provided only when the result field is “CDC has been deleted” and the CDC deleted was an FSK CDC.

Log UNB302 (Sheet 1 of 2)

Field	Value	Action
process_ problem	This field indicates the problem encountered with the CDC. Can be any of the following: • abnormal death • failure to start	
process_ name	This field indicates the process that encountered the problem. • FSBX25 or NBDAUDIT	Determine if the affected process is running using the QUERY PROCESS <process_name> command. If the process is not running, recreate it by performing a warm or cold maintenance SWACT. If the process does not start or ends unexpectedly, contact your Nortel Networks representative to determine further action.

Log UNB302 (Sheet 2 of 2)

Field	Value	Action
	• NBDRCVRY	Determine if SWERRs or TRAPs related to USNBD were generated. If SWERRs and TRAPs were generated, recreate the process by performing a warm or cold maintenance SWACT. If the process does not start or ends unexpectedly, contact your Nortel Networks representative to determine further action. If no SWERRs or TRAPs were generated, no action is required.
result	This field indicates the consequence of the problem. Can be any of the following: • CDC messages are queued, but not sent • The USNBD audit does not run • Process to be recreated • USNBD recovery cannot be performed	

Log UNB303 (Sheet 1 of 5)

Field	Value	Action
ccr_problem	This field indicates the problem the CCR. Can be any one of the following:	
	Cannot route to CCC	
	CCC down	Verify the CCC line state. If required, contact the LEA. Disassociate the CCR and reassociate it.

Log UNB303 (Sheet 2 of 5)

Field	Value	Action
	CCC has become invalid	Verify which changes have been made to the CCR datafill. If required, contact the LEA to determine the problem. Correct the problem and recreate the CCR. Check log UNB304 to determine which surveillances the CCR was associated with and reactivate the surveillance(s).
	CCC in bad state	Verify the CCC line state. If required, contact the LEA. Disassociate the CCR and reassociate it.
	ISUP link released	
	Lost integrity on CCC	Inform your next level of support.
	Missing billing number	
	No answer from CCC	Verify the CCC line state. If required, contact the LEA. Disassociate the CCR and reassociate it.
	Network connection unavailable	Verify the JNET or ENET. In the case of Carrier VoIP Networks, ensure the UAS hosting the BCT node is in service. If required, inform your next level of support.
	Problem outpulsing the correlation tag	Contact the LEA if required.
	Unsupported line class for CCC	Verify which changes have been made to the CCR datafill. If required, contact the LEA to determine the problem. Correct the problem and recreate the CCR. Check log UNB304 to determine which surveillances the CCR was associated with and reactivate the surveillance(s).

Log UNB303 (Sheet 3 of 5)

Field	Value	Action
	Unsupported line format for CCC	Verify which changes have been made to the CCR datafill. If required, contact the LEA to determine the problem. Correct the problem and recreate the CCR. Check log UNB304 to determine which surveillances the CCR was associated with and reactivate the surveillance(s).
	Unsupported trunk bearer capability for CCC	Verify which changes have been made to the CCR datafill. If required, contact the LEA to determine the problem. Correct the problem and recreate the CCR. Check log UNB304 to determine which surveillances the CCR was associated with and reactivate the surveillance(s).
	Unsupported trunk direction, trunk signaling, or trunk type for CCC	Verify which changes have been made to the CCR datafill. If required, contact the LEA to determine the problem. Correct the problem and recreate the CCR. Check log UNB304 to determine which surveillances the CCR was associated with and reactivate the surveillance(s).
	Bearer channel behind private network	Inform the LEA, if required. The voice communication between parties traverses a private network (e.g., enterprise network)
result	Can be any one of the following: • call content cannot be delivered • CCR has been deleted • correlation tag not delivered • switched ISUP CCC call cannot be billed	

Log UNB303 (Sheet 4 of 5)

Field	Value	Action
ccr_index	This field indicates the index number of the CCR that encountered the problem. (1 through 500)	
ccc_index	This field indicates the CCC of the affected CCR. A value of 1 identifies the first (or only) CCC of the CCR. A value of 2 identifies the second CCC of a paired CCR. (1 or 2)	
type	This field indicates if the CCR is a combined or paired CCR. (1 or 2)	
ccr_id	Specifies the type of CCC (line or trunk) and the CCC through four subfields depending on the type of CCR and if they are lines or trunks. (LINE <dn1> [<dn2] <signaling> Trunk <tg1><tn1>[<tg2><tn2>])	
signaling	Specifies if signaling is enabled on the CCC(s). (Y or N)	
tg1	Specifies the CCLI of the trunk group containing the first CCC or the CCR. (String)	
tn1	Specifies the trunk number of the first CCC or the CCR. (Integer 0 to 9999)	
tg2	Specifies the CLLI of the trunk group containing the second CCC or the CCR. (String)	

Log UNB303 (Sheet 5 of 5)

Field	Value	Action
tn2	Specifies the trunk number of the second CCC of the CCR. (Integer 0 to 9999)	
dn1 or dn2	This field indicates the 10-digit DN of CCC1 (combined) or CCC1 and CCC2 (paired)	

Log UNB304 (Sheet 1 of 3)

Field	Value	Action
agency	This field identifies the agency of the surveillance. (1 to 16 characters)	
surv_event	This field identifies the event encountered. Can be any one of the following:	
	CCR has become invalid	Check the corresponding UNB303 log. If the CCR is recreated, reassociate it with the surveillance and reactivate the surveillance if required.
	CDC has become invalid	Check the corresponding UNB301 log. If the CDC was recreated, reassociate it with the surveillance and reactivate the surveillance if required.
	No free usable CCR	Inform the LEA of the problem. Ensure that sufficient CCRs are provisioned for the type of calls the subject can originate or receive.
	Subject has become unsupported	Verify any changes that were made to the subject's service. Contact the LEA to discuss further action.

Log UNB304 (Sheet 2 of 3)

Field	Value	Action
	Subject has been deleted	Verify if the subject's service was moved to another DN, LEN, KEY or LTID. Contact the LEA to discuss further action.
	SURV ACT command successfully processed	
	SURV DEACT command successfully processed	
result	can be any of the following: • Call content cannot be delivered • CCR has been disassociated and surveillance deactivated • CCR has been disassociated from surveillance • CDC has been disassociated and surveillance deactivated • CDC has been disassociated from surveillance • Surveillance has been deleted • Surveillance has been activated • Surveillance has been deactivated	
sin	This field indicates the surveillance identification number of the affected surveillance. (alphanumeric)	
subject	This field identifies the subject of the affected surveillance; handle and subject subfields.	

Log UNB304 (Sheet 3 of 3)

Field	Value	Action
caseid	This field identifies the user who performed the action. This field is optional and is only provided when the event is a surveillance activation or deactivation. (alphanumeric)	
mrp	This field indicates if a monitored replacement party (MRP) was allowed for the affected surveillance. (Y or N)	
clgdlvry	This field indicates if delivery of the calling party number was allowed for the affected surveillance. (Y or N)	
cdc_index	This field indicates the index number of the CDC associated with the surveillance when the surveillance is deleted or the index number of the CDC that is disassociated from the surveillance. (CDC index)	
ccr_list	This field indicates the index number of each CCR associated with the surveillance when the surveillance is deleted or the index number of each CCR that is disassociated from the surveillance. (CCR list)	
user	This field identifies the user who performed the action. This field is optional and is only provided when the event is a surveillance activation or deactivation. (alphanumeric)	

Log UNB305 (Sheet 1 of 2)

Field	Value	Action
user_event	This field identifies the event encountered. Can be any one of the following: • CI user has been deleted • ASSIGN STATE ON command successfully processed • USER ADD command successfully processed • USER DEL command successfully processed	
result	This field identifies the consequence of the event encountered. Can be any one of the following:	
	USNBD user has been added	
	USNBD user has been deleted	
	USNBD administrator has been added	
	USNBD administrator has been deleted	
	Initial USNBD administrator has been defined	
	USNBD administrator has been deleted; no administrator left. When this result appears in the log message, a major alarm is raised in the office.	Contact your Nortel Networks representative for further action.

Log UNB305 (Sheet 2 of 2)

Field	Value	Action
user_id	This field identifies the CI user name that was added or deleted. (alphanumeric)	
user	This field identifies the user who performed the action. This field is optional and is only provided when the event is the successful processing of a command. (alphanumeric)	

Log UNB306 (Sheet 1 of 2)

Field	Value	Action
date	This field represents the date the log was generated. (month-date)	
time	This field represents the time the log was generated. (time)	
datafill-type	This field identifies the type of datafill removed from the appropriate table. Can be any one of the following: • STS • PRETRANSLATOR • LCANAME • PIC • LATA	

Log UNB306 (Sheet 2 of 2)

Field	Value	Action
table-name	This field identifies the table from which the datafill has been deleted. Can be any one of the following: • HNPACONT • STDPRTCT • LCASCRN • OCCNAME • LATANAME	
agency-name	This field identifies the USNBD agency when the recording links cannot be established. (1 to 16 alphanumeric characters)	The USNBD user for the affected agency must determine the missing datafill value using the USNBD command AGENCY. The USNBD user ensures that this value is correct for the agency. If incorrect, the user assigns the correct datafill value for the agency using the AGENCY command. Conversely, if the current agency datafill is correct, it should be validated that the value does not exist in the table name indicated in the log. The user should invoke the operating company procedure to re-add the missing datafill to the table indicated in the log report. The action to be taken depends on the information indicated in the result field.

Log BCT100 - Pool out of Resources

Field	Value	Action
XPM_NO	Together with “BCT” makes the tuple in SERVSINV which had insufficient resources. (0 to 255)	This error comes as a result of having insufficient resources in the BCT Resource pool on the CM. This happens if a mismatch arises between the number of resources provisioned on the CM (in table SERVSINV) and the number of resources actually available on the Centralized Replicator (CR). To fix this problem, the mismatch must be corrected by increasing the number of resources in table SERVSINV to match the actual number of resources on the CR. If there is no mismatch between the number of provisioned resources, then contact the next level of support.

Log BCT101 - Resource pool could not be found for the pool

Field	Value	Action
	A request to reserve a BCT Resource Pool failed because there were no pools with sufficient resources. Alarm: Major	A call that was supposed to be tandemed was not tandemed because a resource pool with sufficient resources could not be found. This problem can arise for the following reasons: • There are not enough BCT capable Centralized Replicators • The BCT capable CRs have insufficient BCT cards • The number of resources provisioned in the CM for BCT is less then the number of resources on the CR For the first two cases, more BCT cards must be added to the existing CRs capable of BCT, or more BCT capable CRs must be added to the network. For the third case, the mismatch in provisioned resources must be remedied. If the problem is recurring and none of the criteria has been met, or the actions above failed to solve the problem, contact the next level of support.

Log BCT200 Resource Pool Update

Field	Value	Action
prev#	The previous number of resources {0,128, ..., 1280}	
cur#	The current number of resources {0, 128, ..., 1280}	
XPM_NO	“BCT” with this number gives the BCT Resource pool that was updated in table SERVSINV. {0 - 255}	

Log BCT300 Insufficient System Memory

Field	Value	Action
		There was insufficient system memory to activate BCT. More memory should be added to the system, and the tuple in table SERVSINV should be re-attempted. No calls can be tandemed until this problem is resolved. If the problem persists, contact the next level of support.

Log BCT400 Resource Pool Update

Field	Value	Action
XPM_NO	High water mark reporting of the most resources in use per BCT Resource pool during the last BCT Audit cycle. “BCT” with this number gives the BCT Resource pool found in table SERVSINV. {0 to 255}	This log is for tracking purposes only. If, however, the usage of a BCT Resource pool is continually near its total, then the operating company can add BCT cards to the CR corresponding to the pool, or add more BCT capable CRs to the network. This type of log is generated for each BCT Resource Pool in table SERVSINV once a day by the BCT Audit Process.
resources_used	This number is between 0 and the number of resources provisioned for the pool. {0 - provisioned resources for pool}	
available	The number of resources provisioned for the pool. {128, 256, ..., 1280}	

Log BCT401 BCT Audit Process Information

Field	Value	Action
event	Reports when the Audit Process is created and killed. Information about the BCT Audit process. • stopped: The BCT Audit Process has died and cannot be recreated • created: The BCT Audit Process has been created and executes when next scheduled. If the process died unexpectedly during execution, then it begins executing immediately after creation. • completed: BCT has been deactivated and the Audit Process is stoppedpermanently. {“created,” “stopped,” “completed”}	These logs are for informational purposes used to verify that BCT has been successfully activated by reporting the status of the BCT Audit Process.
cur#	The current number of resources {0, 128, ..., 1280}	
XPM_NO	“BCT” with this number gives the BCT Resource pool that was updated in table SERVSINV. {0 - 255}	

Carrier Voice over IP

Lawful Intercept (NA)

Product and Technology Fundamentals

Publication number: NN10190-113
Product release: (I)SN09 and up
Document version: Standard 07.02
Date: January 2006

NORTEL NETWORKS™