297-9801-300

DMS-100 Family

North American DMS-100

US Network Broadcast Delivery (USNBD) Feature Guide

SN07 Standard 07.01 December 2004

NORTEL NETWORKS™

DMS-100 Family

North American DMS-100

US Network Broadcast Delivery (USNBD) Feature Guide

Document Number: 297-9801-300
Product Release: SN07
Document Release: Standard 07.01
Date: December 2004

Copyright © 1998 - 2004 Nortel Networks,
All rights reserved

Printed in the United States of America

NORTEL NETWORKS CONFIDENTIAL: The information contained herein is the property of Nortel Networks and is strictly confidential. Except as expressly authorized in writing by Nortel Networks, the holder shall keep all information contained herein confidential, shall disclose the information only to its employees with a need to know, and shall protect the information, in whole or in part, from disclosure and dissemination to third parties with the same degree of care it uses to protect its own confidential information, but with no less than reasonable care. Except as expressly authorized in writing by Nortel Networks, the holder is granted no rights to use the information contained herein.

Nortel Networks, the Nortel Networks logo, the Globemark, How the World Shares Ideas, and Unified Networks are trademarks of Nortel Networks.

Publication history

December 2004

SN07 Standard 07.01. Standard release of the document. Documented the following features and CRs:

- A00003513 - Lawful Interception - Private Network Interception
- A00004037 - USNBD - FSK CDC Over Trunks
- Q00824951 - References to Document NN10190-113
- Q00824973 - Revise Part Number for Cable 1 in Appendix B

September 2003

NA017 Standard 06.02. Standard release of the document.

September 2002

For the NA017 standard release 06.01, NA017 changes were inserted into the NA015 version, with hyperlinks between NA017 chapters or sections and corresponding NA015 chapters and sections.

Section USNBD - CDC in Chapter 3 was revised by CR Q00264962. Section Creating a CDC in Chapter 8 was revised by CR Q00264962. Section USNBD - SURV in Chapter 3 was revised by CR Q00284110.

March 2001

NA015 Standard 05.01. Standard release of the document.

September 2000

NA014 Standard 04.02. Standard release of the document.

March 2000

NA013 Standard 03.02. Standard release of the document.

October 1999

NA012 Standard 02.02. Standard issue of the document.

April 1999

NA011 Standard 02.00; Second standard release of this document.

October 1998

NA010 Standard 01.00; first standard issue of this document.

Contents

About this document **xiii**
Structure of this document xiii
Input prompt (>) xiv
Commands and fixed parameters xiv
Variables xiv
Responses xiv

Chapter 1: Feature description **1-1**
Description 1-3
Network overview 1-3
Operating company premises 1-4
Law Enforcement Agency (LEA) premises 1-4
Functionality 1-5
Call monitoring 1-5
Call content delivery 1-6
Voice levels on paired CCRs 1-10
Monitoring information delivery 1-10
Administration 1-12
Capacity 1-12
Operation 1-13
Delivering call content 1-13
Creation of a CCR 1-14
Association of a CCR 1-14
Assignment of a CCR 1-15
Activation of a CCR 1-16
Deactivation of a CCR 1-17
Reactivation of a CCR 1-17
Release of a CCR 1-17
Disassociation of a CCR 1-18
Deletion of a CCR 1-19
Failure of a CCR 1-19
Delivering monitoring information 1-19
Creation of a CDC 1-19
Association of a CDC 1-19
Delivery of monitoring information to the LEA 1-19
Disassociation of a CDC 1-20
Deletion of a CDC 1-20
Failure of a CDC 1-20

Monitoring calls 1-21
FSK transport 1-21
Intercepting calls within private networks 1-23
DMS switch processes used for USNBD 1-23
Packet Data Call monitoring 1-24
Packet Data Interception and Delivery overview 1-24
Packet Data Channels 1-25
Packet Data Channel provisioning 1-25
Packet Data Channel processing 1-26
Intercepted data call content 1-29
Packet segmentation 1-29
Packet loss 1-29
Failure of a Packet Data Channel 1-29
PVC endpoints 1-30
Monitoring information delivery 1-30
CDC message set for Packet Data monitoring 1-30
CCOpen parameter changes 1-30
Packet Data Call monitoring 1-30
Activation of monitoring for Packet Data 1-31
Deactivation of monitoring for Packet Data 1-31
USNBD data integrity for Packet Data monitoring 1-31
Inband Digit Collection 1-33
Management of digit receivers 1-33
Modifications to USNBD setup process 1-34
Making changes to datafill 1-34
Hardware requirements 1-36
Limitations and restrictions 1-36
Software optionality control 1-37
Interactions 1-39
Service orders 1-39
Operational measurements 1-39
Logs 1-39
Office parameters 1-39
Data store 1-40
User interface 1-40
Billing 1-40
One-night process, restarts, and SWACTs 1-40
Packet data calls 1-41

Chapter 2: CDC messages **2-1**

Overview 2-1
Description of messages 2-2
Answer message 2-2
CCClose message 2-3
CCOpen message 2-4
CCUnavailable message 2-5
Change message 2-5
Connect 2-6
Disconnect 2-7
Feature Status message 2-7

InbandDigit message 2-8
Notification message 2-8
Origination message 2-9
Redirection message 2-10
Release message 2-11
Surveillance Status message 2-12
TerminationAttempt message 2-12

Chapter 3: USNBD commands 3-1
USNBD 3-2
USNBD - AGENCY 3-3
USNDB - CCR 3-9
USNBD - CDC 3-23
USNBD - HELP 3-31
USNBD - QUIT 3-41
USNBD - SURV 3-43
USNBD - TEST 3-52
USNBD - UNB_OFCWIDE 3-59
USNBD - USER 3-65
OBJMGRCI 3-70
PHRRCI - MOVE 3-73
PVCOBJCI 3-74
QCOUNTS 3-77
QPHF 3-81
UNPERMIT 3-84
Qualifications 3-84
XPSCI 3-87
Error responses 3-89
Information-type messages 3-112

Chapter 4: Operational measurements 4-1
OM group CF3P 4-2
OM group EXT 4-7
OM group FCNF 4-11
OM group UNBCDC 4-17
OM group UNBMISC 4-21
OM group XLIUL3 4-27

Chapter 5: Log reports 5-1
UNB300 5-2
UNB301 5-5
UNB302 5-10
UNB303 5-12
UNB304 5-17
UNB305 5-22
UNB306 5-24

Chapter 6: Data schema 6-1
Table PVCINFO 6-2
Table LIDINFO 6-4

Chapter 7: Provisioning USNBD 7-1
Calculating hardware requirements 7-1
Input data 7-1
Hardware and circuit calculations 7-2
Calculating the number of conference circuits 7-2
Calculating the number of X.25 links 7-3
Calculating the number of DTMF senders 7-3
Calculating the number of DTMF receivers 7-3
Calculating the number of CCC circuits 7-4
Provisioning surveillances 7-4

Chapter 8: USNBD administrator and user procedures 8-1
Summary of surveillance setup commands 8-2
Activating SOC option NBD00003 8-3
Adding USNBD users 8-7
Adding an agency 8-11
Creating CCRs 8-15
Creating a CDC 8-21
Adding a surveillance 8-26
Associating a CDC with a surveillance 8-31
Associating a CCR with a surveillance 8-36
Activating a surveillance 8-41
Ensuring inband digits delivery 8-49
Deactivating a surveillance 8-54
Taking down a surveillance 8-58
Deleting a CCR 8-63
Deleting a CDC 8-67
Deleting USNBD agencies 8-71
Deleting USNBD users 8-75
Deactivating SOC option NBD00003 8-78

Appendix A: Surveillance checklists 9-1
Information required prior to surveillance setup 9-1
Switch provisioning considerations 9-2
Pre-provisioning of X.25 interfaces 9-2
Low- or high-speed links 9-2
Facilities to LEAs 9-2
Checklist for each surveillance 9-2
Recommended CCR provisioning guidelines 9-6
Typical trunk datafill for trunks used for CCRs 9-7

Appendix B: Sample USNBD X.25 connections 10-1
Cable 1 10-5
Cable 2 10-6
Cable 3 10-8
Table datafill sequence 10-8
Table MPC 10-9
Description 10-9
Table MPC datafill sequence 10-9

Datafilling table MPC 10-9
Datafill example for table MPC 10-11
Table MPCLINK 10-12
Description 10-12
Table MPCLINK datafill sequence 10-13
Table size 10-13
Datafilling table MPCLINK 10-13
PROTOCOL = X2584 10-15
Datafill example for table MPCLINK 10-20

List of terms **11-1**

About this document

When to use this document

This document describes the US Network Broadcast Delivery (UNSBD) feature.

The document is a response to customer requests that Nortel Networks consolidate descriptive information into one document.

Structure of this document

The following table describes the contents of each chapter in this NTP.

Chapter	Chapter
1 Feature description	describes USNBD and provides information on the operation of USNBD, interactions with other features, restrictions and limitations, datafill, and other necessary parameters
2 CDC messages	provides a description of the CDC messages that USNBD can generate
3 USNBD commands	provides a description of USNBD commands
4 Operational measurements	provides a description of the OM registers used for USNBD
5 Log reports	describes the log reports that USNBD can generate
6 Data schema	provides a description of the data schema tables that USNBD uses
7 Provisioning USNBD	contains provisioning procedures for USNBD

Chapter	Chapter
8 USNBD administrator and user procedures	contains procedures for USNBD administrators and users on how to provide USNBD functionality, set up and control surveillances
9 Appendix A	contains checklists for surveillances
10 Appendix B	contains sample X.25 setups for USNBD
11 List of terms	defines terms used with the feature

How commands, parameters, and responses are represented

Commands, parameters, and responses in this document conform to the following conventions.

Input prompt (>)

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

```
>BSY
```

Commands and fixed parameters

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

```
>BSY CTRL
```

Variables

Variables are shown in lowercase letters:

```
>BSY  CTRL  ctrl_no
```

The letters or numbers that the variable represents must be entered. Each variable is explained in a list that follows the command string.

Responses

Responses correspond to the MAP display and are shown in a different way:

```
FP 3 Busy CTRL 0: Command request has been submitted.

FP 3 Busy CTRL 0: Command passed.
```

The following excerpt from a procedure shows the command syntax used in this document:

Busy the CTRL on the inactive plane by typing the following

>BSY CTRL ctrl_no

and then press the Enter key.

where

ctrl_no is the number of the CTRL (0 or 1)

Example of a MAP response:

```
FP 3 Busy CTRL 0: Command request has been submitted.
FP 3 Busy CTRL 0: Command passed
```

Chapter 1: Feature description

This chapter describes the US Network Broadcast Delivery (USNBD) feature, and provides information on the operation of USNBD, interaction with other features, restrictions and limitations, datafill, and parameters.

US Network Broadcast Delivery

Functionality name

US Network Broadcast Delivery (USNBD)

Functional group ordering code

NBD0001

Functionality ordering code

NBD00003

USNBD was introduced in NA010.

The USNBD feature has no prerequisites.

This chapter contains changes invoked by the following design activities:

- AU2775 - USNBD-3
- A00003513 - Lawful Interception - Private Network Interception
- A00004037 - USNBD - FSK CDC Over Trunks

Description

The Communications Assistance for Law Enforcement Act (CALEA) requires that telecommunications equipment manufacturers provide operating companies with the capability to support lawfully authorized electronic surveillance (LAES) activities. 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 USNBD feature complies with CALEA requirements, and provides North American DMS-100, DMS-100/200, and DMS-500 switches with the capability to support lawfully authorized electronic surveillance activity. With the USNBD feature, operating companies can monitor calls made and received by a switch-based subject and deliver the monitored information to authorized LEAs that require it.

The USNBD feature applies to Service Switching Point (SSP) and non-SSP end office switches.

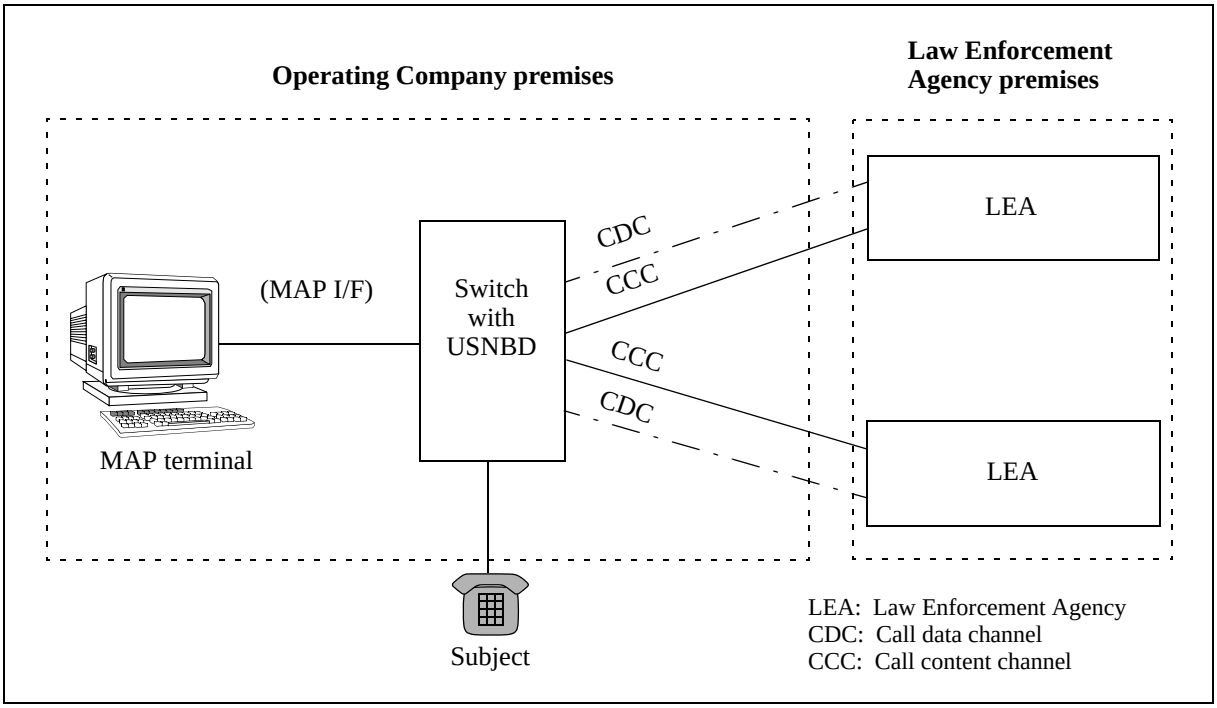
Network overview

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.

US Network Broadcast Delivery

Figure 1-1 illustrates the network overview of USNBD.

Figure 1-1 Network overview of USNBD



Operating company premises

The operating company provides the communications facilities between the subject switch and the LEAs. The communications facilities consist of

- trunks or analog lines, referred to as call content channels (CCC) in the USNBD software, which are used to deliver the call content of a monitored call
- X.25 datalinks or FSK local line dial-out call data channels (CDCs) in the USNBD software, which are used to deliver monitoring information

The operating company allows authorized operating company personnel to set up the USNBD feature, and establish and control surveillances. Access is through a MAP terminal, which communicates with the subject switch.

Law Enforcement Agency (LEA) premises

The LEAs provide the equipment to monitor a call. The equipment can include headsets, recording devices, or both for the termination of CCCs, and X.25 message decoders and processors for the termination of CDCs.

US Network Broadcast Delivery

Functionality

The functionality of the USNBD feature consists of capabilities in the following areas:

- call monitoring
- call content delivery
- monitoring information delivery
- administration

Call monitoring

The objective of the USNBD feature is to monitor the telephone service of selected individuals, called subjects, and deliver the monitored information to the LEAs that require it.

In the event that a monitored call is redirected to another party by the subject's service, USNBD continues to monitor the call. The party to which a monitored call is redirected is called the monitored replacement party (MRP).

The party or parties with which the subject or the MRP is linked during a monitored call are called associates, and the information that can be delivered to the LEAs is

- call content, which is the telephone conversation between the subject or MRP and one or more associates
- monitoring information, which includes information about the call established using the subject's telephone service and information about the CCCs used for the monitored call

  Note: Call monitoring only applies to the subject's telephone service and not the MRP's or associates' telephone service. Therefore, no monitoring information is reported to the LEAs for events that occur from an MRP's or associate's telephone service, except for answer and release events.

Call monitoring is available for basic two-party calls (calls with a single call leg and no features), and calls on which features are active.

Note: For USNBD, a call refers to either a single call leg (for example, A is talking with B) or a set of related call legs (for example, A is talking with B, and C calls A who has call waiting [CWT]).

Call monitoring is set up through surveillances. A surveillance refers to one LEA monitoring one subject. While one LEA can monitor many subjects, and

US Network Broadcast Delivery

many LEAs can monitor one subject, one surveillance must be set up between each LEA and each subject.

For example, if one LEA wants to monitor 10 subjects, 10 surveillances (one for each subject) are set up. If three different LEAs want to monitor the same subject, three surveillances (one for each LEA) are set up. (Refer to "Capacity" on page 1-12 for surveillance capacity.)

Multiple surveillances can monitor one call. Each monitored call of a surveillance is uniquely identified by a call id.

A monitored call can be one with a set of related call legs or one with a single call leg. When a new call leg is created by or for the subject's telephone service, USNBD assigns a new call ID to the call leg.

When an LEA requests a surveillance, the LEA gives the surveillance a case identity. A case identity is unique for each surveillance that an LEA requests, however, it may not be unique across the surveillances that all the LEAs request. Therefore, the operating company assigns a surveillance identification number (SIN) to each surveillance, which is unique across all surveillances within a subject switch.

Surveillances can have different characteristics that determine whether

- call content is delivered to the LEA
- monitoring information is delivered to the LEA
- monitoring information and call content, if applicable, are delivered to the LEA for calls redirected by the subject's service
- calling party directory numbers are delivered to the LEA

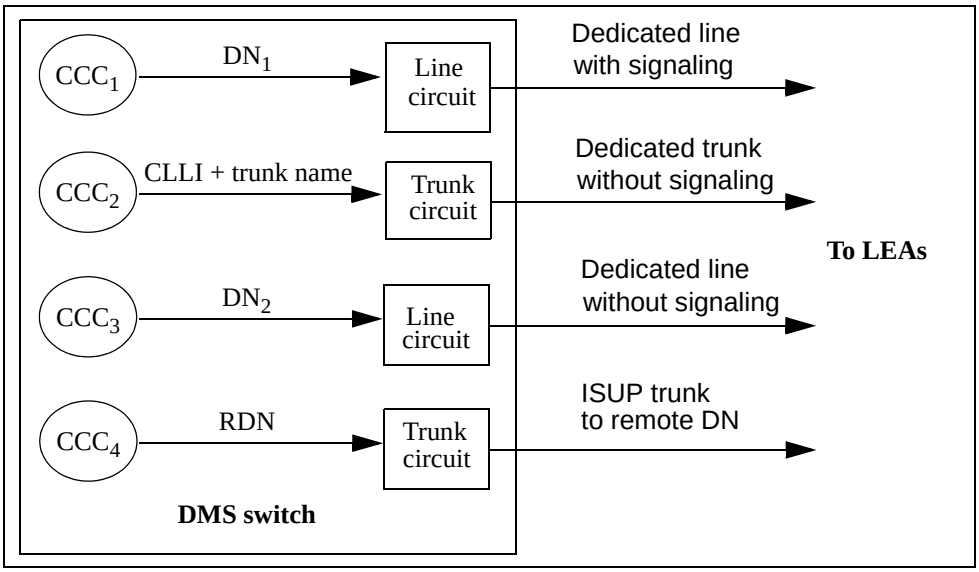
Call content delivery

Call content refers to the telephone conversation between the subject or MRP and one or more associates. Call content is delivered to the LEA through call content channels (CCC) over trunks or analog lines, using dedicated or remote switched connections.

A CCC is a logical channel internal to the USNBD software. Each CCC is represented by a directory number (DN) or a CLLI and external trunk name that corresponds to a physical facility on the subject's switch called a CCC line or trunk circuit (see Figure 1-2).

US Network Broadcast Delivery

Figure 1-2 CCC interface types



USNBD supports four types of interfaces to an LEA:

- dedicated lines with signaling
- dedicated lines without signaling
- dedicated trunks without signaling
- remote switched access

Non-signaling lines and trunks do not use handshaking between the switch and the LEA to establish a communication channel. For example, going off-hook at the LEA's end on a non-signaling line or trunk has no effect. Only the operating company can establish or take down a call to a CCC circuit using a non-signaling line or trunk.

Dedicated lines with signaling consist of analog lines. To use a dedicated line with signaling as a CCC circuit, the line

- must have a non-ambiguous 10-digit DN
- must have a line class code (LCC) of 1FR, 1MR or RES

  Note 1: An LCC of RES can only be assigned to a line if table OFCVAR parameter RES_SO_SIMPLIFICATION is set to N Y. If this parameter is set to N N or Y N, an LCC of RES cannot be assigned to the line.

US Network Broadcast Delivery

Note 2: 1FR lines can only have options COD, DGT, and NAME assigned. 1MR and RES lines must not have any options assigned and must be maintained without any options, as no option checking is performed.

Dedicated lines without signaling consist of 1FR lines. To use a dedicated line without signaling as a CCC circuit, the line must meet the same requirements as dedicated lines with signaling.

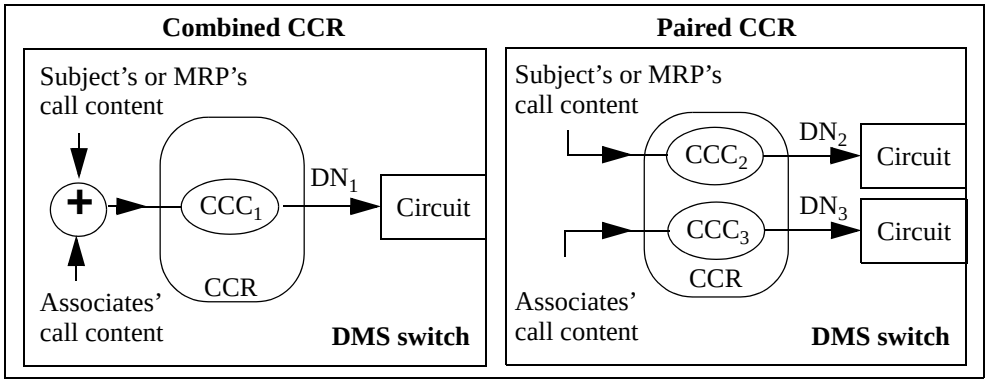
Note: The same line cards can be used for non-signaling and signaling types of dedicated lines.

Dedicated trunks without signaling consist of nailed-up (NU) type trunks that provide 64 Kbps DS0 channels.

Call content is delivered to the LEA using either a combined or paired call content resource (CCR). A combined CCR delivers the subject's or MRP's and associates' call content on one CCC. A paired CCR delivers the subject's or MRP's and associates' call content on two CCCs as shown in Figure 1-3. When paired CCRs are used for surveillances, both CCCs must be of the same physical interface type (line or trunk).

The CCRs associated with a surveillance need not use the same channel delivery method and physical interface type. However, for a paired CCR, both CCC circuits must have the same physical interface type (line or trunk).

Figure 1-3 Combined and paired CCRs



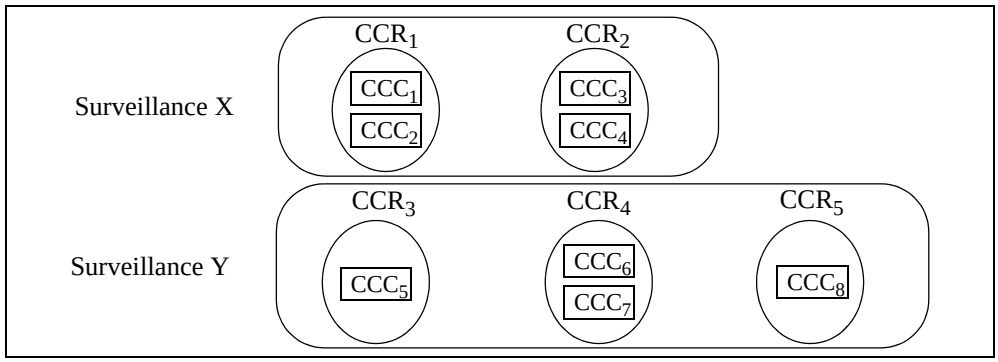
A CCR is associated with a surveillance when an LEA requests to receive call content for monitored calls. A CCR can be associated with only one surveillance at a time. A mixture of combined and paired CCRs can be associated with the same surveillance to deliver call content, as illustrated for

US Network Broadcast Delivery

Surveillance Y in Figure 1-4. As well, a mixture of line type CCRs and trunk type CCRs can be associated with the same surveillance.

The CCCs for combined CCRs are provisioned one at a time, while the CCCs for paired CCRs are provisioned in pairs.

Figure 1-4 CCRs associated with surveillances



Remote switched connections handle an idle subject differently from dedicated connections. Dedicated connections use an H4L3 tone to prevent recording when the subject is idle. When the subject becomes active, the H4L3 tone is removed and recording begins. The access type of the recording device is specified using the CCR ADD command.

For switched connections, there is no H4L3 tone when the subject is idle. Connections to the recording device are established as soon as links have answered and the network connections of the monitored call have been established. The Bellcore ISUP TR-317 standard is the only signaling supported for reaching remote recording devices. USNBD waits up to 30 seconds for a switched CCC to answer. Any failure or unexpected event that occurs during or after call establishment causes the appropriate log to be generated, informing the agency of the problem.

If the switched links fail to connect during the call setup, USNBD makes only one retry after 5 seconds to establish a switched connection. For paired CCRs, if only one connection to the recording device completes successfully, recording takes place and only the party associated with this link will be recorded. The switched connection that failed will not be re-established during the call. The two connections to the recording device will be set up again only when the subject is involved in a subsequent call. An audit will not re-establish the switched links that failed, even if the monitored call is not complete.

US Network Broadcast Delivery

When the subject disconnects, the call is terminated and the recorder DNs and billing records are generated if applicable. Switched connections are taken down following the ISUP TR-317 signaling standard. CCClose CDC messages are generated when the recorder link is disconnected.

> ***Note:*** It is possible to register the same DN for multiple CCRs in the same switch or in multiple switches. This would mean that multiple subjects could be associated to a single recorder. If two or more subjects become active at the same time, the recording device may capture only one call if sufficient resources are not available. The other may not be recorded, although monitoring still generates X.25 messages. The service provider and the LEA must ensure that a either one-to-one mapping exists between a subject and a recorder, or that the recording device uses multiple line DNs (for example, hunt groups) with sufficient resources to meet the interception needs.

Remote switched locations can only be set up utilizing SS7 TO, IT, or T2 type trunks. To route to remote switched locations through an Equal Access (EA) network, SS7 trunks of type TO, IT, or T2 can be datafilled with translations to terminate to a virtual DN which is call forwarded to the remote location (Remote Call Forwarded DN with PIC assigned.) The SS7 trunks can be looped back to back or terminate to an another switch in the network using existing spans.

ATC type trunks, which are Nortel's trunk type used to connect to different long distant carriers, cannot be used for the first trunk leg of the call. Local Number Portability (LNP) and 800 numbers cannot be used if they are triggered from the host switch where the surveillance is provisioned. Both LNP and 800 can be used if they are triggered from a remote switch and the call egresses the host switch via TO, IT, or T2 trunks.

Voice levels on paired CCRs

A separated CCR provides the subject's transmit content on one CCC circuit, and the associate's transmit content on the other CCC circuit. Because the 2-wire to 4-wire conversion hybrid in the subject's or associate's line card does not provide complete channel separation, call content from one channel will appear about 20 dB lower in the other channel.

Monitoring information delivery

Monitoring information refers to information about the call established through the subject's telephone service and information about the CCC(s) used for the call. Monitoring information is delivered to the LEAs through call data channels (CDC) over a point-to-point facility.

US Network Broadcast Delivery

A CDC is a logical link between the subject switch and the LEA. The physical link currently used for CDCs is an X.25 datalink configured as a Switched Virtual Circuit (SVC), which uses the X.25 protocol to exchange information.

A CDC is provisioned using the CDC command, and is associated with a surveillance when an LEA requests to receive call monitoring information for a monitored call. A CDC can be associated with one or more surveillances. Different surveillances for the same LEA can share the same CDC.

When a CDC is associated with a surveillance, all monitoring information for that particular surveillance is sent to the LEA in CDC messages through the provisioned CDC.

The CDC messages that USNBD generates are as follows:

Message	Message is generated when...
Answer	a monitored call is answered
CCClose	a CCC is released
CCOpen	a CCC is assigned
CCUnavailable	CCC links could not be established due to a connection failure, or content (of an intercepted call) is not available because the call is in a private network
Change	two calls are merged into one or when a call ID is changed
Connect	a connection is established between the Network Module (NM) and a peripheral module (PM), between a monitored party (subject or MRP) and an associate or conference circuit
Disconnect	a connection is broken in the NM or in a PM between a monitored party (subject or MRP) and an associate or conference bridge
Feature Status	the LEA is informed about the line options assigned to the subject
InbandDigit	a call is being monitored, inband digits are delivered to the LEA as soon as they are available to the call data intercept access point (CDIAP)
Notification	the LEA is informed about the treatment encountered by the subject, or with an indication of message waiting that is applied towards the subject by the IAP switch
Origination	the subject originates a call

US Network Broadcast Delivery

Message	Message is generated when...
Redirection	a monitored call is redirected by the subject's service from the subject to another party
Release	monitoring ends on a call with an identification of the non-monitorable feature that caused the surveillance release
Surveillance Status	a surveillance is activated, deactivated, or updated
TerminationAttempt	the subject receives a call

For a description of the CDC messages and their parameters, refer to Chapter 2 "CDC messages".

Administration

The USNBD feature provides the USNBD command directory that allows authorized operating company personnel to set up the USNBD feature, and establish and control surveillances. This command directory is accessed from the CI level of a MAP terminal.

For details on the USNBD command directory, refer to Chapter 3 "USNBD commands".

Capacity

Capacity limits for USNBD are provided in Table 1-1 and Table 1-2. The limits indicated in Table 1-1 are enforced during provisioning. When the USNBD administrator or a USNBD user performs an operation that exceeds the limit, the operation is not executed, and an error message is displayed. The limits indicated in Table 1-2 are enforced during operation of the feature. These limits are USNBD-specific and do not affect the normal processing of events.

Table 1-1 USNBD provisioning limits

Resource	Limit
Number of surveillances per switch	400
Number of concurrent surveillances on a subject	5
Number of call content resources (CCRs) per switch	500
Number of CCRs per surveillance	5
Number of call data channels (CDCs) per switch	200

Table 1-1 USNBD provisioning limits (Continued)

Resource	Limit
Number of CDCs per surveillance	1
Number of users/administrators	20

Table 1-2 USNBD run-time capacity limits

Resource	Limit
Number of simultaneous monitored calls ***Note:*** When the number of simultaneous monitored calls reaches the limit, any new calls that require monitoring are not monitored. Only a Release message with release reason “capacity exceeded” is sent to the LEA.	512
Number of assigned CCRs per surveillance ***Note:*** When the number of assigned CCRs for a subject reaches the limit, any new calls that require assignment of a CCR can still be monitored, but call content is not delivered.	as provisioned (0 to 5)

Operation

The USNBD feature operates on a switch basis, and allows operating companies to monitor calls made and received by a subject and deliver the monitored information to the LEAs that require it.

> ***Note:*** Complete instructions for feature operation are contained in Chapter 8 “USNBD administration and user procedures”. This chapter provides only brief summaries of each command.

Delivering call content

Call content from a monitored call is delivered to the LEAs using combined or paired CCRs. A CCR can be in one of four states as described in Table 1-3.

Table 1-3 CCR states

CCR state	Description
UNASSOCIATED	The CCR is defined (added), but not associated with a surveillance.
ASSOCIATED	The CCR is associated with a surveillance, but not assigned to a monitored call (C-tone provided).

US Network Broadcast Delivery

Table 1-3 CCR states (Continued)

CCR state	Description
ASSIGNED	The CCR is assigned to a monitored call, but call content delivery is not activated
ACTIVATED	The CCR is assigned to a monitored call and call content delivery is activated

Note: The state of the CCC circuit(s) is the same as the state of the CCR to which it belongs, unless a failure occurs on a CCC circuit, in which case the state of the CCC circuit can be different from the state of the CCR.

Creation of a CCR

An authorized USNBD user creates one or more CCRs using the CCR ADD command. The AGENCY parameter is prompted only for an administrative user, who can add any CCR. For non-administrative users, the user's agency is taken as the CCR agency and the user is not prompted for this parameter. The USNBD user creating the CCR also must be associated with the same agency as the CCR or have USNBD administrative rights. Once a CCR is added, the CCC circuits are idle and the CCR is ready to be associated with a surveillance.

Association of a CCR

An authorized USNBD user associates a CCR with a surveillance using the CCR ASSOC command. The CCR agency and the surveillance agency must be the same. The USNBD user performing this procedure also must be associated with the same agency as the CCR or have USNBD administrative rights.

Once a dedicated CCR is associated with a surveillance, USNBD makes a call to the CCC circuit(s). When call setup is successful, C-tone is applied on the CCC circuit(s). If call setup is unsuccessful, the CCR is not associated and an error message is displayed. If USNBD is unable to establish a call to one of the CCCs of a paired CCR, the CCR is not associated.

Note: Each USNBD call to a CCC circuit requires one USNBD extension block. If no extension block is available, CCR association fails, and the FBSEXT register in the EXT operational measurement (OM) group is incremented.

US Network Broadcast Delivery

Assignment of a CCR

In most cases, USNBD assigns a CCR to a monitored call when the monitored call is routed, that is, after an Origination, TerminationAttempt, or Redirection message is generated.

When the subject is LEN surveillance on a keyset or ISDN terminal and the subject receives a call, a CCR is assigned when

- the subject answers the call (USNBD assigns a CCR after the Answer message is generated)
- the subject redirects the call to another party and monitoring is supported for all agents on the call (USNBD assigns a CCR after the Redirection message is generated)

When more than one CCR associated with a surveillance is unassigned, USNBD assigns the first combined CCR with a working CCC or paired CCR 64 Kbps clear channel with two working CCCs. If no CCRs match this condition, USNBD assigns the first paired CCR with only one working CCC. When a paired CCR with only one working CCC is assigned, only half the call content is delivered.

When a combined dedicated CCR is assigned:

- a conference circuit is assigned to the monitored call
- C-tone is removed from the CCC circuit
- a one-way connection is made from the conference circuit to the CCC circuit
- a CCOpen message is generated

Note 1: If assignment of a conference circuit fails, register FCNFFAIL of OM group FCNF and registers in group CF3P are pegged. If assignment succeeds, register FCNFSUCC and registers in group CF3P are pegged. (For details on these OM registers, refer to Chapter 4 “Operational measurements”.)

Note 2: If no conference circuit is available, the CCR is still assigned to the monitored call but not activated, and other attempts to assign the conference circuit occur every time USNBD activates or deactivates a CCR.

When a paired dedicated CCR is assigned:

- C-tone is removed from the CCC circuits

US Network Broadcast Delivery

- two CCOpen messages are generated

A CCR is not assigned to a monitored call when

- the call is routed to a treatment locally
- the call is not routed because the call was abandoned
- no more unassigned CCRs are available or no CCRs have their CCC circuit(s) in working condition

Activation of a CCR

A CCR is activated prior to call answer (as soon as a connection has been established in the Network Module (NM) between a monitored subject and an associate). CCRs are activated on calls to monitored ISDN and KSET lines only when the subject answers. The following table summarizes the activation triggers:

CCR activation triggers

Line type	Call to subject	Call from subject	Calls redirected from subject
KSET by LEN/ ISDN	answer	network connection	network connection
Other	network connection	network connection	network connection

When a combined CCR is activated:

- a one-way connection is made from the subject to the conference circuit
- a one-way connection is made from the other party to the conference circuit
- the inputs from the subject and other party to the conference circuits are combined and are output on the conference circuit connected to the CCC circuit

When a paired CCR is activated:

- a one-way connection is made from the subject to the first CCC circuit
- a one-way connection is made from the other party to the second CCC circuit

Deactivation of a CCR

A CCR is deactivated when the connection in the NM has been broken, or when the call is placed on hold.

A CCR is deactivated when the call leg or legs of the monitored call are no longer active.

When a combined dedicated CCR is deactivated:

- the one-way connection from the subject to the conference circuit (if any) is broken
- the one-way connection from the other party to the conference circuit (if any) is broken
- the CCC circuit is placed on hold and is silent

  Note: If the conference circuit that provides the one-way connection from the subject to the conference circuit and the one-way connection from the other party to the conference circuit is not already assigned, an attempt is made to assign one at this stage.

When a paired dedicated CCR is deactivated:

- the one-way connection from the subject to the first CCC circuit is broken
- the one-way connection from the other party to the second CCC circuit is broken
- the CCC circuits are placed on hold and are silent

Reactivation of a CCR

The CCR is reactivated when the call is retrieved from hold, provided that a connection is established in the NM when retrieving the call.

Release of a CCR

A CCR is released when

- monitoring ends on the call (release occurs after a Release message is generated)
- the subject is an ISDN terminal, and the subject puts the monitored call on hold (a CCR is reassigned when the call is retrieved)

  Note: The CCR is released when an ISDN subject puts a call on hold, **only** if SOC options NI000050 and NI000051 are turned on and option PVC2 is assigned to the monitored LTID.

US Network Broadcast Delivery

CCC tag delivery enables LEAs to make a correlation between the end of a call content and a CCClose message. The beginning of the CCC tag transmission corresponds to the sending of the CCClose message.

The CCC tag delivery is supported for all types of dedicated CCRs (lines and trunks, signaling or not). To prevent the loss of call content, the CCC tag is delivered at the end of call content before the C-tone is applied to the CCR. The information delivered to the CCR is the CALLID provided as part of the CCC message of the terminating monitored call.

When a combined dedicated CCR is released

- the one-way connection from the conference circuit to the CCC circuit is released
- the conference circuit assigned to the monitored call (if any) is released
- the CCC tag is delivered (if set to Y for the CCR) and provides the call ID of the terminating monitored call
- C-tone is applied to the CCC circuit
- a CCClose message is generated

When a paired dedicated CCR is released

- the one-way connection from the subject to the first CCC circuit is released
- the one-way connection from the other party to the second CCC circuit is released
- the CCC tag is delivered on each of the CCCs (if set to Y for the CCR) and provides the call ID of the terminating monitored call
- C-tone is applied to the CCC circuits
- two CCClose messages are generated

Disassociation of a CCR

An authorized USNBD user disassociates a CCR from a surveillance using the CCR DISASSOC command. The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights. Once a CCR is disassociated from a surveillance, the call to the CCC circuit(s) ends, and the CCC circuits are idle.

Deletion of a CCR

An authorized USNBD user deletes a CCR using the CCR DEL command. The USNBD user performing this procedure must be associated with the same agency as the CCR or have USNBD administrative rights.

Failure of a CCR

If a CCC circuit of an associated signaling dedicated link fails, USNBD immediately attempts to recover it. If the attempt fails, a USNBD audit (NBDAUDIT), which runs every 15 minutes or less if required, and makes two attempts to recover the failed CCC circuits.

No immediate retry mechanism is attempted on the non-signaling dedicated trunks or lines of failed CCC circuits. However, the USNBD audit attempts to recover all types of dedicated CCCs.

If the CCC circuit of a combined CCR fails when the CCR is assigned to a monitored call, call content is no longer delivered. If one of the CCC circuits of a paired CCR fails when the CCR is assigned to a monitored call, the remaining CCC circuit continues to deliver call content to the LEA, but only half of the call content is delivered.

Log UNB303 is generated to report failure of a CCR (refer to Chapter 5 “Log reports” for details).

Delivering monitoring information

Monitoring information from a monitored call is formatted into messages, which are delivered to the LEAs over CDCs. (For details on the CDC messages, refer to Chapter 2 “CDC messages”.)

Creation of a CDC

An authorized USNBD user creates a CDC using the CDC ADD command.

Association of a CDC

When an LEA requires monitoring information for monitored calls, an authorized USNBD user runs the CDC ASSOC command to associate a CDC with a surveillance. The CDC agency must be the same as the surveillance agency. The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights.

Different surveillances for the same agency can share the same CDC.

Delivery of monitoring information to the LEA

The delivery mechanisms available for delivery of CDC messages include X.25 and Frequency Shift Keying (FSK) on a dedicated POTS line.

US Network Broadcast Delivery

FSK delivery supports three access types:

- dedicated
- switched local
- switched remote

After an **X.25** CDC is associated with the first surveillance, a switched virtual circuit (SVC) is created, and all monitoring information for that surveillance and other surveillances (if any) is delivered to the LEA using the CDC over a point-to-point facility.

After a **dedicated** FSK CDC is associated with the first surveillance, the local DN is called by the switch.

A **switched local** FSK CDC is not initially called by the switch until the surveillance to which it is associated is activated. After the surveillance is activated, a call to the local DN is made and the surveillance status message is delivered to test the FSK resources. USNBD will not attempt to recover switched CDCs after they are taken down (go on hook, restart, etc.) until the next call-related message is to be delivered. This allows a collection facility to take the CDC down after not receiving any messages for a defined period to save resources.

Prior to SN06, FSK functionality was provided using software patches.

Disassociation of a CDC

An authorized USNBD user disassociates a CDC from a surveillance using the CDC DISASSOC command. The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights. Once the CDC is disassociated from its last surveillance and all the CDC messages have been sent, the SVC on the CDC is released.

Deletion of a CDC

An authorized USNBD user deletes a CDC using the CDC DEL command. The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights.

Failure of a CDC

When a CDC link fails, any messages that are generated are placed in the audit message queue. The audit, which runs every 15 minutes or less if required, re-queues the messages for retransmission and makes an attempt to re-establish the CDC. If the messages cannot be sent the second time, they are

again placed in the message queue for retransmission. If the messages cannot be sent on the third attempt, they are discarded.

Log UNB301 is generated to report failure of a CDC (refer to Chapter 5 “Log reports” for details).

> ***Note:*** The LEA can receive CDC messages out of order with respect to the time they are generated. This applies to messages that are re-queued and sent at a later time.

Monitoring calls

After an authorized USNBD user sets up a surveillance on a subject and activates the surveillance through the SURV ACT command, any calls made or received by that subject are monitored. If a surveillance is activated while calls related to this surveillance are in progress, these calls are not monitored. Only calls made or received by the subject after the subject has become idle are monitored.

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

If an authorized USNBD user deactivates a surveillance through the SURV DEACT command while calls to or from the subject are in progress, monitoring on those calls stops immediately.

After the surveillance is deactivated, no more CDC messages related to the calls in progress are sent to the LEA, unless any were queued prior to the deactivation of the surveillance.

FSK transport

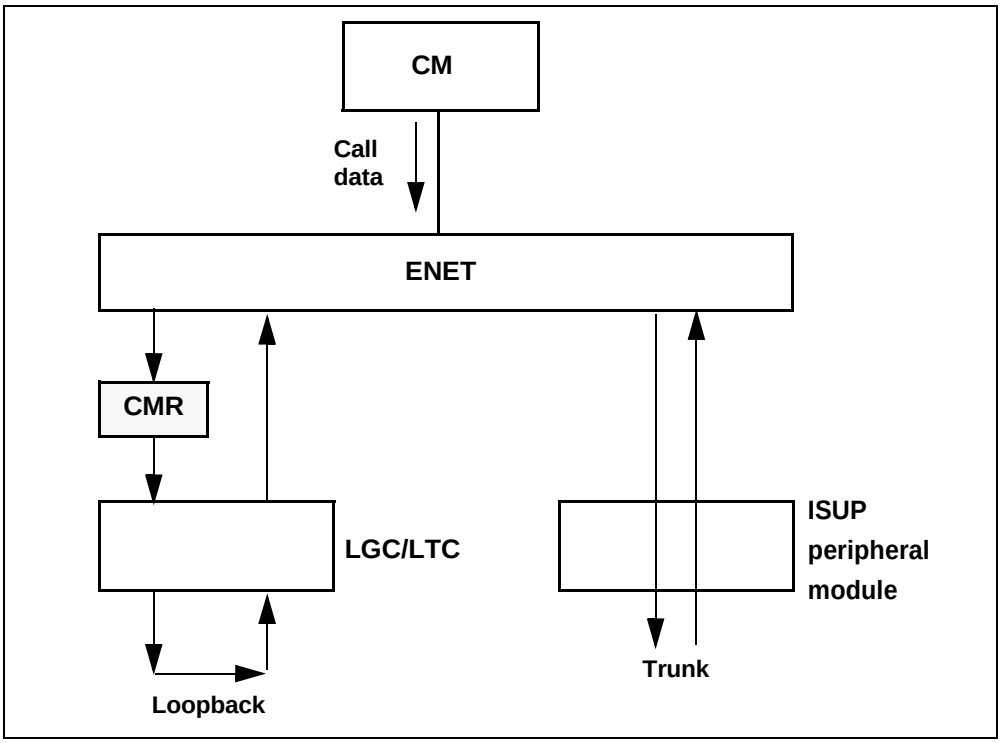
SN07 introduced the delivery of switched remote FSK messages using dedicated POTS lines. Data is sent from the CM, through a Custom Local Area Signaling Services (CLASS) modem resource (CMR) card in an LGC or LTC peripheral module. A P-side looparound is then used to forward the messaging data via the outgoing trunk to the LEA. Refer to the block diagram, Figure 1-5, "Use of CLASS modem resource card in digital trunk controller".

FSK is a method of converting digital data into its analog equivalent. Information is passed by varying the signal frequency (a high frequency represents a 1 and a low frequency represents a 0). The CMR card performs the digital-to-analog conversion using FSK. The CMR card generates Pulse Code Modulation (PCM) samples of 202 modem signals, based on messaging

US Network Broadcast Delivery

from the XPM signaling processor. These samples are passed on to the line card in the Line Concentrating Module (LCM), where they are converted to analog modem signals and sent along the loop to the CLASS subscriber. The CMR card normally provides such CLASS services as Calling Name Display, Calling Number display, etc.

Figure 1-5 Use of CLASS modem resource card in digital trunk controller



This method supports Equal Access calls to trunk CDCs and switched CCRs to agencies. ISUP IT and ATC trunks with FGD signaling may be used.

The use of FSK messaging requires SOC options NBD00003 and NBD00004. To create a switched remote FSK CDC circuit, the following conditions must also be present:

- At least one LGC or LTC XPM, running load QLI17AY1 or higher, must be present and have an in-service CMR card.
- The terminating line (which is connected to the modem and the personal computer which decodes the CDC messages), must have a cut-off on disconnect feature (COD for Nortel equipment) which allows the line to be idled if the trunk is released. If this feature is not present, the modem

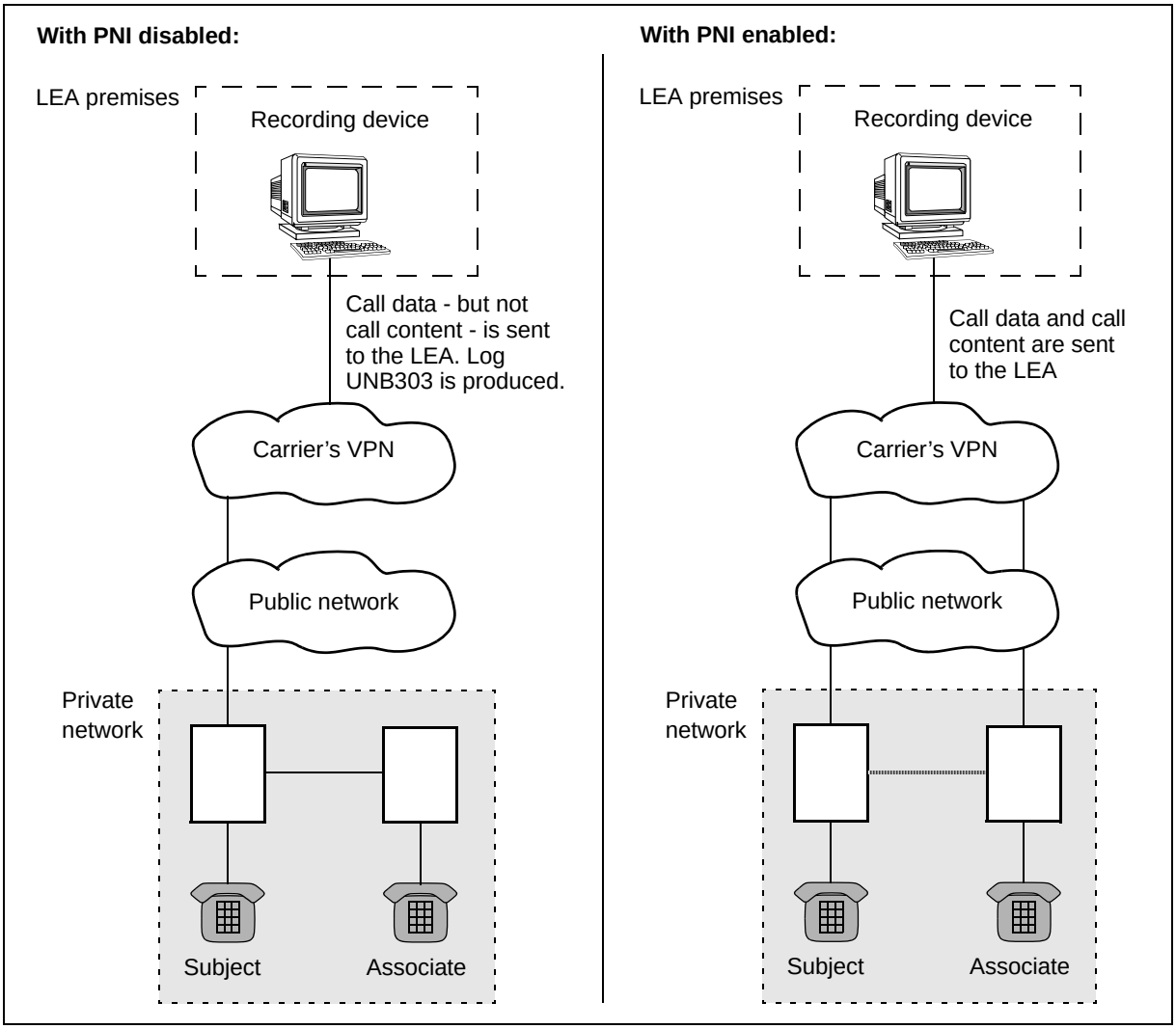
US Network Broadcast Delivery

will remain offhook, and put the line in a busy or lockout state until the modem is released manually.

Intercepting calls within private networks

SN07 introduced a means of intercepting calls made between parties who use a private network. The method is called Private Network Interception (PNI) and requires the service provider's cooperation to transfer subject calls to the public network where they can be monitored. Figure 1-6 illustrates the interception of calls within a private network.

Figure 1-6 Private network interception



US Network Broadcast Delivery

To set up PNI functionality on a surveillance, specify “Y” for the PNI parameter in the “SURV ADD” command. Calls between agents in a private network may then be intercepted. (The LEA must inform the private network service provider that the content of calls on the private network will be intercepted.)

If a call is intercepted and PNI functionality is disabled, call data message “CCUnavailable” (as described in Chapter 2 “CDC messages”) is sent to the LEA, indicating that call content is not available. Log UNB303 is also produced.

DMS switch processes used for USNBD

To operate, USNBD requires the following processes in the DMS switch:

- NBDAUDIT, which verifies the integrity of all USNBD data, flags any problems and reacts accordingly (see “Making changes to datafill” on page 1-35)
- FBSX25, which encodes CDC messages that have been generated, and sends these messages to the LEA
- NBDRCVRY, which attempts to recover from a restart, switch of activity (SWACT), or one-night process (ONP), in particular, attempts to re-establish calls to CCRs

If the NBDAUDIT or FBSX25 process ends unexpectedly once or twice within a five-minute period, USNBD attempts to recreate the process. However, if either process ends unexpectedly a third time within 5 min., USNBD does not attempt to recreate the process.

Failure of the NBDAUDIT process can impact call processing of a subject’s calls, call content delivery, and monitoring information delivery.

When the FBSX25 process is not running, CDC messages are queued (until the queue is full), but are not sent to the LEAs. When the process is re-created, all the messages in the queue are sent to the LEAs.

> ***Note:*** Failure of the FBSX25 process neither impacts call content delivery, nor activation or deactivation of monitoring.

The NBDRCVRY process runs after a restart, SWACT, or ONP and terminates after having recovered all CCRs. If the NBDRCVRY process terminates before recovering all CCRs, USNBD does not attempt to recreate the process. The NBDAUDIT attempts to recover the CCRs the next time it runs.

US Network Broadcast Delivery

Note: All three processes are recreated following a restart.

Packet Data Call monitoring

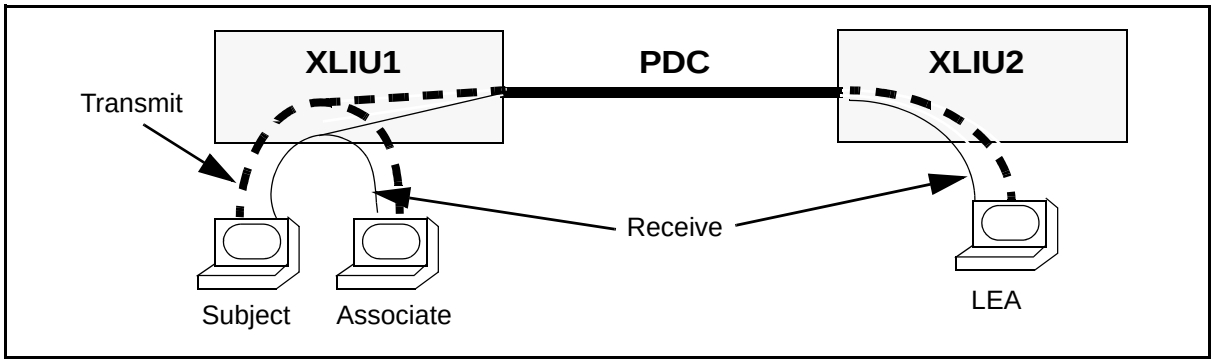
Packet Data Interception and Delivery overview

Data call content is replicated and delivered logically over a Packet Call Content Resource (Packet CCR) and physically over one or more transport facilities.

Delivery of intercepted packet data to the LEA requires the establishment of Packet Data Channels (PDCs), which is a set of two Permanent Virtual Circuit (PVC) endpoints (one for the data transmitted by the subject, and the other for data received by the subject), and the connection of these endpoints to the intercepted data signals transmitted and received from the subject.

The Intercept Access Point (IAP) for packet data interception is within the X2575 Link Interface Unit (XLIU), to which the subject's Data Terminal Equipment (DTE) is nailed-up. The PDC endpoints are ISDN BRI nailed-up connections to a XLIU (not necessarily the same XLIU as the subject, but a XLIU hanging off the subject's switch). When packets are intercepted, they are delivered to the authorized LEA through the PDC terminated at the LEA's DTE. This feature only addresses the interception of packet data on the internal packet handler (the XLIU); it does not allow for the interception of packet data on the DPN-100.

Figure 1-7 Overview of Packet Data interception and delivery



Packet Data Channels

Packet Data Channels (PDCs) represent logical channels that are internal to USNBD. A PDC is represented in USNBD by a set of two endpoints, which in turn refer to a physical facility on the subject's switch, called PVC circuits. These endpoints can either be a set of two DN/Logical Channel Number (LCN) or Trunk Common Language Location Identifier (CLLI)/external number/LCN.

US Network Broadcast Delivery

Packet Data Channel provisioning

Provisioning a PDC for use with USNBD can be broken down into four steps:

1 Installing and provisioning the PVC circuits

2 Defining a DN or trunk for the PVC circuits

3 Defining the PDC using the endpoints of its PVCs

4 Associating the PDC with a surveillance

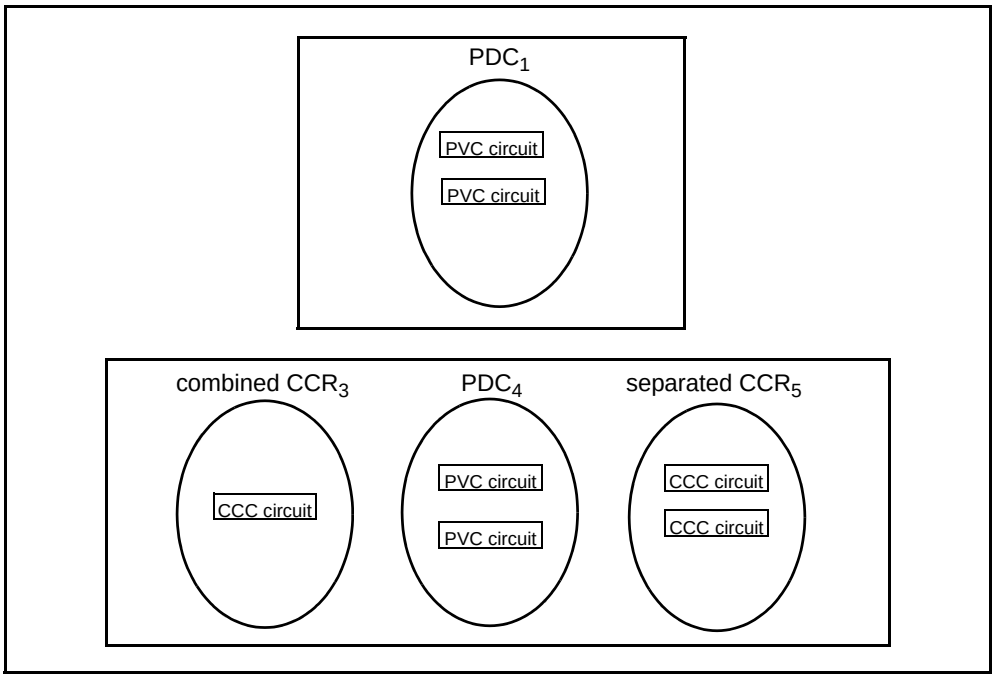
A PVC circuit is an ISDN BRI facility capable of D-packet or B-packet mode communication. It must be installed, provisioned, and assigned a DN or trunk CLLI (depending on the required endpoint) before it can be used by USNBD for packet data interception.

PDCs are defined using the CCR ADD command. The only delivery method for PDCs is separated. A PDC can either be defined using DN endpoints or trunk CLLI endpoints. The PDC is composed of two endpoints, the first endpoint for the transmission of data from the subject and the second for the reception of data by the subject.

PDCs are associated with a surveillance by the CCR ASSOC command. A surveillance can either have zero or one PDC associated with it. However, if the subject is capable of both voice and data calls, the traditional voice CCRs (up to a maximum of four) can be used in conjunction with the PDC, for a total of five CCRs associated with a given surveillance.

All the PDCs associated with a given surveillance are uniquely associated with that surveillance. They cannot be associated with another surveillance until the association with the first surveillance is removed. Figure 1-8 illustrates a PDC associated with a surveillance, and a combination of both voice CCRs and a PDC. The CCRs associated with a surveillance need not be of the same type. PVC endpoints are provisioned in pairs, similar to how the provisioning of separated CCCs is done. The provisioning of independent separated PVC endpoints is not supported.

Figure 1-8 CCRs associated with a surveillance



Packet Data Channel processing

Each operation on a PDC is translated into operations on the PVCs comprising the CCR, which in turn are translated into operations on the PVC circuits of the PDC. There are no independent operations on the individual PVC circuits of a PDC; the PVC circuits are operated as a pair.

In a fully operational PDC, the PVC circuits are synchronized, both being in the same state. However, if a failure occurs on one PVC circuit, the PVC circuits may no longer be synchronized. In this case, operations on the PDC continue to be translated into operations on the still functioning PVC circuit, if any.

A PDC may be in one of three states, UNASSOCIATED, ASSOCIATED-ACTIVE, or ASSOCIATED-INACTIVE. The UNASSOCIATED state is created when the CCR ADD command is issued for a PDC. USNBD commands are entered to move the PDC through the state transitions described in Table 1-4 "PDC state transitions" and shown in Figure 1-9 “PDC state transition diagram” on page 1-29.

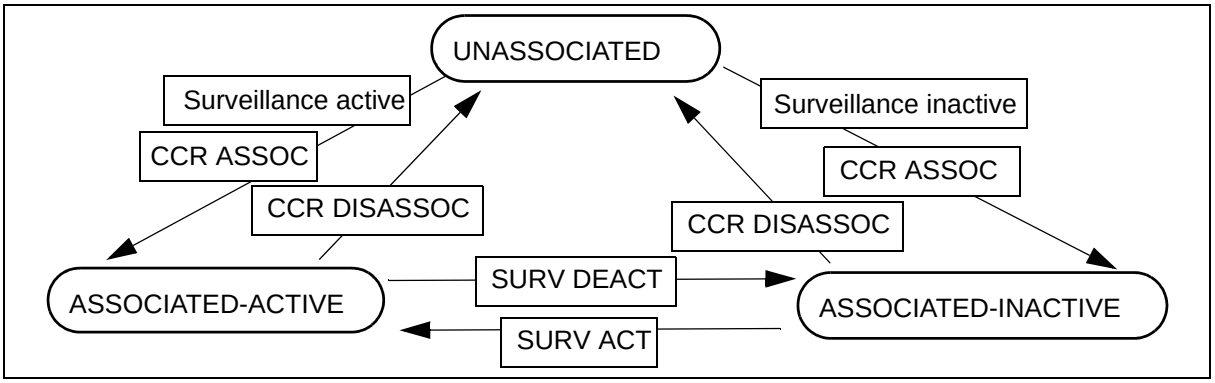
US Network Broadcast Delivery

A PDC may be in one of three states, as shown in the following table:

Table 1-4 PDC state transitions

PDC state	USNBD command	Surv-eillance status	Resulting state transition	Resulting PVC circuit state
UNASSOCIATED The PDC is defined, but is not associated with a surveillance	CCR ASSOC	Active	ASSOCIATED - ACTIVE	A call is established to each of the PVC endpoints. CCOpen messages (one for each PVC) are sent to the LEA and delivery of intercepted data begins.
	CCR ASSOC	Inactive	ASSOCIATED - INACTIVE	A call is established to each of the PVC endpoints. Delivery of intercepted data does not begin, as the surveillance is not active.
ASSOCIATED - INACTIVE The PDC is associated with an inactive surveillance	SURV ACT	Inactive	ASSOCIATED - ACTIVE	CCOpen messages (one for each PVC) are sent to the LEA and delivery of intercepted data begins.
	CCR DISASSOC	Inactive	UNASSOCIATED	The calls to the PVC endpoints are taken down.
ASSOCIATED - ACTIVE The PDC is associated with an active surveillance	SURV DEACT	Active	ASSOCIATED - INACTIVE	CCClose messages (one for each PVC) are sent to the LEA and data interception ends. The calls to the PVC endpoints are not taken down.
	CCR DISASSOC	Active	UNASSOCIATED	CCClose messages (one for each PVC) are sent to the LEA and data interception ends. The calls to the PVC endpoints are taken down.

Figure 1-9 PDC state transition diagram



The following two figures illustrate the connections between the receive and transmit channels of the subject and associate and how packets are copied to the LEA when the PDC is in an ASSOCIATED - ACTIVE state.

Figure 1-10 PDC in ASSOCIATED - INACTIVE state

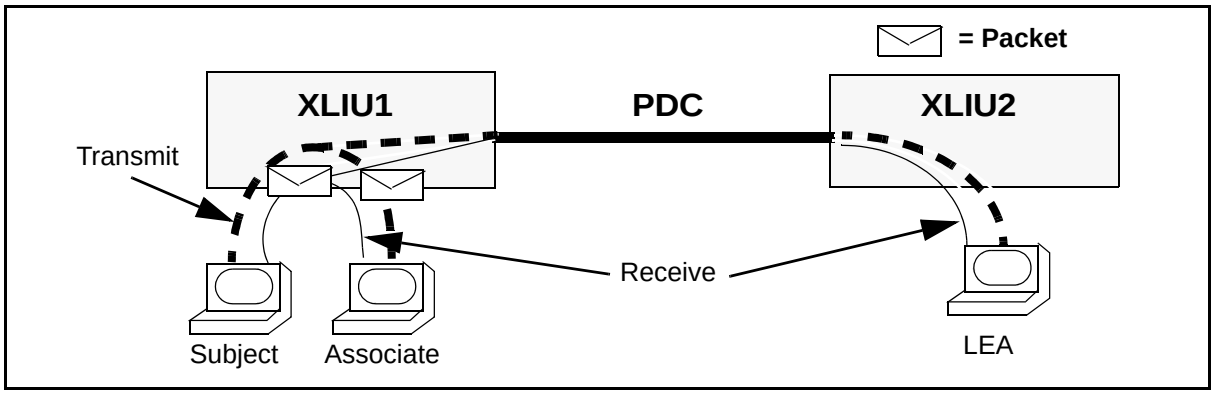
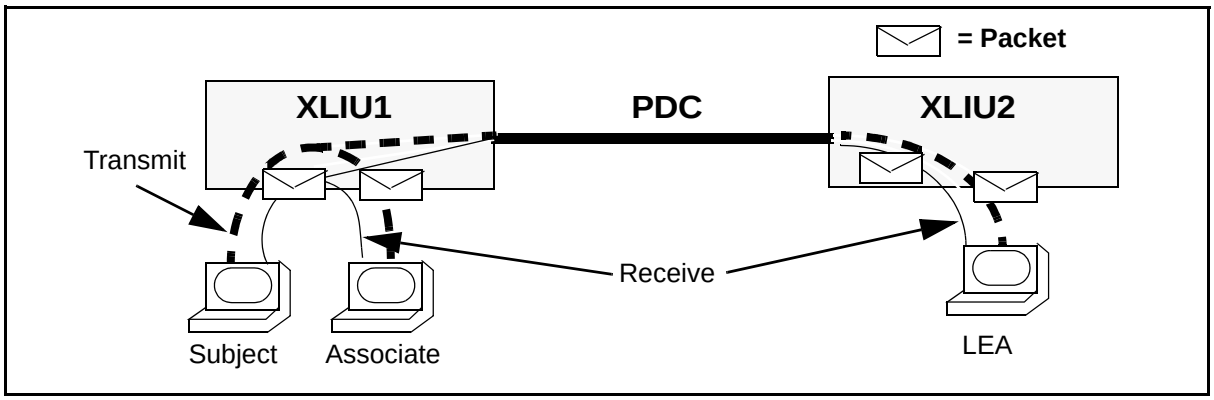


Figure 1-11 PDC in ASSOCIATED - ACTIVE state



US Network Broadcast Delivery

PDC surveillance functions only if the subject's LTID is attached to hardware. If the subject's LTID is not attached to any hardware the state transitions are identical, but calls are not established with the PVC endpoints, intercepted data is not delivered, and CCOpen or CCClose messages are not sent to the LEA.

Intercepted data call content

The intercepted packets are encapsulated in a PDC Envelope message and sent to the LEA's endpoints.

Packet segmentation

The maximum packet size permitted in the XLIU is 256 bytes. The size of the PDC Envelope message will exceed this maximum if the size of the intercepted packet is greater than 193 bytes. In this case, the packet will be segmented into two packets. The first packet will be 256 bytes. The M bit (More bit) in the first packet's header is set to indicate that it is only part of a full packet. The second packet contains the remaining contents of the intercepted packet.

Packet loss

A buffering mechanism for intercepted packets has been created to minimize packet loss. The following list describes situations where packet loss can occur:

- The LEA DTE sends a Receiver Not Ready (RNR) packet indicating that it is not ready to receive data while packets are being intercepted from the subject's transmit and receive channels.
- The physical link between the subject's switch to the LEA is unstable, which results in many retransmissions.
- The LEA DTE is slow in acknowledging packets which are intercepted and sent, which results in the transmit window becoming full.

Failure of a Packet Data Channel

When a PDC is associated with a surveillance and a PVC circuit fails, the following events will occur:

- a UNB303 log is generated indicating the failure of the PVC circuit
- if the surveillance was active, a CCClose message is generated for the failed PVC circuit

If one PVC fails, the other will continue to deliver data. The functioning PVC will not deliver data that was intended for the failed PVC.

US Network Broadcast Delivery

PVC endpoints

To function as a USNDB PVC endpoint, a line must have a non-ambiguous 10-digit DN, and be an ISDN BRI line capable of D-channel or B-channel packet switched data calls.

To function as a USNDB PVC endpoint, a trunk must be an outgoing X.75 trunk.

Monitoring information delivery

CDC message set for Packet Data monitoring

The USNBD feature generates messages that are sent on the CDC to deliver the appropriate monitoring information.

These CDC messages are used to deliver call-identifying information as well as non-call-identifying information. The following CDC messages are associated with packet data monitoring:

- CCClose - reports the release of a PVC
- CCOpen - reports the assignment of a PVC
- Surveillance Status - reports the activation or deactivation of a surveillance

  Note: No other CDC messages are generated during the monitoring of a packet data call.

CCOpen parameter changes

The CCOpen message contains a new parameter, PDUType, which is used when a packet call is being monitored. This parameter is used to identify the type of packet data units being intercepted.

Packet Data Call monitoring

For packet data call monitoring, a surveillance must be defined, using the SURV ADD command, on a Logical Terminal IDentifier (LTID) capable of performing packet mode communication. The AGENCY parameter is prompted only for an administrative user, who can add any surveillance. For non-administrative users, the user's agency is taken as the surveillance agency and the user is not prompted for this parameter.

When defining a surveillance, an option is provided for allowing Monitored Replacement Party (MRP). If the surveillance is being used for packet mode surveillance, the MRP option may be set, but will have no effect as MRPs are not supported when performing packet mode surveillance.

US Network Broadcast Delivery

Activation of monitoring for Packet Data

Packet data monitoring begins when the SURV ACT command is issued. CCOpen messages, reflecting the PVCs, are generated. The USNBD user activating the surveillance must be associated with the same agency as the surveillance or have USNBD administrative rights.

Deactivation of monitoring for Packet Data

Packet data monitoring stops when the SURV DEACT command is issued and the corresponding CCClose messages, reflecting the PVCs, are generated. The USNBD user deactivating the surveillance must be associated with the same agency as the surveillance or have USNBD administrative rights.

USNBD data integrity for Packet Data monitoring

USNBD uses data from different sources that when changed, may affect the integrity of USNBD data. For example, a packet surveillance may have been defined on a particular LTID. If the LTID is deleted by a SERVORD command, the surveillance becomes invalid.

When datafill changes are communicated to USNBD as they occur, USNBD reacts immediately. The following list describes events affecting packet mode surveillance where immediate actions are performed:

- **Detaching an LTID -** The following table describes the actions performed by USNBD when a subject's LTID is detached from hardware using the SLT DET SERVORD command.

Table 1-5 Actions performed when an LTID is detached

PDC state	Actions taken
UNASSOCIATED	Nothing is done in this state, as the PDC is not associated with a surveillance.
ASSOCIATED - INACTIVE	Calls to the PVC endpoints have been established, but delivery is not activated. When the subject's LTID is detached, the established calls are taken down.
ASSOCIATED - ACTIVE	Calls to the PVC endpoints are established and the delivery of intercepted packet data is active. When the subject's LTID is detached, delivery of packet data stops and the calls to the PVC endpoints are taken down. CCClose messages (one for each of the PVCs) are sent to the LEA, indicating delivery of packet data has stopped.

- **Attaching an LTID -** The following table describes the actions performed by USNBD when a subject's LTID is attached to hardware using the SLT ATT SERVORD command.

Table 1-6 Actions performed when an LTID is attached

PDC state	Actions taken
UNASSOCIATED	Nothing is done in this state, as the PDC is not associated with a surveillance.
ASSOCIATED - INACTIVE [1]	When the subject's LTID is attached to hardware, USNBD reacts by establishing the calls to the PVC endpoints. If there is a failure establishing the calls to the endpoints, the following occurs: - the CCR is disassociated from the surveillance - a UNB303 log is generated for the defective CCR - a UNB304 log is generated pertaining to the surveillance the defective CCR was disassociated from
ASSOCIATED - ACTIVE	When the subject's LTID is attached to hardware, USNBD reacts by establishing the calls to the PVC endpoints, activating the delivery of intercepted packet data, and by sending CCOpen messages (one for each of the PVCs) to the LEA, indicating delivery has started. If a failure occurs in the establishment of the calls to the PVC endpoints or if delivery could not be started, the following occurs: - the CCR is disassociated from the surveillance - a UNB303 log is generated for the defective CCR - if the defective CCR was the only monitoring resource associated with the subject, the surveillance is deactivated - a UNB304 log is generated pertaining to the surveillance the defective CCR was disassociated from

- **Moving an LTID -** The SLT MOVE SERVORD command is a combination of one detach and one attach event. USNBD reacts as indicated in Detaching and Attaching an LTID above.
- **Removing an LTID -** When a LTID is removed using the SLT REM SERVORD command, the LTID has already been detached and the PDC

US Network Broadcast Delivery

has been brought down. USNBD reacts by deleting the surveillance and disassociating any existing CCRs or CDCs. A UNB304 log is generated indicating the deletion of the surveillance.

Inband Digit Collection

Inband digits refer to a subject's post full cut-through dual tone multi frequency (DTMF) digits. These are the digits dialed by the subject when a call is connected to another telecommunication service provider's (TSP) switch for processing and routing. These digits are not processed by the subject's local switch. If a CCR is associated with the surveillance, these digits are heard over the CCR as distinct tones.

In a post full cut-through condition, any digits dialed by the subject are considered as inband digits, whether or not they are used for translations and processing by another TSP's switch.

Inband Digit Collection allows the monitoring and delivery of the subject's post cut-through DTMF digits, capturing calls that terminate to a subject. An InbandDigit CDC message is generated for the LEA as soon as the inband digits are available to the call data intercept access point (CDIAP) on a monitored call.

The digit receivers attached to capture the inband digits on an IDC call will report them to the CDIAP when one of the following events occurs:

- Elapsed time between two digits dialed by the subject exceeds a predetermined value called inter-digit timer. This value is set to 10 s.
- number of digits buffered exceed 15 digits
- monitored call ends or is put on hold

Management of digit receivers

A digit receiver is allocated only when a subject originates a call or a call terminates on the subject. It is freed as soon as the call ends. If a digit receiver cannot be immediately allocated, the inband digits are not captured.

The management of the receiver is similar to a CCR. If a CCR is associated with a surveillance, the CCR would be connected/disconnected, as would the receiver be connected/disconnected. The inband digits delivery functionality is available only for the subject. The inband digits delivery always stops when the subject is replaced. For example, inband digits of a Monitored Replacement Party (MRP) are never captured.

Note: It is not necessary for a CCR to be associated with a surveillance for inband digits to be reported.

A digit receiver is attached to a subject if any of the surveillances associated with the subject has inband delivery activated. The inband digits are reported only to that surveillance. A single digit receiver is attached to the subject when the inband delivery is activated and the subject has multiple surveillances. The inband digits are reported to all the surveillances associated with the subject having the activated inband delivery.

A digit receiver attached to an IDC call is released within 12 seconds of a monitored call going down. The delay is introduced to ensure that any digits received by the receiver, just as the monitored call goes down, are reported to the CM before the receiver is released.

Modifications to USNBD setup process

To ensure inband digit delivery, one new exec_lineup defined by this feature, MTM1EX, needs to be downloaded to MTMs which host the digit receivers. An exec_lineup is a logical set of exec IDs which can be used as a group to perform tasks needed to originate, handle and supervise a call for a given peripheral type. Up to 254 exec IDs may be placed in a given exec_lineup. The downloading of an exec_lineup to the MTMs needs to be done as part of the USNBD setup process to ensure that inband digits delivery functionality works properly.

Refer to Chapter 8 “USNBD administrator and user procedures” and follow the procedure “Ensuring inband digits delivery”.

Making changes to datafill

Some datafill changes, for example, deleting a DN, can affect the integrity of USNBD data, therefore, an audit (NBDAUDIT) runs every 15 minutes or less if required, to verify the integrity of USNBD data. Any changes that affect USNBD data are flagged by this audit to allow USNBD to handle the changes.

Datafill changes that affect the integrity of USNBD data are provided below with the action USNBD takes to handle the change. For details on the log reports that are generated, refer to Chapter 5 “Log reports”. For details on data schema tables related to USNBD, refer to Chapter 6 “Data schema”.

- If data for a monitored DN, LEN, KEY, or LTID is changed, for example, the line is deleted, a non-monitorable feature is added to the line, or the line is changed to a non-monitorable type of line, USNBD automatically

  — generates log UNB304

US Network Broadcast Delivery

— deactivates the surveillance if the surveillance is active

— disassociates any CCRs and the CDC from the surveillance

— deletes the surveillance

- If data for a CDC is changed, for example, the MPC link is removed, USNBD automatically

  — generates log UNB301 for the affected CDC

  — deactivates the surveillances to which the CDC is associated, but only if no CCRs are associated with the surveillances, in which case the surveillance is not deactivated

  — disassociates the CDC from all its surveillances

  — generates log UNB304 for each affected surveillance

  — deletes the CDC

- If data for a CCR is changed, for example, the DN of a CCC is deleted, USNBD automatically

  — generates log UNB303 for the affected CCR

  — deactivates the surveillance to which the CCR is associated, but only if no CDC or other CCRs are associated with the surveillance

  — disassociates the CCR from the surveillance if the CCR is associated

  — generates log UNB304 for each affected surveillance

  — deletes the CCR

- If a CI user defined as a USNBD user or a USNBD administrator is deleted, USNBD automatically

  — generates log UNB305

  — deletes the USNBD user or administrator

  Note: If the CI user who was deleted was the last USNBD administrator, contact your Nortel Networks representative.

US Network Broadcast Delivery

Hardware requirements

The USNBD feature does not introduce any new hardware. However, the following existing hardware is required for proper operation of USNBD:

Card	Description
NT1X81AA or NT3X67AA	3-port conference circuit for combined CCRs
NT6X18AA or NT6X18B	type-B line cards for CCC circuits ground-start lines
NT6X17AC or NT6X17BA	type-A line cards for CCC circuits (loop-start and signaling non-signaling lines)
NT6X50AB	DS1 card for non-signaling trunks
NT1X89BA, NT1X89BB or IOM equivalent	multiprotocol controller (MPC) card, or enhanced multiprotocol controller (EMPC) card for X.25 datalinks
NT3X68AB	dual tone multi-frequency (DTMF) digits sender card
NTFX30AA	controller card
NTFX31AA	paddle board
NTFX34AA	MPC card
NTFX4101	IOM shelf
NT22X48AB	dual tone multi-frequency digits (DTMF) sender card

Refer to Chapter 7 “Provisioning USNBD” for advice on how to calculate hardware requirements.

Limitations and restrictions

The following limitations and restrictions apply to USNBD:

- Any lines used as CCC circuits cannot host off a line module (LM), because LMs cannot provide C-tone.
- The USNBD feature does not support call content delivery of announcements or tones, unless the connection to the announcement or tone comes from a trunk.
- When recording a MAP session, the OPENSECRET command can be used to display log information.
- The maximum number of surveillances handled by one XLIU is 256.

US Network Broadcast Delivery

- FSK CDC does not support the assignment of DNs that are remote to the subject switch – that is, trunk delivery is not supported.
- Only five LEAs can monitor a single subject using five PDCs. Each PDC consists of two PVCs: one for carrying incoming traffic to the subject, and the other for carrying outgoing traffic from the subject.
- In SN07, Private Network Interception cannot intercept calls if agents use different switches within the private network. PNI works only if agents share the same switch.

The following limitations and restrictions apply to Inband Digits Delivery functionality:

- When a subject dials inband digits, places the call on hold and retrieves it before the inter-digit timer expires, all the inband digits may not be reported.
- When a subject does not dial post-cut through DTMF digits, no digits are reported to the LEA. A receiver continues to remain attached to the subject.
- If PNI is set to N and the monitored call is behind a private network (call content is not replicated), inband digits may not be collected.
- Once the monitored call goes down, the DTMF receivers remain attached to the subject for about 12 seconds. This is to ensure that any digits dialed by the subject before the monitored call went down and before the inter-digit timer expired, are reported. This refers to a delay in the freeing of DTMF receivers and a delay in their availability for other calls when an IDC call goes down.
- Depending on the sensitivity of the provisioned DTMF receivers, digits dialed by the associate or talk-off can be reported as inband digits. The capturing of inband digits is bound to the limitations and the sensitivity of DTMF receivers (NT2X48AB series cards).

Software optionality control

Software optionality control (SOC) is used to activate and deactivate USNBD.

Prior to activating USNBD, a key code must be obtained from Nortel Networks. The key code is an alphanumeric password that allows an authorized CI user to set the Right-to-Use (RTU) to Yes or No. The RTU is set to No by default, and must be changed to Yes. Once the RTU is set to Yes, the CI user can activate USNBD by changing the state of the USNBD SOC option from Idle to On.

US Network Broadcast Delivery

The state of USNBD is set to Idle by default, which indicates USNBD is available but not functional, and must be changed to ON, which indicates that USNBD is fully functional.

> ***Note:*** To activate USNBD, the CI user must be authorized to use the SOC ASSIGN command as well as the USNBD USER command. Also, for security reasons, it is strongly recommended to create a privilege class specific to USNBD using the PRIVCLAS command, and to assign this privilege class to authorized users using the PERMIT command prior to obtaining the key code and activating USNBD for the first time.

The CI user who activates USNBD for the first time becomes the initial USNBD administrator.

> ***Note:*** It is strongly recommended that the initial USNBD administrator define a second administrator. Having two administrators at all times will avoid having to contact Nortel Networks for further action should the only USNBD administrator be deleted or should this administrator forget their password.

To deactivate USNBD, the state must be changed to Idle. Only a USNBD user with administrator privileges can change the SOC state for USNBD. The state of USNBD can only be changed to Idle once all surveillances, CDCs, and CCRs have been deleted, and all CDC messages have been sent or remain to be sent.

> ***Note:*** The Agency data and the TEST_CALL_BILLNO is deleted when the USNBD SOC is turned IDLE.

Information about SOC for the USNBD feature is provided in the following table:

Feature name	SOC option name	Ordering code
US Network Broadcast Delivery	NANBD	NBD00003, NBD00004
BRI Svcs Ph 1	NI-2/3	NI000050
BRI Svs Ph 2	NI-2/3	NI000051

Refer to Chapter 8 “USNBD administrator and user procedures” for a procedure on activating and deactivating the USNBD SOC option.

US Network Broadcast Delivery

Interactions

The USNBD feature does not affect the functionality of any of the DMS-100 or DMS-500 features with which it interacts. The ISUP Call Control Channels feature introduced in NA015 requires the Agency Separator feature to associate the CCR with an agency.

Service orders

The USNBD feature does not affect SERVORD.

Operational measurements

The USNBD feature created OM groups UNBMISC and UNBCDC, and uses registers in the OM groups CF3P, EXT, and FCNF. For details on the OM groups and registers used by USNBD, refer to Chapter 4 “Operational measurements”.

Logs

The USNBD feature introduces the following log reports:

- TRIG600 reports the generation of UNB300 to UNB304 secret logs
- TRIG700 reports the generation of UNB305 or UNB306 secret logs
- UNB300 reports problems with shared resources and availability of DTMF senders
- UNB301 reports problems with the CDCs
- UNB302 reports problems with USNBD processes
- UNB303 reports problems with the CCRs
- UNB304 reports problems with surveillances and surveillance activation and deactivation
- UNB305 reports problems that affect USNBD administration data and reports all user and administrator creations and deletions
- UNB306 indicates when an STS, PRETRANSLATOR, or LCANAME assigned to an USNBD agency is deleted

For details on these logs, refer to Chapter 5 “Log reports”.

Office parameters

The USNBD feature does not introduce or modify any office parameters.

US Network Broadcast Delivery

Data store

Memory is allocated when the USNBD feature is activated. Memory resources are deallocated when the USNBD feature is deactivated.

User interface

The USNBD feature uses command directory USNBD. Command directories USNBDUSR and USNBDADM which were used in earlier software releases have been deleted.

For details, refer to Chapter 3 “USNBD commands”.

Billing

The USNBD feature does not affect billing. Dedicated lines used as CCCs do not produce billing records. Switched-access lines support remote billable connection to an agency’s recording device. Billing is performed on the basis of call type, which generates a call code 006 (Station Paid) for any toll call toward the agency.

When generating billing records for switched ISUP CCC calls, the billing number specified for the agency is used as the bill number. For TEST calls, the number specified in the USNBD office-wide parameter TEST_CALL_BILLNO is used as the bill number.

One-night process, restarts, and SWACTs

It is recommended that the LEAs be notified prior to performing an ONP.

The USNBD feature fully supports one-night processes (ONP), restarts, and switches of activity (SWACT) with the following limitations:

- When a cold or reload restart is performed, all calls are taken down, therefore, all CCRs are taken down. Once the restart is complete, USNBD attempts to re-establish all CCRs. If a call that is under surveillance is made before an associated CCR is re-established, no call content is delivered for that call. Switched links survive a WARM RESTART but not a COLD or RELOAD RESTART; the links are not re-established when the RESTART completes. Remote links are also affected by any COLD or RELOAD RESTART on tandem switches.
- The maintenance SWACT (MTCSWACT) is recommended for switching activity. MTCSWACT reduces the switch outage time, allowing performance of maintenance tasks that require a restart.
- During a NORESTARTSWACT or RESTARTSWACT, all links are taken down during the LIMITED_PRESWACT.

US Network Broadcast Delivery

- A PM Warm SWACT does not take down the switched links if they were recording. However, any link which has not been answered is taken down.
- When a PM Cold SWACT occurs on a PM which hosts both links to a recording device (paired CCR), the links are taken down. If the two links are hosted by different PMs and a Cold SWACT is performed on one of them, only the link attached to the SWACTed PM will be taken down.
- USNBD will not attempt to recreate the switched links after a PM Cold SWACT.
- During the NBD_PRESWACT step of a SWACT or ONP, all CCRs are taken down, and call content delivery stops on all monitored calls in progress. Once the SWACT or ONP is complete or if the SWACT or ONP is aborted, the dedicated CCRs are set up again, but the switched CCRs are not. Monitoring does not resume for the previous calls, but starts for any new calls.

  Note: Once the NBD_PRESWACT step has started, all USNBD CI commands are disabled. The USNBD CI commands are enabled when the data transfer, recovery, or both have completed or have been aborted.

During an ONP to a subsequent release, all USNBD users (including administrators) are transferred from the old side to the new side even if USNBD is inactive. All surveillance data is transferred from the old side to the new side.

When upgrading to NA15 or subsequent releases, pre-NA015 data will have the link ACCESS type set to dedicated (DE). All CCR, CDC, surveillance, and non-admin user agencies are set to DEFAULT.

Note: In some markets, agency separator is not required and can be overridden. To override, the USNBD administrator gives DEFAULT as the agency name for all USNBD data. When the non-ADMIN USNBD user is created with the agency of DEFAULT, all the USNBD data added by this user has DEFAULT as agency, and any valid USNBD user can view or modify all USNBD data. Using the DEFAULT agency in this manner gives the same behavior as in pre-NA015 for non-administrative USNBD users.

Packet data calls

Packet data call surveillance is affected by system restarts and ONPs as follows:

- During a warm SWACT, only calls in the Data Transfer state survive. All other calls are terminated.

US Network Broadcast Delivery

- All calls are terminated with a cold and reload restart.
- All calls survive an ONP or maintenance SWACT.

US Network Broadcast Delivery

Chapter 2: CDC messages

Overview

During a surveillance, USNBD generates messages that contain monitoring information, and delivers these messages to the Law Enforcement Agencies (LEAs) over X.25 datalinks, referred to as call data channels (CDC) in the USNBD software.

The CDC link is connected to an enhanced multiprotocol controller (EMPC) or a multiprotocol controller (MPC) card, which resides in an input/output controller (IOC) shelf on a DMS switch, and is directly connected through dedicated point-to-point facilities to the LEA.

The messages that USNBD generates are

- Answer
- CCClose
- CCOpen
- CCUnavailable
- Change
- Connect
- Disconnect
- Feature Status
- InbandDigit
- Notification
- Origination
- Redirection
- Release
- Surveillance Status
- TerminationAttempt

Description of messages

The sections that follow describe the CDC messages and their parameters. The parameters in each message are either mandatory (M) or conditional (C). A mandatory parameter is provided in every instance of the message, whereas a conditional parameter is provided only in specific instances of the message.

Answer message

The Answer message is generated when a call leg of a monitored call is answered.

The following table provides the parameters that can be included in the Answer message.

Answer message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CallIdentity`	M	Call identity assigned to the monitored call
`Answering_PartyIdentity`	C	Identity of the party who answered the call, when known. If the party who answered is the subject, this parameter is only included if it is more precise than the subject identity provided by CaseIdentity.
`BearerCapability`	C	Bearer capability granted for the call

CCClose message

The CCClose message is generated when a CCC assigned to a monitored call is released and includes the parameters provided in the following table.

> ***Note:*** Two CCClose messages are generated for a separated CCR, which uses two CCCs. One CCClose message is generated for a combined CCR, which uses only one CCC.

CCClose message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CCCIdentity`	M	Identity of the released CCC, which can include the directory number of the combined CCC, or the directory number of the CCC for the subject or MRP or directory number of the CCC for the associate(s).

CCOpen message

The CCOpen message is generated when a CCC is assigned to a monitored call and includes the parameters provided in the following table.

Note: Two CCOpen messages are generated for a separated CCR, which uses two CCCs. One CCOpen message is generated for a combined CCR, which only uses one CCC.

CCOpen message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CallIdentity` `(voice calls only)`	C	Call identity assigned to the monitored voice call
`CCCIdentity` `(voice calls only)`	C	Identity of the assigned CCC, which can include the directory number of the combined CCC, or the directory number of the CCC for the subject or MRP or directory number of the CCC for the associate(s).
`PDUType` `(data calls only)`	C	Identifies the type of packet data units being intercepted. Values are isdnBchannel, isdnDchannel, ip (internet protocol), ppp (Internet point-to-point protocol), and X25. For ISDN-BRI packet mode interception, the only valid parameters are X25 and isdnDchannel.

CCUnavailable message

The CCUnavailable message is generated if the content is not available for an intercepted call. The message occurs if CCC links could not be established because of a connection failure, or if call content is not accessible because both agents are served by the same private network (see Chapter 1, “Intercepting calls within private networks”).

The following table provides the parameters included in the CCUnavailable message.

CCUnavailable message parameters

Parameter		Description
`CaseIdentity`	M	Identifies the intercept subject
`TimeStamp`	M	Date and time the event was detected
`CallIdentify`	M	Call, call appearance, call leg or session within the system
`UnavailabilityReason`	M	Reason the content was not available

Change message

The Change message is generated when two monitored calls are merged into one or when a call ID is changed.

The following table provides the parameters included in the Change message.

Change message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`Previous_Calls`	M	Call id of the monitored call to be split, or call ids of the monitored calls to be merged
`Resulting_Calls`	M	Call id and assigned CCR of the monitored call that resulted from the merge, or call ids and assigned CCRs of the monitored calls that resulted from the split

Connect

The Connect message is generated when a connection is established between the Network Module (NM) and a peripheral module (PM), between a monitored party (subject or MRP) and an associate or conference circuit. The NetworkConnect message may report the same parties identified in a previous NetworkConnect message for the same call if there was a previous connection between them in the NM of the IAP switch (for example, a subject switch-hook flash).

The Connect message identifies the parties in the connection depending on their appearance in the switch. When a party's appearance is a line, the PartyId parameter identifies the line. When a party's appearance is a trunk, the trunk member number is identified.

Up to 10 PartyIds can be listed in the Connect message if the associate or MRP is a conference circuit.

The following table lists the parameters included in the Connect message.

Connect message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CallIdentity`	M	Call identity assigned to the monitored call
`ConnectedParties`	M	Consists of the following entries
`Calling_PartyIdentity`	M	Identity of the party who made the call. Included when known and when more precise than the identity of the subject provided by the CaseIdentity
`Called_PartyIdentity`	M	Identity of the called party when known

Disconnect

The Disconnect message is generated to report the breaking of a connection in the NM or in a PM between a monitored party (subject or MRP) and an associate or conference bridge.

The following table provides the parameters included in the Disconnect message.

Disconnect message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CallIdentity`	M	Call identity assigned to the monitored call

Feature Status message

The Feature Status message provides LEAs with a list of line options (features) that are assigned to the subject. The line options are listed using the DMS-100 abbreviated name, and do not use Telcordia or operating company service designations.

The following table provides the parameters that can be included in the Feature Status message.

Feature Status message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the call data intercept access point is informed of the event
`FeatureInformation`	M	A list of subject line options (features)

InbandDigit message

The InbandDigit message delivers the inband digits to the LEA as soon as they are available to the call data intercept access point (CDIAP) on a monitored call.

The following table provides the parameters that can be included in the InbandDigit message.

InbandDigit message parameters

Parameter		Description
`CaseIdentity`	M	Identifies the intercept subject
`TimeStamp`	M	Date and time the call data intercept access point is informed of the event
`CallIdentity`	M	Uniquely identifies a call for a given surveillance
`UserInput`	M	Identifies specific user input when it is detected

Notification message

The Notification message provides LEAs with the treatment encountered by the subject, or with an indication of message waiting that is applied towards the subject by the intercept access point (IAP) switch. The Notification message is generated for any surveillance that is active.

The following table provides the parameters that can be included in the Notification message.

Notification message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the call data intercept access point is informed of the event
`CallIdentity`	O	Uniquely identifies a call for a given surveillance
`NotificationInfo`	M	Identifies the treatment or message waiting indication

Origination message

The Origination message is generated when a call attempt is made from the subject.

When a Freephone (Enhanced 800), AIN retranslation, or Speed Call list call is invoked by a subject, a second Origination message is generated by USNBD. This second origination message contains the “translated” information that is received from the SCP or the subject’s speed call list.

The following table provides the parameters that can be included in the Origination message.

Origination message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CallIdentity`	M	Call identity assigned to the monitored call
`Calling_PartyIdentity`	C	Identity of the party who made the call. Included when known and when more precise than the identity of the subject provided by the CaseIdentity.
`Called_PartyIdentity`	C	Identity of the called party when known
`Input`	M	Actual digits dialed by the subject
`TransitCarrier Identity`	C	Identity of the transit carrier for equal access calls
`BearerCapability`	C	Requested (or default) bearer service for the call

Redirection message

The Redirection message is generated when the subject service redirects a monitored call to another party. A Redirection message is not generated when a monitored call is redirected by the associate or MRP service.

The following table provides the parameters that can be included in a Redirection message.

Redirection message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CallIdentity`	M	Call identity assigned to the monitored call
`Redirected-to_PartyIdentity`	M	Identity of the party to whom the monitored call was redirected
`TransitCarrierIdentity`	C	Identity of the transit carrier for equal access calls
`BearerCapability`	C	Requested (or default) bearer service for the call

Release message

The Release message is generated when monitoring ends on a call. Monitoring can end on a call for any one of the following reasons:

Reason	Reason text
the call ended	---
the call was redirected from the subject and became a non-monitorable call	---
a non-monitorable agent became involved in the call	---
the call is being redirected and USNBD does not support this type of redirection or the surveillance has been defined to not provide follow	Follow not supported
a non-monitorable feature was activated on the call	Non-monitored feature ***Note:*** The identification of the feature causing the release of monitoring is identified by a text string or in the form FTRxxx. This feature identification information is the same as that provided in log FTR138.
the surveillance was deactivated	Surveillance deactivated
capacity of monitored calls was reached	Capacity exceeded
the call was routed to treatment	Treatment
the call was redirected, but the surveillance was not defined with a monitored replacement party (MRP)	Follow not supported
a replacement party did not replace the subject, because the subject was re-involved in a call on which monitoring will start	Subject re-involved in call
the subject was on a 2FR line and was talking to the other party on the same 2FR line	Intra 2FR

The following table provides the parameters included in the Release message.

Release message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CallIdentity`	M	Call identity assigned to the monitored call
`Reason`	C	Reason monitoring ended on a call (see “Reason text” above)

Surveillance Status message

The Surveillance Status message reports the activation, deactivation, or update of a surveillance. A Surveillance Status message is generated whenever a surveillance is activated or deactivated, a CCR is associated with an active surveillance, or a CCR is disassociated from an active surveillance. No Surveillance Status message is generated when a surveillance is created or deleted, or when a CCR is associated with or disassociated from an inactive surveillance.

The following table provides the parameters that can be included in the Surveillance Status message.

Surveillance Status message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`SurveillanceStatusType`	M	The change of state made to the surveillance
`AssignedCCCs`	C	The CCRs associated with the surveillance

TerminationAttempt message

The TerminationAttempt message is generated when the subject switch detects an incoming call attempt to the subject’s line, regardless of whether the subject’s line is idle or busy or the call is redirected.

The following table provides the parameters that can be included in the TerminationAttempt message.

TerminationAttempt message parameters

Parameter		Description
`CaseIdentity`	M	Surveillance identification as assigned by the LEA
`TimeStamp`	M	Date and time the message was generated
`CallIdentity`	M	Call identity assigned to the monitored call
`Calling_PartyIdentity`	M	Identity of the calling party when known or allowed. If not know or allowed, the word UNAVAILABLE appears.
`Called_Party_Identity`	C	Identity of the called party when known
`BearerCapability`	C	Requested (or default) bearer service for the call
`RedirectedFromInformation`	C	Information about any previous redirections when known, which can consist of the DN of the party who redirected the call to the subject (LastRedirecting), the DN of the original party who was called (OriginalCalled), and the total number of times the call was redirected (NumRedirections).

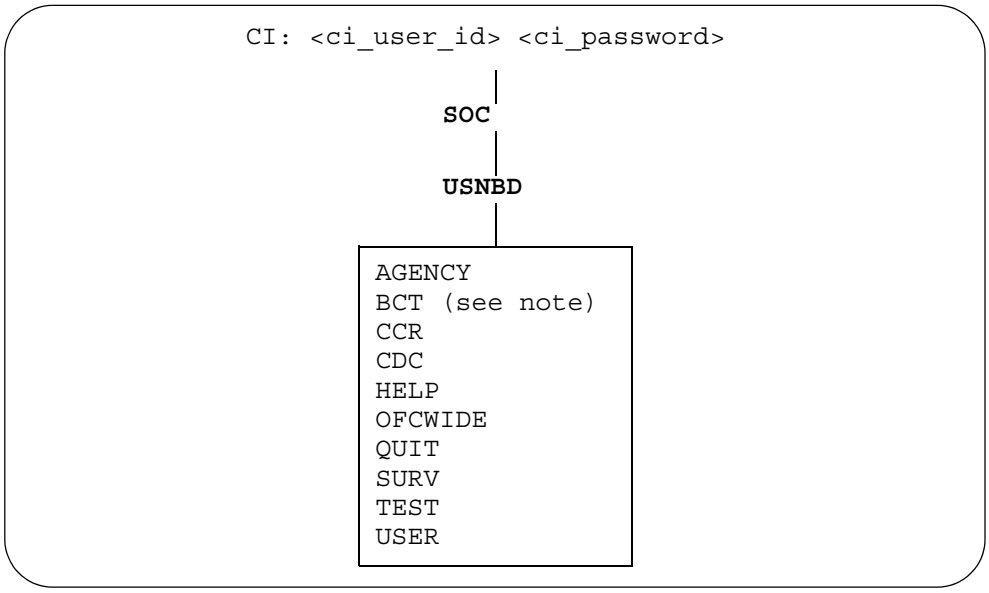
Chapter 3: USNBD commands

This chapter describes the USNBD command directory and provides details on each of the USNBD-specific commands.

The USNBD command directory is accessed from the CI level of a MAP terminal, and allows authorized operating company personnel to set up the USNBD feature, and establish and control surveillance functions.

Figure 3-1 shows the structure of the USNBD user interface and the commands available.

Figure 3-1 USNBD user interface structure



Note: The BCT command is used for voice over IP and should be set up only after following the requirements specified in the Lawful Intercept Product and Technology Fundamentals document (NA) NN10190-113.

USNBD

USNBD

Function

The USNBD command is used to access the USNBD level of the MAP.

This command is available to authorized USNBD users (with or without administrator privileges) at the CI level of the MAP. To enter the USNBD directory level, type USNBD at the CI prompt. To return to the CI level, type QUIT.

At the USNBD command directory, users can:

- add and delete CCRs, display a list of CCRs, and associate CCRs to and disassociate CCRs from a surveillance
- add and delete CDCs, display a list of CDCs, and associate CDCs to and disassociate CDCs from surveillances
- add, activate, deactivate, and delete a surveillance
- add, delete, and display a list of USNBD users (only USNBD users with administrator privileges can execute the USER command)

Command syntax

The USNBD command syntax is as follows:

Command	Parameters
USNBD	none

USNBD - AGENCY

Function

The AGENCY command associates STS, PRETRANSLATOR, LCANAME, and BILLNO with a particular agency. You can use the command to:

- add or delete agency information
- display a list of agencies

This command is available to USNBD users (with or without administrator privileges) at the USNBD level of the MAP.

Command syntax

The AGENCY command syntax is as follows:

Command	Parameters
AGENCY ADD	<agency_name> <STS> <pretranslator> <lca> <billno> <pic> <lata>
AGENCY DELETE	<agency_name>
AGENCY LIST	None

Parameter description

Parameter	Value	Description
agency_name	1 to 16 characters	Identifies the agency having access to switched ISUP CCCs to their remote recording device
billno	10 numbers	The 10-digit billing number used for generating billing record for the switched ISUP CCC call pertaining to the specified agency
lata	alphanumeric	The LATA to use for switched CCRs or FSK switched remote CDCs using equal access dialing to the LEA. If equal access is not required, enter NILLATA.
lca	alphanumeric	Local Calling Area screening name
pic	alphanumeric	The PIC to use for switched CCRs or FSK switched remote CDCs using equal access dialing to the LEA. If equal access is not required, enter NILC.
pretranslator		Pretranslator name
STS		Serving Translation Scheme

USNBD - AGENCY

Usage examples

Usage examples of the AGENCY command

Task	Sample command and output
To add an agency as USER	**>AGENCY ADD agency1 613 p621 l667 1234567890** *MAP response:* AGENCY ADD DONE.
To delete an agency as USER	**>AGENCY DEL agency1** *MAP response:* AGENCY DEL DONE.
To list all agencies in a switch that have access to switched ISUP CCCs	**>AGENCY LIST** *MAP 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.

Usage responses

Usage responses for the AGENCY command

MAP output	Meaning and action
AGENCY FAILED: UNAUTHORIZED COMMAND.	**Meaning:** User is not authorized to use AGENCY command. **Action:** None.

USNBD - AGENCY

Usage responses for the AGENCY command

MAP output	Meaning and action
AGENCY FAILED: USNBD RECOVERY IN PROGRESS, PLEASE TRY AGAIN LATER.	
	Meaning: After a RESTART (cold or reload), USNBD performs some initialization. The AGENCY command cannot be used during that short period of time. **Action:** Try again few seconds later.
AGENCY FAILED: USNBD DATA TRANSFER IN PROGRESS, PLEASE TRY AGAIN LATER.	
	Meaning: A load application is in progress. The AGENCY command is not allowed while USNBD data is being transferred. **Action:** Try again after the load application is completed.
AGENCY ADD FAILED: INTERNAL ERROR.	
	Meaning: USNBD is not able to claim FLAG for executing AGENCY ADD command. **Action:** Try again later.
AGENCY ADD DONE.	
	Meaning: Agency is added successfully with the specified translation data. **Action:** None.
AGENCY ADD FAILED: STS NOT FOUND IN TABLE HNPACONT	
	Meaning: STS specified in the AGENCY ADD command does not exist in table HNPACONT. **Action:** Verify that the user is assigned the correct STS value with the agency through AGENCY command. If the current agency STS is correct, confirm that the value does not exist in table HNPACONT. The user should invoke the operating company procedure to add the missing datafill to the table. Then re-issue the AGENCY ADD command.

USNBD - AGENCY

Usage responses for the AGENCY command

MAP output	Meaning and action
AGENCY ADD FAILED: PRETRANSLATOR NOT FOUND IN TABLE STDPRTCT	
	Meaning: PRETRANSLATOR specified in the AGENCY ADD command does not exist in table STDPRTCT. **Action:** Verify that the user assigned the correct PRETRANSLATOR value with the agency using AGENCY ADD command. If the current agency PRETRANSLATOR is correct, confirm that the value does not exist in table STDPRTCT. The user should invoke the operating company procedure to add the missing datafill to the table. Then re-issue the AGENCY ADD command.
AGENCY ADD FAILED: LCANAME NOT FOUND IN TABLE LCASCRCN OR LCA INFO.	
	Meaning: LCANAME specified in the AGENCY ADD command does not exist in table LCASCRCN or LCA. **Action:** Verify that the user assigned the correct LCANAME value with the agency via AGENCY command. If the current agency LCANAME is correct, confirm that the value does not exist in table LCASCRCN or LCA. The user should invoke the operating company procedure to add the missing datafill to the table. Then re-issue the AGENCY ADD command.
AGENCY ADD FAILED: BILLING NUMBER MUST BE OF 10 DIGITS.	
	Meaning: 10-digit bill number is not specified in the AGENCY ADD command. **Action:** Re-issue the AGENCY ADD command with proper 10-digit bill number.
AGENCY ADD FAILED: AGENCY CAPACITY EXCEEDED FOR SWITCHED ISUP CCCS.	
	Meaning: User is trying to add 9th agency with switched ISUP CCC feature. **Action:** None.
AGENCY ADD FAILED: AGENCY ALREADY EXISTS.	
	Meaning: User is trying to add agency data with similar agency name that already exists. **Action:** None.
AGENCY ADD FAILED: PIC/LATA MUST BE BOTH NIL (NILCAR/NILLATA), OR A VALID CARRIER AND LATA	

USNBD - AGENCY

Usage responses for the AGENCY command

MAP output	Meaning and action
	Meaning: PIC or LATA fields set to incorrect values. **Action:** Try the command with new values for PIC and LATA.
AGENCY ADD FAILED: PIC NOT FOUND IN TABLE OCCNAME **AGENCY ADD FAILED: TABLE OCCINFO - ACCESS FIELD FOR THIS CARRIER IS NOT EAP** **AGENCY ADD FAILED: LATA NOT FOUND IN TABLE LATANAME**	
	Meaning: PIC or LATA fields set to incorrect values. **Action:** Add the agency using new values in the PIC and LATA fields.
AGENCY DEL FAILED: INTERNAL ERROR.	
	Meaning: USNBD is not able to claim FLAG for executing AGENCY DEL command. **Action:** Try again later.
AGENCY DEL DONE.	
	Meaning: Agency data used for translation pertaining to specified agency is deleted. **Action:** None.
AGENCY DEL FAILED: NO MATCHING AGENCY FOUND	
	Meaning: Agency specified in the AGENCY DEL command does not exist. **Action:** Verify that the agency exists using AGENCY LIST command.
AGENCY DEL FAILED: SWITCHED REMOTE FSK CDCS ARE ASSOCIATED	
	Meaning: User attempted to delete an agency with an active surveillance. **Action:** None.
AGENCY LIST FAILED: INTERNAL ERROR.	
	Meaning: USNBD is not able to claim FLAG for executing AGENCY LIST command. **Action:** Try again later.

USNBD - AGENCY

Usage responses for the AGENCY command

MAP output	Meaning and action
`NO MATCHING AGENCY FOUND` `AGENCY LIST DONE.`	**Meaning:** Translation data specific to the agency not found. **Action:** None.

USNDB - CCR

Function

The CCR command is used to

- add or delete call content resources (CCRs)
- associate CCRs to or disassociate CCRs from a surveillance
- display a list of CCRs

This command is available to USNBD users (with or without administrator privileges) at the USNBD level of the MAP. The USNBD user adding, deleting, associating, disassociating, or viewing CCRs must be associated with the same agency as the CCR or have USNBD administrative rights.

For CCR ADD, the parameter AGENCY is prompted only for administrative users. For non-administrative users, the user agency is taken as the CCR agency and the user is not prompted for this parameter.

For CCR DEL, administrative users can delete the CCR for any agency, but non-administrative users can only delete CCRs for their own agency.

The CCR ASSOC command is allowed only if the CCR agency is the same as the surveillance agency. For both CCR ASSOC and CCR DISASSOC, administrative users can associate or disaassociate any CCR. Non-administrative users can only associate or disaassociate a CCR for the user's agency.

For CCR LIST, administrative users will see the agency information for all options. An administrative user can choose to view either a specific agency's information or all agencies' information. Non-administrative users will see only CCRs belonging to the user agency, and agency information is not displayed.

Command syntax

The CCR command syntax is as follows:

Command	Parameters
CCR ADD	**For administrative users:** <index> <ccr_content> <ccr_definition> <ccr_id> <access><signaling> <ccc_tag> <ccr_packet_ definition><agency> **For non-administrative users:** <index> <ccr_content> <ccr_definition> <ccr_id> <access><signaling> <ccc_tag> <ccr_packet_ definition>

USNDB - CCR

Command	Parameters
CCR DEL	<index>
CCR LIST	<option>
CCR ASSOC	<index> <sin>
CCR DISASSOC	<index>

Parameter description

Parameter	Value	Description
access	SW or DE	Specifies the access of the CCR. For switched access, type SW. For dedicated access, type DE.
agency	1 through 16 alphanumeric characters	Specifies the agency of the CCR. This parameter is prompted for if the user executing the command has ADMIN access. When a non-administrative user types the command, the user agency is taken as the CCR agency and the user is not prompted for this parameter.
ccr_content	VOICE or PACKET	Specifies if the CCR is to be used for voice or packet surveillance
ccr_voice_ definition	COMBINED <ccr_id> or PAIRED <ccr_id>	Specifies the type of CCR.
ccr_id (COMBINED)	LINE <10-digit DN> <signaling> or TRUNK <CLLI> <trk_no>	Specifies the type of combined CCC (LINE or TRUNK) and identifies the CCC through two subfields. For LINES, enter the 10-digit directory number. For TRUNKS, enter the CLLI and trunk number for the trunk that is to be used for the CCC.

USNDB - CCR

Parameter description (Continued)

Parameter	Value	Description
ccr_id (PAIRED)	LINE <10-digit DN (CCC1)> <10-digit DN (CCC2)> <signaling> or TRUNK <CLLI (CCC1)> <trk_no (CCC1)> <CLLI (CCC2)> <trk_no (CCC2)>	Specifies the type of paired CCC (LINE or TRUNK) and identifies the CCC through three subfields for lines and four subfields for trunks. For switched LINES, enter the two 10- or 11-digit directory numbers for the CCCs and Y or N to indicate whether signaling is required on these lines. For dedicated LINES, enter the two 10-digit directory numbers for the CCCs and Y or N to indicate whether signaling is required on these lines. For TRUNKS, enter the CLLI and trunk number of the two trunks that are to be used for the CCCs.
signaling	Y or N	Specifies if signaling is enabled on the CCC(s).
ccc_tag	Y or N	Specifies if the delivery of the CCC tag is required for this CCR.
ccr_packet_ definition	LINE 10-digit DN (PVC1) LCN (0 to 4095) PVC1 10-digit DN (PVC2) LCN (0 to 4095) PVC2 or	For lines, PVC1 and PVC2 10-digit DNs specify the DN of the endpoint of the first and second PVCs that are to be used for packet data interception of packets transmitted from the subject. PVC1 and PVC2 LCNs specify the logical channel numbers (LCN) used when setting up the PVC connection to the LEA's endpoint DN.
	TRUNK <CLLI> (PVC1) <trk_no> (PVC1) <LCN> (PVC1) <CLLI> (PVC2) <trk_no> (PVC2) <LCN> (PVC2)	For trunks, enter the CLLI and trunk number of the two trunks that are the endpoints of the first and second PVCs and are used for packet data interception of packets transmitted by the subject. PVC1 and PVC2 LCNs specify the logical channel numbers (LCN) used when setting up the PVC connection to the LEA's endpoint DN.
index	1 through 500	Identifies the CCR.

USNDB - CCR

Parameter description (Continued)

Parameter	Value	Description
option	ALL, ASSOC, UNASSOC, FREE, or AGENCY	Specifies which CCRs to list: • ALL displays all CCRs • ASSOC displays all of the CCRs that are associated with surveillances • UNASSOC displays all of the CCRs that are not associated with surveillances • FREE displays the unused index numbers that can be assigned to new CCRs • The AGENCY option is used only by the administrative user. This is used to list all the CCRs for a particular agency.
sin	1 through 25 alphanumeric characters	Surveillance identification number (SIN), which uniquely identifies the surveillance.

USNDB - CCR

Usage notes

A CCR can be associated or disassociated while a surveillance is active.

The valid DNs differ for dedicated CCRs and switched CCRs as follows:

- For dedicated CCRs, only 10-digit CCC DNs are accepted. Each DN must be a POTS line off the switch hosting the agency recorder.
- For switched CCRs, 10- or 11-digit CCC DNs are accepted. DN1 and DN2 must be distinct for paired CCRs. The DN must not be present on the host switch. Each DN is not required to be a POTS line off the switch hosting the agency recorder.

Usage examples

Usage examples of the CCR command

Task	Sample command and output
To create a paired CCR as USER with signaling dedicated lines and the CCC tag delivery for voice monitoring for user's agency	**>ccr add 2 voice paired line de 4188326520 4183427653 Y Y** *MAP response:* CCR ADD DONE.
To create a paired CCR as USER with signaling dedicated lines and without the CCC tag delivery for voice monitoring for user's agency	**>ccr add 2 voice paired line de 4188326655 4188327652 Y N** *MAP response:* CCR ADD DONE.
To create a combined CCR as ADMIN with a non-signaling dedicated trunk and the CCC tag delivery for voice monitoring	**>ccr add 2 voice combined trunk de trunkgroup1 19 Y AGENCY2** *MAP response:* CCR ADD DONE.

USNDB - CCR

Usage examples of the CCR command (Continued)

Task	Sample command and output
To create a combined CCR as ADMIN with a non-signaling dedicated line and without the CCC tag delivery for voice monitoring	
	>ccr add 2 voice combined line de 4188326655 N N AGENCY1 *MAP response:* CCR ADD DONE.
To add a switched CCR as USER	
	>CCR ADD 1 VOICE COMBINED LINE SW 16136631001 N Y *MAP response:* CCR ADD DONE.
To add a dedicated CCR as USER	
	>CCR ADD 1 VOICE COMBINED LINE DE 6136631001 N Y *MAP response:* CCR ADD DONE
To add a CCR as USER with CCC DN present on host switch	
	>CCR ADD 1 VOICE COMBINED LINE SW 4164631001 N Y *MAP response:* CCR ADD FAILED: SWITCHED CCC DN 4164631001 PRESENT ON THE HOST SWITCH
To create a packet line CCR as USER for user's agency	
	>ccr add packet line 9059631001 1 9059631001 2 *MAP response:* CCR ADD DONE.
To create a packet trunk CCR as USER for user's agency	

USNDB - CCR

Usage examples of the CCR command (Continued)

Task	Sample command and output
	>ccr add 33 packet trunk pt1x75og 1 1 pt1x75og 1 2 *MAP response:* CCR ADD DONE.
To delete a CCR as USER for user's agency	
	>ccr del 2 *MAP response:* CCR DEL DONE.
To delete a CCR as USER for a different agency	
	>ccr del 9 *MAP response:* CCR DEL FAILED: USER AGENCY NOT SAME AS CCR AGENCY.
To delete a CCR as ADMIN	
	>ccr del 9 *MAP response:* CCR DEL DONE.
To associate a CCR with a surveillance as USER, where user's agency is the same as surveillance agency and CCR agency	
	>ccr assoc 2 sin1 *MAP response:* CCR ASSOC DONE.

USNDB - CCR

Usage examples of the CCR command (Continued)

Task	Sample command and output
To associate a CCR with a surveillance as USER, where user's agency is the same as CCR agency, but surveillance agency is different	
	>ccr assoc 2 sin3 *MAP response:* CCR ASSOC FAILED: CCR AGENCY NOT SAME AS SURVEILLANCE AGENCY.
To associate a CCR with a surveillance as ADMIN, where CCR agency and surveillance agency are the same	
	>ccr assoc 2 sin3 *MAP response:* CCR ASSOC DONE.
To disassociate a CCR as USER from a surveillance, where user's agency, CCR agency, and surveillance agency are all the same	
	>ccr disassoc 2 *MAP response:* CCR DISASSOC DONE.
To disassociate a CCR as ADMIN from a surveillance	
	>ccr disassoc 2 *MAP response:* CCR DISASSOC DONE.

USNDB - CCR

Usage examples of the CCR command (Continued)

Task	Sample command and output
To display a list as ADMIN of all CCR indexes	**>ccr list all** *Example of a MAP response:* Index Content CCRtype Acc CCRid CCC1/PVC1 [CCC2/PVC2] [Sig] [Tag] [Sin] Agency ---------- 1 PACKET PAIRED LINE DE 9059631003 19059631003 AGENCY1 2 VOICE PAIRED LINE DE 6135519970 6135519971 Y Y DEFAULT 3 PACKET PAIRED TRUNK PT1X75OG 1 1PT1X75OG 12 AGENCY2 33 VOICE COMBINED LINE DE 6135510102 N Y AGENCY1 66 PACKET PAIRED TRUNK PACKETDATATRK 2 4095 PACKET DATATRK 3 3999 AGENCY3
To display a list as USER of all CCR indexes, where user's agency is AGENCY1	**>ccr list all** *Example of a MAP response:* Index Content CCRtype Acc CCRid CCC1/PVC1 [CCC2/PVC2] [Sig] [Tag] [Sin] ---------- 1 PACKET PAIRED LINE DE 9059631003 19059631003 33 VOICE COMBINED LINE DE 6135510102 N Y

USNDB - CCR

Usage examples of the CCR command (Continued)

Task	Sample command and output
To display a list as ADMIN of all CCR indexes for a specific agency	
	>ccr list agency agency1 *Example of a MAP response:* Index Content CCRtype Acc CCRid CCC1/PVC1 [CCC2/PVC2] [Sig] [Tag] [Sin] Agency ---------- 1 PACKET PAIRED LINE DE 9059631003 19059631003 AGENCY1 33 VOICE COMBINED LINE DE 6135510102 N Y AGENCY1
To display a list as USER of all CCR indexes for a specific agency	
	>ccr list agency default *Example of a MAP response:* AGENCY is not a valid option for USER.

Usage responses

Usage responses for the CCR command

MAP output	Meaning and action
CCCn: DN IS NOT A PACKET AGENT.	
	Meaning: A packet line CCR is being defined and endpoint one (1) is not capable of handling a packet data call. **Action:** Ensure that the DN that is being used as the endpoint in the CCR is capable of making a packet data call. If required, contact the LEA to discuss further action.
CCCn: TRUNK IS NOT AN X75 TRUNK.	
	Meaning: A packet trunk CCR is being defined with a trunk that is not capable of making a packet data call. **Action:** In table TRKGRP, ensure that the trunk being used has a trunk group type of X75.

USNDB - CCR

Usage responses for the CCR command (Continued)

MAP output	Meaning and action
CCCn: TRUNK ENDPOINT IS NOT IN TABLE X75INFO	
	Meaning: The trunk endpoint of the PACKET TRUNK CCR entry cannot be found in table X75INFO. **Action:** Datafill the trunk endpoint in table X75INFO.
CCCn: DN ENDPOINT IS NOT IN TABLE DNCHNL	
	Meaning: The DN endpoint of the PACKET LINE CCR entry cannot be found in table DNCHNL. **Action:** Datafill the DN endpoint in table DNCHNL.
CCCn: ENDPOINT CANNOT HAVE A PVC	
	Meaning: The NPVC option in table DNCHNL is set to zero. **Action:** Change the entry in NPVC (number of PVCs) to a value between 1 and 64.
CCCn: LCN IS OUT OF RANGE	
	Meaning: The LCN provided is out of range. **Action:** Consult table DNCHNL for the values of SLCN (starting LCN) and NPVC. Choose an LCN for the endpoint that is greater than or equal to the SLCN value and less than SLCN + NPVC.
CCR AGENCY NOT SAME AS SURVEILLANCE AGENCY	
	Meaning: The agency of the CCR is different from the agency of the surveillance. The CCR agency must be the same as the surveillance agency. **Action:** None.
CCR ADD DONE.	
	Meaning: The CCR ADD command has been executed successfully, and the specified CCR can now be associated with a surveillance. **Action:** None.

USNDB - CCR

Usage responses for the CCR command (Continued)

MAP output	Meaning and action
`CCR ADD FAILED: SWITCHED CCC DN MUST BE OF 10 OR 11 DIGITS`	
	Meaning: CCC DN(s) specified in the CCR ADD command for switched access type of CCR are not of 10- to 11-digits long. **Action:** Find a new valid remote CCC DN. Replace the local directory number originally entered by the new one. Re-issue the CCR ADD subcommand with the new parameters.
`CCR ADD FAILED: SWITCHED CCC DN <DN> PRESENT ON THE HOST SWITCH.`	
	Meaning: With switched access, CCC DN given as a parameter in the CCR ADD subcommand should not be a local DN. **Action:** Find a new valid remote CCC DN. Replace the local directory number originally entered by the new one. Re-issue the CCR ADD subcommand with the new parameters.
`CCR DEL DONE.`	
	Meaning: The CCR DEL command has been executed successfully, and the specified CCR no longer exists. **Action:** None.
`CCR ASSOC DONE.`	
	Meaning: The CCR ASSOC command has been executed successfully, and the specified CCR is now associated with the specified surveillance. **Action:** None.
`CCR DISASSOC DONE.`	
	Meaning: The CCR DISASSOC command has been executed successfully, and the specified CCR is no longer associated with a surveillance. **Action:** None.
`CCR LIST DONE.`	
	Meaning: The CCR LIST command has been executed successfully. **Action:** None.

USNDB - CCR

Usage responses for the CCR command (Continued)

MAP output	Meaning and action
COULD NOT ESTABLISH PVC CONNECTION.	
	Meaning: The PVC connection between the VLINK and the LEAs endpoint could not be made. **Action:** Ensure that the proper translations are datafilled in order to make a data call to the LEA's endpoint.
INVALID AGENCY NAME	
	Meaning: The agency name entered by the ADMIN exceeds the maximum allowed size of agency. Names should be 16 characters or less. **Action:** None.
NO MATCHING CCR FOUND	
	Meaning: No CCRs match the specified criteria for listing. **Action:** None
PACKET CCR ALREADY ASSOCIATED WITH THIS SURVEILLANCE.	
	Meaning: A packet CCR entry has already been associated with this surveillance. **Action:** Only one packet CCR can be associated with any given packet surveillance. A new surveillance can be defined on the same LTID, and then a second packet CCR can be associated with it.
SUBJECT IS NOT EQUIPPED FOR PACKET MODE DATA COMMUNICATION.	
	Meaning: A packet CCR is being associated with a surveillance that is not capable of performing packet mode communication. **Action:** Verify that the line or trunk specified in the CCR is correct and re-enter the command.
SUBJECT IS NOT EQUIPPED FOR CIRCUIT MODE COMMUNICATION.	
	Meaning: A voice CCR is being associated to a subject that is only capable of packet mode communication. **Action:** Verify that the line or trunk specified in the CCR is correct and re-enter the command.

USNDB - CCR

Usage responses for the CCR command (Continued)

MAP output	Meaning and action
`SURVEILLANCE HANDLE NOT COMPATIBLE WITH A PACKET CCR.`	
	Meaning: A packet CCR is being associated with a surveillance that is not defined on an LTID. When performing packet mode surveillance, the subject must be defined by an LTID. **Action:** Verify that the line specified in the CCR is correct and re-enter the command.
`USER AGENCY NOT SAME AS CCR AGENCY`	
	Meaning: Agency of the user executing the command is different from the agency of the CCR. **Action:** None.
`USER AGENCY NOT SAME AS CCR AGENCY`	
	Meaning: Agency of the user (who executes the command) is different from the agency of the CCR. **Action:** None.

USNBD - CDC

USNBD - CDC

Function

The CDC command is used to

- add or delete call data channels (CDCs)
- associate CDCs to or disassociate CDCs from a surveillance
- display a list of CDCs

This command is available to authorized USNBD users (with or without administrator privileges) at the USNBD level of the MAP. Administrative users can execute these commands on any agency and view information for all agencies. Non-administrative users can add, delete, associate, or disassociate CDCs only for their own agencies.

For CDC ADD, the parameter AGENCY is prompted only for an administrative user. The administrative user can add any CDC. For non-administrative users, the user's agency is taken as the CDC agency and the user is not prompted for this parameter.

For CDC DEL, the admin can delete any CDC. Non-administrative users can only delete CDCs for the user's agency.

The CDC ASSOC command is allowed only if the CDC agency is the same as the surveillance agency. For both CDC ASSOC and CDC DISASSOC, administrative users can associate or disaassociate any CDC provided that the CDC agency and the surveillance agency are the same. A non-administrative user can only associate or disaassociate a CDC for the user's agency.

For CDC LIST, administrative users will see the agency information for all options. An administrative user can choose to view either a specific agency's information or all agencies' information. Non-administrative users will see only CDCs belonging to the user's agency, and agency information is not displayed.

USNBD - CDC

Command syntax

The CDC command syntax is as follows:

Command	Parameters
CDC ADD	**For administrative users:** <index> <transport_protocol> <MPCIndex> <MPCLinkNumber> <address> <protocol1> <protocol2> <protocol3> <protocol4> <agency> **For non-administrative users:** <index> <transport_protocol> <MPCIndex> <MPCLinkNumber> <address> <protocol1> <protocol2> <protocol3> <protocol4> <agency>
CDC ASSOC	<index> <sin>
CDC DEL	<index>
CDC DISASSOC	<sin>
CDC LIST	<option>

Parameter description

Parameter	Value	Description
10-digit DN	string of 10 or 11 digits	Identifies the DN of the FSK SL or DE CDC circuit. For FSK switched remote CDC circuits, the 10- or 11-digit DN must translate to a trunk
access	DE, SL, or SR	Specifies whether the FSK CDC is Dedicated, Switched Local, or Switched Remote
address	string of 1 through 15 digits	Specifies the address to use for the CDC
agency	1 through 16 alphanumeric characters	Specifies the agency of the CDC. This parameter is prompted for if 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.
index	1 through 200	Identifies the CDC
MPCIndex	0 through 255	Identifies the MPC to use for the CDC, which is taken from table MPC

USNBD - CDC

Parameter description (Continued)

Parameter	Value	Description
MPCLinkNumber	0 through 3	Identifies the MPC link to use for the CDC, which is taken from table MPCLINK
option	ALL, ASSOC, UNASSOC, FREE, or AGENCY	Specifies which CDCs to list: ALL displays all CDCs ASSOC displays all of the CDCs that are associated with surveillances UNASSOC displays all of the CDCs that are not associated with surveillances FREE displays the unused index numbers that can be assigned to new CDCs AGENCY is only prompted for administrative users.This is used to list all the CDCs for a particular agency.
protocol1, protocol2, protocol3, protocol4	0 through 255	The CDC X.25 protocol field is mapped to the X.25 Call Request Packet (Call User Data parameter) that is transmitted to the LEA by the command “CDC ASSOC”. Protocol value may also be used by the terminating equipment to identify a specific CDC message stream.
sin	1 through 25 alphanumeric characters	Surveillance identification number (SIN), which uniquely identifies the surveillance
transport_protocol	X.25, FSK, or IP	Identifies the protocol to be used. For FSK, specify the access method using the <access> parameter and specify the 10- or 11-digit DN.

Usage notes

A CDC can be associated or disassociated while a surveillance is active.

USNBD - CDC

Usage examples

Usage examples of the CDC command

Task	Sample command and output
To create a CDC as ADMIN	
	>cdc add 1 X.25 7 2 22222222 3 1 128 0 agency1 *MAP response:* CDC ADD DONE.
To create a CDC as USER	
	>cdc add 1 X.25 7 2 22222222 3 1 128 0 *MAP response:* CDC ADD DONE.
To delete a CDC as USER, where user's agency and CDC agency are the same	
	>cdc del 10 *MAP response:* CDC DEL DONE.
To delete a CDC as ADMIN	
	>cdc del 8 *MAP response:* CDC DEL DONE
To associate a CDC with a surveillance as USER, where user's agency, CDC agency, and surveillance agency are the same	
	>cdc assoc 1 sin1 *MAP response:* CDC ASSOC DONE.
To associate a CDC with a surveillance as ADMIN, where CDC agency and surveillance agency are the same	

USNBD - CDC

Usage examples of the CDC command (Continued)

Task	Sample command and output
	>cdc assoc 1 sin1 *MAP response:* CDC ASSOC DONE.
To disassociate a CDC from a surveillance as USER, where user agency and CDC agency are the same	
	>cdc disassoc sin1 *MAP response:* CDC DISASSOC DONE.
To disassociate a CDC from a surveillance as ADMIN	
	>cdc disassoc sin1 *MAP response:* CDC DISASSOC DONE.
To display a list of all CDCs as ADMIN	
	>cdc list all *MAP response:* Index Type Access CDC DN Agency [Associated SINs] ---------- 1 X.25 7 2 22222222 3 1 128 0 SIN1 SIN2 SIN3 SIN8 AGENCY1 2 6 2 22222222 3 1 128 0 SIN4 SIN5 SIN6 SIN7 AGENCY2 3 FSK SR 16137458239 CSIS CDC LIST DONE.
To display a list of all CDCs belonging to a specific agency as ADMIN	

USNBD - CDC

Usage examples of the CDC command (Continued)

Task	Sample command and output
	>cdc list agency AGENCY1 *MAP response:* Index Type Access CDC DN Agency [Associated SINs] ---------- 1 X.25 7 2 22222222 3 1 128 0 SIN1 SIN2 SIN3 SIN8 AGENCY1 CDC LIST DONE.
To display a list of associated CDCs as USER	
	>cdc list assoc *MAP response:* Index Type Access CDC DN Agency [Associated SINs] ---------- 1 X.25 7 2 22222222 3 1 128 0 SIN1 SIN2 SIN3 SIN8 CDC LIST DONE.
To display a list of all CDCs as USER for AGENCY1	
	>cdc list all *MAP response:* Index Type Access CDC DN Agency [Associated SINs] ---------- 1 X.25 7 2 22222222 3 1 128 0 SIN1 SIN2 SIN3 SIN8 2 FSK SL 6501184726 MI5 CDC LIST DONE.

USNBD - CDC

Usage responses

Usage responses for the CDC command

MAP output	Meaning and action
CDC ADD DONE.	
	Meaning: The specified CDC has been added and can now be associated with a surveillance. **Action:** None.
CDC ADD FAILED: CDC DN ON HOST SWITCH	
	Meaning: An attempt was made to add a switched remote FSK CDC, but the DN resides on the current switch. **Action:** None.
CDC ADD FAILED: NO INSERVICE CMR CARD FOUND **CDC ADD FAILED: NO PHYSICAL CMR CARD DATAFILLED ON ANY PERIPHERAL**	
	Meaning: The CLASS modem resource (CMR) card on the LGC or LTC PM is busy or was not datafilled. **Action:** Confirm that the CMR card is in service and is properly datafilled.
CDC AGENCY NOT SAME AS SURVEILLANCE AGENCY	
	Meaning: Agency of the CDC is different from the agency of the surveillance. **Action:** None.
CDC ASSOC DONE.	
	Meaning: The specified CDC is now associated with the specified surveillance. **Action:** None.
CDC ASSOC FAILED: AGENCY DATA NOT FOUND **CDC ASSOC FAILED: CDC AGENCY NOT SAME AS SURVEILLANCE AGENCY**	
	Meaning: A switched remote FSK CDC has been set up, but the agency has not been added or is the wrong agency. **Action:** Confirm that the agency has been added correctly.
CDC DEL DONE.	

USNBD - CDC

Usage responses for the CDC command (Continued)

MAP output	Meaning and action
	Meaning: The specified CDC no longer exists. **Action:** None.
CDC DISASSOC DONE.	
	Meaning: The specified CDC is no longer associated with the specified surveillance. **Action:** None.
CDC LIST DONE.	
	Meaning: The CDC LIST command has been executed successfully. **Action:** None.
INVALID AGENCY NAME	
	Meaning: The agency name entered by the ADMIN exceeds the maximum allowed size of agency. **Action:** None.
NO MATCHING CDC FOUND	
	Meaning: No CDCs match the specified criteria. **Action:** None.
USER AGENCY NOT SAME AS CDC AGENCY	
	Meaning: Agency of the user (who executes the command) is different from the agency of the CDC. **Action:** None.

USNBD - HELP

USNBD - HELP

Function

The HELP command is used to obtain information on the purpose and the correct syntax of a particular USNBD command.

The HELP command is available to authorized USNBD users (with or without administrator privileges) at the USNBD level of the MAP.

Command syntax

The HELP command syntax is as follows:

Command	Parameters
HELP	<subcommand>

Parameter description

Parameter	Value	Description
subcommand	CCR CDC HELP QUIT SURV USER UNB_OFCWIDE AGENCY TEST	Subcommands at the USNBD level for which help is provided.

Usage notes

The command syntax of the HELP command is provided when either the HELP command is entered without a subcommand, or the HELP command is entered with the HELP subcommand.

The HELP command is available even when USNBD is not activated.

USNBD - HELP

Usage examples

Usage example of the HELP command

Task	Sample command and output
To obtain help information at the USNBD level as a USER	
	>help *MAP response:* HELP INFORMATION Parms: [<SUBCOMMAND> {CCR CDC HELP QUIT SURV USER UNB_OFCWIDE AGENCY TEST}]
To obtain help information about the AGENCY command at the USNBD level as an ADMIN	
	>help agency *MAP response:* MANAGES OR LISTS AGENCY TRANSLATION DATA Parms: <command> {ADD <AGENCY-NAME> STRING <STS> STRING <PRETRANS> STRING <LCA> STRING <BILLNO> STRING <PIC> STRING <LATA> STRING DEL <AGENCY-NAME> STRING LIST}

USNBD - HELP

Usage example of the HELP command

Task	Sample command and output
To obtain help information about the USER subcommand at the USNBD level as an ADMIN	
	>help user *MAP response:* MANAGE OR LIST USNBD USERS Parms: <command> {ADD <user_id> STRING <admin> {N <Agency> STRING, Y} DEL <user_id> STRING LIST <user_list_opt> {ALL, AGENCY <agency> STRING}}
To obtain help information about the TEST command at the USNBD level as a USER	
	>help test *MAP response:* TEST AND VERIFY THE SWITCHED CCC LINKS Parms: <CCR> {1 TO 500}

USNBD - HELP

Usage example of the HELP command

Task	Sample command and output
To obtain help information about the CCR command at the USNBD level as an ADMIN	**>help CCR** *MAP response:* MANAGES OR LISTS CCRs Parms: <command> {ADD <index> {1 TO 500} <ccr_content> {VOICE <ccr_definition> {COMBINED <ccr_id> {LINE <CCC1 -> 10-digit DN> STRING <signaling> {N, Y}, TRUNK <CCC1 -> CLLI> STRING <CCC1 -> trunk number> {0 TO 9999}}, PAIRED <ccr_id> {LINE <CCC1 -> 10-digit DN> STRING <CCC2 -> 10-digit DN> STRING <signaling> {N, Y}, TRUNK <CCC1 -> CLLI> STRING <CCC1 -> trunk number> {0 TO 9999} <CCC2 -> CLLI> STRING <CCC2 -> trunk number> {0 TO 9999}}} <ccc_tag> {N, Y}, PACKET <ccr_id> {LINE <PVC1 -> 10-digit DN> STRING <PVC1 -> LCN> {0 TO 4095} <PVC2 -> 10-digit DN> STRING <PVC2 -> LCN> {0 TO 4095}, TRUNK <PVC1 -> CLLI> STRING <PVC1 -> trunk number> {0 TO 9999} <PVC1 -> LCN> {0 TO 4095} <PVC2 -> CLLI> STRING <PVC2 -> trunk number> {0 TO 9999} <PVC2 -> LCN> {0 TO 4095}}} <Agency> STRING, DEL <index> {1 TO 500}, LIST <ccr_list_opt> {ALL, ASSOC, UNASSOC, FREE, AGENCY <AGENCY> STRING}, ASSOC <index> {1 TO 500} <sin> STRING, DISASSOC <index> {1 TO 500}}
To obtain help information about the CDC command at the USNBD level as an ADMIN	

USNBD - HELP

Usage example of the HELP command

Task	Sample command and output
	>help CDC *MAP response:* MANAGES OR LISTS CDCs Parms: <command> {ADD <index> {1 TO 200} <Transport_Protocol> {X25 <MPCindex> {0 TO 255} <MPClinknumber> {0 TO 3} <address> STRING <protocol1> {0 TO 255} <protocol2> {0 TO 255} <protocol3> {0 TO 255} <protocol4> {0 TO 255}, IP <IPaddress1> {0 to 255} <IPaddress2> {0 to 255} <IPaddress3> {0 to 255} <IPaddress4> {0 to 255} <IPPort) {0 to 32767}, FSK <Access> {SL <10-digit DN> STRING, DE <10-digit DN> STRING, SR <10 or 11-digit DN> STRING}} <Agency> STRING, ASSOC <index> {1 TO 200} <SIN> STRING, DISASSOC <SIN> STRING, DEL <index> {1 TO 200}, LIST <CDC_list_opt> {ALL, ASSOC, UNASSOC, FREE, X25, IP, FSK, AGENCY <AGENCY> STRING}}

USNBD - HELP

Usage example of the HELP command

Task	Sample command and output
To obtain help information about the CDC command at the USNBD level as a USER	

```
help CDC

MANAGES OR LISTS CDCs
Parms: <command> {ADD <index> {1 TO 200}
         <Transport_Protocol> {X25 <MPCindex> {0 TO 255}
                                 <MPClinknumber> {0 TO 3}
                                 <address> STRING
                                 <protocol1> {0 TO 255}
                                 <protocol2> {0 TO 255}
                                 <protocol3> {0 TO 255}
                                 <protocol4> {0 TO 255},
                               IP <IPaddress1> {0 to 255}
                                  <IPaddress2> {0 to 255}
                                  <IPaddress3> {0 to 255}
                                  <IPaddress4> {0 to 255}
                                  <IPPort) {0 to 32767},
                           FSK <Access> {SL <10-digit DN> STRING,
                                         DE <10-digit DN> STRING,
                                  SR <10 or 11-digit DN> STRING}}
                                       ASSOC <index> {1 TO 200}
                                             <SIN> STRING,
                                        DISASSOC <SIN> STRING,
                                        DEL <index> {1 TO 200},
                                        LIST <CDC_list_opt>
                              {ALL, ASSOC, UNASSOC, FREE, X25, IP, FSK}}
```

USNBD - HELP

Usage example of the HELP command

Task	Sample command and output
To obtain help information about the SURV command at the USNBD level as an ADMIN	

```
>help SURV

MAP response:

MODIFY OR VIEW SURVEILLANCES
Parms: <command> {ADD <handle> {DN <subject_dn> STRING,
       KEY [<SITE > STRING]
       <FRAME> {0 TO 511}
       <UNIT> {0 TO 9}
       <DRAWER> {0 TO 99}
       <CIRCUIT> {0 TO 99}
       <KEY> {1 TO 64},
       LEN [<SITE > STRING]
       <FRAME> {0 TO 511}
       <UNIT> {0 TO 9}
       <DRAWER> {0 TO 99}
       <CIRCUIT> {0 TO 99},
       LTID <LTGRP> STRING
       <LTNUM> {0 TO 1022}}
       <case_id> STRING
       <SIN> STRING
       <MRP> {N, Y}
       <calling_party_num_delivery> {N, Y}
       <inband_delivery> {N, Y}
       <feature_status_periodic> {N, Y
       [<Feature_Status_Interval> {15 TO 1440}]}
       <surveillance_status_periodic> {N, Y
       [<Surveillance_Status_Interval> {60 TO 1440}]}
       <Agency> STRING,
       DEL <SIN> STRING,
       LIST <Surv_list_opt> {ALL,
       ACT,
       INACT,
       SIN <SIN> STRING,
       DN <subject_dn> STRING,
       KEY [<SITE > STRING]
       <FRAME> {0 TO 511}
       <UNIT> {0 TO 9}
       <DRAWER> {0 TO 99}
```

(MAP response continues on next page)

USNBD - HELP

Usage example of the HELP command

Task	Sample command and output
To obtain help information about the SURV command at the USNBD level as an ADMIN	
	(Continuation of MAP display for usage example on previous page)

```
<CIRCUIT> {0 TO 99}
<KEY> {1 TO 64},
LEN [<SITE > STRING]
<FRAME> {0 TO 511}
<UNIT> {0 TO 9}
<DRAWER> {0 TO 99}
<CIRCUIT> {0 TO 99},
LTID <LTGRP> STRING
<LTNUM> {0 TO 1022},
AGENCY <agency> STRING},
ACT <SIN> STRING,
DEACT <SIN> STRING}
```

USNBD - HELP

Usage example of the HELP command

Task	Sample command and output
To obtain help information about the SURV command at the USNBD level as an USER	

```
>help SURV

MAP response:

MODIFY OR VIEW SURVEILLANCES
Parms: <command> {ADD <handle> {DN <subject_dn> STRING,
       KEY [<SITE > STRING]
       <FRAME> {0 TO 511}
       <UNIT> {0 TO 9}
       <DRAWER> {0 TO 99}
       <CIRCUIT> {0 TO 99}
       <KEY> {1 TO 64},
       LEN [<SITE > STRING]
       <FRAME> {0 TO 511}
       <UNIT> {0 TO 9}
       <DRAWER> {0 TO 99}
       <CIRCUIT> {0 TO 99},
       LTID <LTGRP> STRING
       <LTNUM> {0 TO 1022}}
       <case_id> STRING
       <SIN> STRING
       <MRP> {N, Y}
       <calling_party_num_delivery> {N, Y}
       <inband_delivery> {N, Y}
       <feature_status_periodic> {N, Y
       [<Feature_Status_Interval> {15 TO 1440}]}
       <surveillance_status_periodic> {N, Y
       [<Surveillance_Status_Interval> {60 TO 1440}]}
       DEL <SIN> STRING,
       LIST <Surv_list_opt> {ALL,
       ACT,
       INACT,
       SIN <SIN> STRING,
       DN <subject_dn> STRING,
       KEY [<SITE > STRING]
       <FRAME> {0 TO 511}
       <UNIT> {0 TO 9}
       <DRAWER> {0 TO 99}
       <CIRCUIT> {0 TO 99}
```

(MAP response continues on next page)

USNBD - HELP

Usage example of the HELP command

Task	Sample command and output
To obtain help information about the SURV command at the USNBD level as a USER	
	(Continuation of MAP display for usage example on previous page) <KEY> {1 TO 64}, LEN [<SITE > STRING] <FRAME> {0 TO 511} <UNIT> {0 TO 9} <DRAWER> {0 TO 99} <CIRCUIT> {0 TO 99}, LTID <LTGRP> STRING <LTNUM> {0 TO 1022}, ACT <SIN> STRING, DEACT <SIN> STRING}

USNBD - QUIT

USNBD - QUIT

Function

The QUIT command is used to exit the USNBD level of the MAP.

The QUIT command is available to authorized USNBD users (with or without administrator privileges) at the USNBD level of the MAP.

Command syntax

The QUIT command syntax is as follows:

Command	Parameters
QUIT	<parameter>

Parameter description

Parameter	Value	Description
parameter	all, name, or n_levels	Indicates how many or up to which levels of the MAP to exit

Usage notes

The QUIT command is available even when USNBD is not activated.

Usage examples

Usage example of the QUIT command

Task	Sample command and output
To exit the USNBD level of the MAP	
	>quit *Example of a MAP response:* CI:
	>quit usnbd *Example of a MAP response:* CI:

USNBD - QUIT

Usage example of the QUIT command (Continued)

Task	Sample command and output
	>quit 1 *Example of a MAP response:* `logutil:`
	>quit all *MAP response:* `CI:`

USNBD - SURV

USNBD - SURV

Function

The SURV command is used to add, delete, activate, deactivate, and view a list of surveillances.

This command is available to authorized USNBD users (with or without administrator privileges) at the USNBD level of the MAP. Administrative users can execute these commands on any agency and view information for all agencies. Non-administrative users can add, delete, activate, deactivate, or view surveillances only for their own agencies.

For SURV ADD, the parameter AGENCY is prompted only for administrative users. For non-administrative users, the user's agency is taken as the surveillance agency and the user is not prompted for this parameter.

For SURV DEL, an administrative user can delete a surveillance for any agency. A non-administrative user can delete surveillances for only the user's agency.

For SURV ACT and SURV DEACT, an administrative user can activate or deactivate a surveillance for any agency. A non-administrative user can activate or deactivate surveillances for only the user's agency.

For SURV LIST, administrative users will see the agency information for all options. Non-administrative users will see only surveillances belonging to the user's agency. An administrative user can choose to view either a specific agency's information or all agencies' information, and agency information is not displayed.

Command syntax

The SURV command syntax is as follows:

Command	Parameters
SURV ACT	<sin>
SURV ADD	**For administrative users:** <handle> <case_id> <sin> <mrp> <calling_party_num_delivery> <inband_delivery> <feature_status_periodic> <feature_status_interval> <surveillance_status_periodic> <surveillance_status_interval> <PNI> <agency>

USNBD - SURV

Command	Parameters
	For non-administrative users: <handle> <case_id> <sin> <mrp> <calling_party_num_delivery> <inband_delivery> <feature_status_periodic> <feature_status_interval> <surveillance_status_periodic> <surveillance_status_interval> <PNI>
SURV DEACT	<sin>
SURV DEL	<sin>
SURV LIST	**For administrative users:** <option> <agency> **For non-administrative users:** <option>

Parameter description

Parameter	Value	Description
agency	1 through 16 alphanumeric characters	Specifies the agency of the user. This parameter is prompted for if 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.
case_id	1 through 16 alphanumeric characters	Surveillance identity provided by the LEA
calling_party_num_delivery	Y or N	Indicates whether the calling party's DN can be delivered to the LEA
handle	DN, LEN, KEY, or LTID with subfields	Identifies the subject of the surveillance: • DN with <subject_dn> • LEN with <site> <frame> <unit> <drawer> <circuit> • KEY with <site> <frame> <unit> <drawer> <circuit> <key>, or • LTID with <ltgrp> <ltnum>
inband_delivery	Y or N	Indicates whether inband digits delivery is supported on a particular subject

USNBD - SURV

Parameter description (Continued)

Parameter	Value	Description
mrp	Y or N	Indicates whether monitoring of replacement parties is allowed for the surveillance
option	ALL, ACT, INACT, SIN, DN, KEY, LEN, LTID, or AGENCY	Specifies which surveillances to list: • ALL displays all surveillances • ACT displays all of the surveillances that are activated • INACT displays all of the surveillances that are deactivated • SIN displays the surveillance with the specified surveillance identification number (SIN) • DN <subject_dn> displays the surveillances on the specified directory number • KEY <site> <frame> <unit> <drawer> <circuit> <key> displays the surveillance on the specified key • LEN <site> <frame> <unit> <drawer> <circuit> displays the surveillance on the specified LEN • LTID <ltgrp> <ltnum> displays the surveillance on the specified LTID • AGENCY is prompted only for administrative users. This is used to list all the surveillances for a particular agency.
opt	ON, OFF, or STATUS	Enables and disables, on an office-wide basis, or displays the status of the Held Conference feature
PNI	Y or N	If PNI is set to “Y”, call content and inband digits (if a CCR is provisioned) of calls made on a private network will be intercepted. If PNI is set to “N”, call content and inband digits (if a CCR is provisioned) of calls made on private networks will not be intercepted.

USNBD - SURV

Parameter description (Continued)

Parameter	Value	Description
sin	1 through 25 alphanumeric characters	Surveillance identification number (SIN) provided by the operating company, which uniquely identifies the surveillance
surveillance_status_ periodic	Y or N	Indicates whether a surveillance status periodic message should be generated for the surveillance
surveillance_status_ interval	60 to 1440 (in increments of 15 mins)	Specifies the time interval in minutes between periodic messages

Usage notes

When adding a surveillance using the SURV ADD command, it is necessary to identify the subject. Here are some guidelines on what to use to identify a subject. Identify a subject using the subject's DN when the subject

- has a single DN, which is not shared with any other party
- is not a member of a hunt group
- is not an ISDN line
- is not a member of MADN group

Note: On a 2FR line, a surveillance can be defined independently on each of the two DNs.

Identify a non-ISDN subject who is a member of a hunt group according to the hunt group type:

- BNN (of DLH or MLH) LEN or KEY
- BNN (of DNH or KSH) primary DN, LEN, or KEY
- DLH LEN or KEY
- DNH DN, LEN, or KEY
- KSH DN or KEY
- MLH LEN or KEY
- PRH DN, LEN, or KEY

USNBD - SURV

Note: A surveillance on a BNN subject applies to the entire line. Therefore, whether the subject is identified using the primary DN, LEN, or KEY, calls to either the primary DN or the bridge night number (BNN) are monitored.

Identify a subject who is a MADN group member (MCA or SCA) using LEN or KEY.

Identify an EBS subject using the subject's LEN or DN.

Identify an SDN or ESDN subject using the primary DN.

Note: Surveillances are only performed on the PDN. Even though the subject is identified using the primary DN, calls to either the primary or secondary DNs are monitored.

Identify an ISDN subject using the subject's LTID.

Note: For fully initialized terminals (FIT), the LTID identifies a single terminal. When a surveillance is activated on the LTID of a FIT, the entire FIT, including all the keys, is monitored. For non-initializing terminals (NIT), the LTID can be shared by several terminals. When a surveillance is activated on the LTID of a NIT, all the NITs that correspond to the LTID are monitored.

Usage examples

Usage example of the SURV command

Task	Sample command and output
To add a surveillance as ADMIN on an ISDN subject with no Feature Status Periodic and with Surveillance Status Periodic	
	`>surv add ltid isdn 100 1234 sin1 y y n y 60 agency1` *MAP response:* **SURV ADD DONE.**
To add a surveillance as a USER on an ISDN subject with no Feature Status Periodic and with Surveillance Status Periodic	

USNBD - SURV

Usage example of the SURV command (Continued)

Task	Sample command and output
	>surv add ltid isdn 100 1234 sin1 y y n y 60 *MAP response:* **SURV ADD DONE.**
To delete a surveillance as a ADMIN	
	>surv del sin1 *MAP response:* SURV DEL DONE.
To delete a surveillance as a USER belonging to the same agency as surveillance	
	>surv del sin1 *MAP response:* SURV DEL DONE.
To display a list of all surveillances as ADMIN	
	>surv list all *Example of a MAP response:* Subject CaseID SIN MRP Clg_dlvry Inband_dlvry (Feat_status Interval) (Surv_status Interval) PNI Agency Status {Associated_CDC} {Associated_CCRs} --- LTID ISDN2 1 CASE1 SIN1 Y Y (Y 15) (N 0) AGENCY1 ACTIVE {1} {8 6} DN 6135520302 CASE2 SIN4 Y Y (Y 15) (Y 60) Y DEFAULT INACTIVE {1} {3}

USNBD - SURV

Usage example of the SURV command (Continued)

Task	Sample command and output
To display a list of all surveillances as USER belonging to the same agency as surveillance	
	>surv list all *Example of a MAP response:* Subject CaseID SIN MRP Clg_dlvry Inband_dlvry (Feat_status Interval) (Surv_status Interval) PNI Agency Status {Associated_CDC} {Associated_CCRs} --- LTID ISDN2 1 CASE1 SIN1 Y Y (Y 15) (N 0) ACTIVE {1} {8 6} DN 6135520302 CASE2 SIN4 Y Y (Y 15) (Y 60) N INACTIVE {1} {3}
To display a list of all surveillances as ADMIN using the AGENCY option	
	>surv list agency default *Example of a MAP response:* Subject CaseID SIN MRP Clg_dlvry Inband_dlvry (Feat_status Interval) (Surv_status Interval) PNI Agency Status {Associated_CDC} {Associated_CCRs} --- DN 6135520302 CASE2 SIN4 Y Y (Y 15) (Y 60) Y DEFAULT INACTIVE {1} {3}
To activate a surveillance as USER belonging to the same agency as surveillance	
	>surv act sin1 *MAP response:* SURV ACT DONE.
To activate a surveillance as a ADMIN	
	>surv act sin1 *MAP response:* SURV ACT DONE.

USNBD - SURV

Usage example of the SURV command (Continued)

Task	Sample command and output
To deactivate a surveillance as USER belonging to the same agency as surveillance	
	>surv deact sin1 *MAP response:* SURV DEACT DONE.

Usage responses

Usage responses for the SURV command

MAP output	Meaning and action
INVALID AGENCY NAME	
	Meaning: The agency name entered by the ADMIN exceeds the maximum allowed size of agency. **Action:** None.
SURV ADD DONE.	
	Meaning: The surveillance has been added. **Action:** None.
SURV DEL DONE.	
	Meaning: The surveillance has been deleted. **Action:** None.
SURV LIST DONE.	
	Meaning: The SURV LIST command has been executed successfully. **Action:** None.
NO MATCHING SURVEILLANCE FOUND	
	Meaning: No surveillances match the specified criteria. **Action:** None.
SURV ACT DONE.	

USNBD - SURV

Usage responses for the SURV command (Continued)

MAP output	Meaning and action
	Meaning: The surveillance has been activated. **Action:** None.
`SURV DEACT DONE.`	
	Meaning: The surveillance has been deactivated. **Action:** None.
`USER AGENCY NOT SAME AS SURVEILLANCE AGENCY`	
	Meaning: Agency of the user (who executes the command) is different from the agency of the surveillance. **Action:** None.

USNBD - TEST

USNBD - TEST

Function

The TEST command verifies that the switched ISUP CCC links to the recorder can be established properly.

The TEST command is available to authorized USNBD users (with or without administrator privileges) at the USNBD level of the MAP.

Command syntax

The TEST command syntax is as follows:

Command	Parameters and variables
TEST	TEST <CCC> <CR> Next par is: <CCC> {1 TO 500} Enter: <CCC>

Parameter description

Parameter	Description
CCR	Index of the Call Content Resource. This index can take values from 1 to 500.

Usage notes

The TEST is a command under the USNBD directory. A USNBD administrator can use the TEST command to verify any agency's switched links. A user can use TEST to verify the switched links belonging only to the user's agency.

USNBD - TEST

Usage examples

Usage example of the TEST command

Task	Sample command and output
To verify the CCR connectivity as USER using the TEST command	
	>TEST 1 *Example of a MAP response:* SUCCESSFUL TEST CALL FOR CCC DN 6136631001 TEST FAILED: ROUTING FAILED FOR CCC DN 6136631002 TEST CALL DONE.
To verify the CCR connectivity as USER using the TEST command	
	>TEST 2 *Example of a MAP response:* SUCCESSFUL TEST CALL FOR CCC DN 4164631001 SUCCESSFUL TEST CALL FOR CCC DN 4164631002 TEST CALL DONE.

Usage responses

Usage responses for the TEST command

MAP output	Meaning and action
TEST FAILED: UNAUTHORIZED COMMAND	
	Meaning: The user is not authorized to use the TEST command, or the user agency is not the same as CCR agency. **Action:** None.
TEST FAILED: USNBD IS NOT ACTIVE	
	Meaning: USNBD SOC is IDLE. **Action:** Turn the USNBD SOC ON.
TEST FAILED: USNBD RECOVERY IN PROGRESS, PLEASE TRY AGAIN LATER.	
	Meaning: After a RESTART (cold or reload), USNBD performs some initialization. The TEST command cannot be used during that short period of time.

USNBD - TEST

Usage responses for the TEST command (Continued)

MAP output	Meaning and action
	Action: Try again few seconds later.
TEST FAILED: USNBD DATA TRANSFER IN PROGRESS, PLEASE TRY AGAIN LATER.	
	Meaning: A load application is in progress. The TEST command is not allowed while USNBD data is being transferred. **Action:** Try again after the load application is completed.
TEST FAILED: INTERNAL ERROR	
	Meaning: USNBD is not able to claim FLAG for executing TEST command. **Action:** Try again later.
TEST FAILED: CCR ALREADY ASSOCIATED.	
	Meaning: The TEST command cannot be performed because the specified CCR is currently associated to surveillance. **Action:** Disassociate the CCR and then perform the test.
TEST FAILED: CCR DOES NOT EXIST.	
	Meaning: The specified CCR does not exist. **Action:** Verify that CCR is present using the CCR LIST command.
TEST WARNING <DN>: INBAND SIGNALLING ENCOUNTERED.	
	Meaning: At least one leg of the call has been routed over inband signaling trunks, resulting in extra delays in call setup for the specified CCR link. **Action:** None.
TEST FAILED: CCC DN <DN> UNALLOCATED	
	Meaning: The called party cannot be reached, or the specified number is not currently assigned. **Action:** Verify that the correct CCC DN is entered. Verify the DN with the agency.
TEST FAILED: NO ROUTE TO CCC DN <DN>.	
	Meaning: The network is unable to route the call to the requested destination.

USNBD - TEST

Usage responses for the TEST command (Continued)

MAP output	Meaning and action
	Action: Verify that the correct CCC DN is entered. Verify translation/routing tables using the TRAVER command. Verify the DN with the agency.
TEST FAILED: CALL REJECTED BY CCC DN <DN>.	
	Meaning: The remote switching equipment refused the call for the specified link. **Action:** Verify that the correct CCC DN is entered. Verify the DN with the agency.
TEST FAILED: CCC DN <DN> IS OUT OF ORDER.	
	Meaning: The interface to the destination of the specified link is not functioning correctly. **Action:** Verify that the correct CCC DN is entered. Verify that the recorder interface is functioning for the agency. Verify the DN with the agency.
TEST FAILED: CCC DN <DN> CIRCUIT IS NOT AVAILABL	
	Meaning: There is no appropriate circuit currently available to handle the call for the specified link. **Action:** Verify that the correct CCC DN is entered. Verify that trunks are available (in IDLE state) in the required route(s) identified using the TRAVER command, then retry. Verify the DN with the agency.
TEST FAILED: NETWORK FOR CCC DN <DN> IS TEMPORARILY OUT OF ORDER.	
	Meaning: The specified link could not be established because the network is not functioning properly for an indefinite period of time. **Action:** Try again later.
TEST FAILED: NETWORK CONGESTION FOR CCC DN <DN>	
	Meaning: The specified link could not be established because the network is experiencing a period of high traffic. **Action:** Try again later.

USNBD - TEST

Usage responses for the TEST command (Continued)

MAP output	Meaning and action
TEST FAILED: TEST_CALL_BILLNO MISSING.	
	Meaning: The specified CCC DN test call is a billable call and there is no TEST_CALL_BILLNO parameter defined in UNB_OFCWIDE. **Action:** Verify that the call is intended to be billable. If billable, define a TEST_CALL_BILLNO using the UNB_OFCWIDE command. If not billable, find a valid non-billable DN and re-assign it to the current CCC.
TEST FAILED: EXTENSION BLOCK NOT AVAILABLE.	
	Meaning: There are no more NBD extension blocks available to make the connection for the specified CCC link. **Action:** None.
TEST FAILED: DMS RESOURCES NOT AVAILABLE.	
	Meaning: Some DMS resources are not available to make the connection for the specified CCC link. **Action:** Examine AUD594 logs. Verify that no more VIDS are available.
TEST FAILED: COMMUNICATION PROBLEM, PLEASE TRY AGAIN.	
	Meaning: After issuing the TEST command, no response was received, within the maximum time allowed, to acknowledge the proper establishment of the specified CCC link. This should be a temporary situation. **Action:** Try again later.
TEST FAILED: TRANSLATIONS FAILED FOR CCC DN <DN>.	
	Meaning: The specified DN does not translate properly. **Action:** Verify that the correct CCC DN is entered. Verify the translation tables using the TRAVER command. Verify the DN with the agency.
TEST FAILED: ROUTING FAILED FOR CCC DN <DN>.	
	Meaning: A route cannot be found for the specified DN digits.

USNBD - TEST

Usage responses for the TEST command (Continued)

MAP output	Meaning and action
	Action: Verify that the correct CCC DN is entered. Verify the translation/routing tables using the TRAVER command. Verify the DN with the agency.
TEST FAILED: UNSUPPORTED TRUNK TYPE.	
	Meaning: The trunk type used to route to the specified DN is not supported. The trunk types should be ISUP trunks (TO, IT, T2). **Action:** Verify that the translations are correct using the TRAVER command. If necessary, change translations to route to a supported trunk type.
TEST FAILED: UNSUPPORTED TRUNK TYPE FOR CDC DN <DN>	
	Meaning: The trunk type used to route to the specified DN is not valid. The trunk types should be ISUP trunks (TO, IT, T2). **Action:** Verify that the translations are correct using the TRAVER command. If necessary, change translations to route to a supported trunk type.
TEST FAILED: UNSUPPORTED TRUNK SIGNALING FOR CDC DN <DN>	
	Meaning: The trunk used to route to the specified DN does not use a valid signaling type. **Action:** Verify that the trunk path through XPMs to the destination use the correct protocols.
TEST FAILED: CCC DN <DN> IS BUSY.	
	Meaning: The specified DN is in Call Processing Busy state. **Action:** Verify that the correct CCC DN is entered. If it is a DN locally defined on the switch, post the DN at the MAP LTP level to determine the connected line or trunk and take any necessary steps to release the line. Contact the agency to verify if the recorder is off-hook. Verify the DN with the agency.
TEST FAILED: MESSAGING PROBLEM- DN <DN>.	
	Meaning: The connection to the specified DN cannot be made due to some USNBD messaging problem. **Action:** Verify if SWERR logs are being generated and refer them to your support group.

USNBD - TEST

Usage responses for the TEST command (Continued)

MAP output	Meaning and action
TEST FAILED: DISCONNECTED DURING CALL SETUP TO CCC DN <DN>.	
	Meaning: The link associated with the DN answered and then disconnected. **Action:** Verify that the correct CCC DN is entered. Verify that the recorder interface (to the line) with the agency is functioning. Verify the DN with the agency.
TEST FAILED: NO ANSWER FROM CCC DN <DN>.	
	Meaning: The link associated with the DN did not return an answer within the maximum time allowed. **Action:** Verify that the correct CCC DN is entered. Verify that the recorder interface (to the line) with the agency is functioning. Verify the DN with the agency.
TEST FAILED: NO CSIDE LINKS FOR CCC DN <DN>.	
	Meaning: The internal DMS linkage is out of service between the network and the Peripheral Module (PM) to which the specified link (DN) is assigned. **Action:** Refer problem to the maintenance personnel responsible for the DMS switch for corrective action.
TEST FAILED: UNKNOWN PROBLEM.	
	Meaning: Due to some unknown problem (not a resource or communication problem), the link could not be established for the specified DN. This should be temporary. **Action:** Examine LOSTXXX, PM180, and SWERR logs.
SUCCESSFUL TEST CALL FOR CCC DN <DN>. **TEST CALL DONE.**	
	Meaning: The specified CCC link has been properly established for the TEST command. **Action:** After the link has been properly established, the feature will disconnect the link and place it in an IDLE state.

USNBD - UNB_OFCWIDE

Function

The UNB_OFCWIDE admin command has a sub-command HELDMON with options ON, OFF, and STATUS. These options will enable, disable and display the status of content of held conference delivery functionality on an office-wide basis.

Command syntax

The UNB_OFCWIDE command syntax is as follows:

Command	Parameters
UNB_ OFCWIDE	<command> {TRIG_LOGS <trig_log_opts> {ON, OFF, STATUS} HELDMON <heldmon_opts> {ON, OFF, STATUS} TEST_CALL_BILLNO <tc_options> {ADD <billno> STRING, REP <billno> STRING, DEL, LIST}, LIST}

Parameter description

Parameter	Description
UNB_OFCWIDE	UNB_OFCWIDE is an ADMIN command
HELDMON	The HELDMON subcommand enables or disables held conference functionality on an office-wide basis. The UNB_OFCWIDE HELDMON STATUS refers to the status of the content of held conference delivery functionality on an office-wide basis. This is displayed as ON or OFF.
ON	To activate the Held Conference functionality
OFF	To deactivate the Held Conference functionality
STATUS	To display the status of Held Conference functionality on an office-wide basis
TEST_CALL_BILLNO	To add, delete, replace, or list the test-call bill number on an office-wide basis. See usage below.

USNBD - UNB_OFCWIDE

Parameter description

Parameter	Description
TRIG_LOGS	To activate or deactivate the generation of TRIG600 and TRIG700 logs as general log reports
UNB_OFCWIDE TEST_CALL_BILLNO ADD	To add the 10-digit TEST call billing number on an office-wide basis
UNB_OFCWIDE TEST_CALL_BILLNO REP	To replace the 10-digit TEST call billing number on an office-wide basis
UNB_OFCWIDE TEST_CALL_BILLNO DEL	To delete the 10-digit TEST call billing number on an office-wide basis
UNB_OFCWIDE TEST_CALL_BILLNO LIST	To list the 10-digit TEST call billing number on an office-wide basis
LIST	To display all of the USNBD office-wide parameters

Usage notes

The UNB_OFCWIDE is an ADMIN command under the USNBD directory.

Usage examples

Usage example of the UNB_OFCWIDE HELDMON command

Task	Sample command and output
To activate content of held conference delivery functionality on an office-wide basis	
	>UNB_OFCWIDE HELDMON ON *MAP response:* HELDMON ON DONE.
To deactivate content of held conference delivery functionality on an office-wide basis	
	>UNB_OFCWIDE HELDMON OFF *MAP response:* HELDMON OFF DONE.

USNBD - UNB_OFCWIDE

Usage example of the UNB_OFCWIDE HELDMON command (Continued)

Task	Sample command and output
To display status of content of held conference delivery functionality on an office-wide basis	
	>UNB_OFCWIDE HELDMON STATUS *MAP response:* ON (or) OFF.
To activate content of held conference delivery functionality on an office-wide basis when it is already ON	
	>UNB_OFCWIDE HELDMON ON *MAP response:* HELDMON FAILED:HELDMON IS ALREADY ON.
To deactivate content of held conference delivery functionality on an office-wide basis when it is already OFF	
	>UNB_OFCWIDE HELDMON OFF *MAP response:* HELDMON FAILED:HELDMON IS ALREADY OFF.
To activate the Held Conference feature office-wide	
	>surv heldmon on *MAP response:* HELDMON ENABLE DONE.
To add test call billing number office-wide	
	>UNB_OFCWIDE TEST_CALL_BILLNO add 1111111111 *MAP response:* TEST_CALL_BILLNO ADD DONE.
To delete test call billing number	

USNBD - UNB_OFCWIDE

Usage example of the UNB_OFCWIDE HELDMON command (Continued)

Task	Sample command and output
	>UNB_OFCWIDE TEST_CALL_BILLNO delete *MAP response:* TEST_CALL_BILLNO DEL DONE. WARNING: BILLABLE TEST CALLS MAY FAIL.
To list all USNBD parameters on office-wide basis	
	>UNB_OFCWIDE LIST *MAP response:* PARNAME PARVAL ---------- TRIG_LOGS ON HELDMON OFF TEST_CALL_BILLNO NIL UNB_OFCWIDE LIST DONE.

Usage responses

Usage responses for the UNB_OFCWIDE command

MAP output	Meaning and action
HELDMON ON DONE.	
	Meaning: Content of held conference delivery functionality is enabled on an office-wide basis. **Action:** None.
HELDMON OFF DONE	
	Meaning: Content of held conference delivery functionality is disabled on an office-wide basis. **Action:** None.
ON or OFF	
	Meaning: Status of content of held conference delivery functionality on an office-wide basis. **Action:** None.

USNBD - UNB_OFCWIDE

Usage responses for the UNB_OFCWIDE command (Continued)

MAP output	Meaning and action
HELDMON FAILED: HELDMON IS ALREADY ON	
	Meaning: Content of held conference delivery functionality is already enabled on an office-wide basis. **Action:** None.
HELDMON FAILED: HELDMON IS ALREADY OFF	
	Meaning: Content of held conference delivery functionality is already disabled on an office-wide basis. **Action:** None.
TEST_CALL_BILLNO ADD FAILED: BILLING NUMBER MUST BE OF 10 DIGITS.	
	Meaning: The length of the specified TEST call billing number is invalid. **Action:** Enter proper 10-digit TEST call billing number.
TEST_CALL_BILLNO REP FAILED: BILLING NUMBER MUST BE OF 10 DIGITS	
	Meaning: The length of the specified TEST call billing number is invalid. **Action:** Enter proper 10-digit TEST call billing number.
TEST_CALL_BILLNO ADD DONE	
	Meaning: Succeeded in adding the TEST call billing number. **Action:** None.
TEST_CALL_BILLNO REP DONE	
	Meaning: Succeeded in replacing the TEST call billing number. **Action:** None.
TEST_CALL_BILLNO DEL DONE **WARNING: BILLABLE TEST CALLS MAY FAIL**	
	Meaning: TEST call bill number is deleted. **Action:** None.

USNBD - UNB_OFCWIDE

Usage responses for the UNB_OFCWIDE command (Continued)

MAP output	Meaning and action
PARNAME PARVAL **HELDMON <status>** **TEST_CALL_BILLNO <TEST call billing number>** **UNB_OFWIDE LIST DONE.**	
	Meaning: Current values of USNBD office-wide parameters are displayed. **Action:** None.

USNBD - USER

Function

The USER command is used to add or delete USNBD users, and to display a list of the current USNBD users.

This command is only available to USNBD users with administrator privileges at the USNBD level of the MAP.

Command syntax

The USER command syntax is as follows:

Command	Parameters
USER ADD	**For adding an administrative user:** <user_id> <admin> <agency> **For adding a non-administrative user:** <user_id> <admin>
USER DEL	<user_id>
USER LIST	<user_list_opt>

Parameter description

Parameter	Value	Description
user_id	8 through 16 alphanumeric characters	User identification
admin	Y or N	Specifies if the USNBD user to be added is to have administrator privileges. This parameter must be datafilled.

USNBD - USER

Parameter description

Parameter	Value	Description
agency	1 through 16 alphanumeric characters	Specifies the agency of the user. This is prompted for if the added user is not ADMIN, meaning that the admin field (above) is set to N.
user_list_opt	ALL or AGENCY	Specifies the type of user list displayed when this command is typed. To show all valid users of the USNBD, type ALL. To show only the users belonging to a specific agency, type AGENCY and the name used in the agency parameter. Both options will display the user's agency.

Usage notes

A USNBD administrator can delete a user at any time, even when the user is logged on.

The USER command is available after USNBD has been activated in SOC.

Usage examples

Usage example of the USER command

Task	Sample command and output
To add a new non-ADMIN user to USNBD	**>user add user1 N agency1** *MAP response:* USER ADD DONE.
To add a new non-ADMIN user to USNBD	**>user add user1 N agency1589653217654** *MAP response:* USER ADD FAILED. INVALID AGENCY NAME.

USNBD - USER

Usage example of the USER command (Continued)

Task	Sample command and output
To add a new ADMIN user to USNBD	
	>user add user1 Y *MAP response:* USER ADD DONE.
To delete a USNBD user	
	>user del user1 *MAP response:* USER DEL DONE.
To list all USNBD users	
	>user list all *Example of a MAP response:* USER ADMIN AGENCY -------------------------------- USER2 N AGENCY1 USER3 N AGENCY2 USER3 Y - USER LIST DONE.
To list all USNBD users belonging to a particular agency	
	>user list agency agency1 *Example of a MAP response:* USER ADMIN AGENCY -------------------------------- USER2 N AGENCY1 USER LIST DONE.

USNBD - USER

Usage example of the USER command (Continued)

Task	Sample command and output
To list all USNBD users belonging to a particular agency (no users belong to agency)	
	>user list agency agency4 *Example of a MAP response:* NO MATCHING USER FOUND USER LIST DONE.

Usage responses

Usage responses for the USER command

MAP output	Meaning and action
INVALID AGENCY NAME	
	Meaning: The agency name entered by the administrative user exceeds the maximum allowed size of agency. **Action:** None.
NO MATCHING USER FOUND	
	Meaning: No matching user found. No user belongs to the given agency. **Action:** None.
USER ADD DONE.	
	Meaning: The USNBD administrator has successfully added a new user to the list of authorized USNBD users. **Action:** None.
USER DEL DONE.	
	Meaning: The USNBD administrator has successfully deleted a user from the list of authorized USNBD users. **Action:** None.

USNBD - USER

Usage responses for the USER command (Continued)

MAP output	Meaning and action
`USER LIST DONE.`	
	Meaning: The USNBD administrator has successfully displayed the list of the current USNBD users. **Action:** None.

OBJMGRCI

OBJMGRCI

Function

OBJMGRCI commands are used to display the information about objects at the management information tree level. Available options include display, root, displaytree, destroy, and disassociate.

Note: Only the changes associated with USNBD are included in this command description.

For USNBD, the following commands are modified to show virtual links:

- **>DISPLAY xsg <xsg_number> children <level>**

  This command displays objects related to a specific XSG.

- **>DISPLAY link <link_number> children <level>**

  This command displays link object information and the HFP provision state. In the XLIU MIT, the dn object is represented as 13 object, and the PVC object is added as the child of the link object.

- **>ROOT link <link_number>**

  This command displays the root object of the link object.

OBJMGRCI

Usage examples

Usage example of the DISPLAY command with XSG and CHILDREN options

```
display xsg 100 children 5
*****************************************************
Object Type : xsg
Operation : format data, Scan State : finished
Operation : audit check, Scan State : finished
Operation : display    , Scan State : finished
XSG 100
XLIU 0
xsg_ext_no 100
current_number_of_link 12
max_channel_number 30
XLIU 0
echo_links_present 1
virtual_links_present 1
XLIU_LIDS ALLOCATED: 0,2,3,5,6,7,8,9,10,11,12,13,14,
*****************************************************
Object Type: link
Operation : format data, Scan State : finished
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
Virtual link
Link ID=30, Link type=x.25 virtual
XLIU Link ID=0

************************************************
Object Type : pvc
Operation : format data, Scan State : finished
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
PVC Endpoint Types: Master = 0
************************************************
Object Type : link
Operation : format data, Scan State : finished
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
Virtual link
Link ID = 30, Link type = x.25 virtual
XLIU Link ID = 0
PVC Endpoint Types: Slave = 0
************************************************
Object Type : dn
Operation : format data, Scan State : finished
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
dn = 6135550106, ext byte = 0
extracted object index = 0
```

OBJMGRCI

Usage example of the DISPLAY command with LINK and CHILDREN options

```
display link 0 children 3
*****************************************************
Object Type : link
Operation : format data, Scan State : first time
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
Virtual link
Link ID = 30, Link type = x.25 virtual
XLIU 0
xHFP provisioning is FALSE
*****************************************************
Object Type : pvc
Operation : format data, Scan State : first time
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
LCN = 3, XLIU_LID = 5, INDEX = 2
Sendtc = 10, Sendps = 7, Sendws = 2
Recvtc = 10, Recvps = 7, Recvws = 2
no children
```

Usage example of the ROOT command with the LINK option

```
root link 12
*****************************************************
Object Type : xsg
Operation : format data, Scan State : finished
Operation : audit check, Scan State : finished
Operation : display    , Scan State : finished
XSG 100
XLIU 0
xsg_ext_no 100
current_number_of_link 12
max_channel_number 30
XLIU 0
echo_links_present 1
virtual_links_present 1
XLIU_LIDS_ALLOCATED: 0,2,3,5,6,7,8,9,10,11,12,13,14,
```

PHRRCI - MOVE

PHRRCI - MOVE

Function

This command is used to move the LTID to destinations such as an X.25/X.75 service group (XSG), X.25/X.75 link interface unit (XLIU), or from one XSG to another XSG.

Command syntax

The PHRRCI MOVE command syntax is as follows:

Command	Parameters
MOVE	<LTID> to <XSG> (0 to 749) [force] <XLIU> [ ]

Parameter description

Parameter	Value	Description
LTID	0 to 32 for LTGRP; 1 to 1022 for LTNUM	Logical Terminal Identifier (LTID) consisting of the logical terminal group (LTGRP) number and the logical terminal number (LTNUM)
XSG	0 to 749	X.25/X.75 service group number
XLIU		X.25/X.75 link interface unit
force		Release the LTID and drop calls in progress

Usage notes

When the subject LTID is moved from one XLIU to another, all the PVCs associated with the virtual link are disassociated, the CCClose message is sent to the USNBD interface, and the virtual link is removed. If the subject LTID is later reattached to another XLIU, the virtual links are not recreated in the destination XLIU. If a surveillance is required on the same LTID, it must be reprovisioned using USNBD commands.

PVCOBJCI

PVCOBJCI

Function

PVCOBJCI commands are used to display information about PVC objects. Available options include display, associate, disassociate, update, and cplookup.

Note: Only the changes associated with USNBD are included in this command description.

For USNBD, the following commands are modified to show virtual links:

- **>DISPLAY pvc <pvc_id>**

  This command displays details of a particular PVC connection.

- **>UPDATE pvc <lpvc_id> children <slave_point_info>**

  PVC objects are created and associated with the virtual link by the CCR ASSOCIATE command. As a result, the slave end point of a PVC associated with the virtual link cannot be changed. If an attempt is made to change the slave end point, an error message is generated.

- **>CPLOOKUP <link_id> <lcn>**

  This command displays information about the PVC object associated with a dn_child object of the link object for the given link_id and lcn.

PVCOBJCI

Usage examples

Usage example of the DISPLAY command with PVC <pvc_id> option

```
display pvc 1 self
*****************************************************
Object Type : pvc
Operation : format data, Scan State : finished
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
PVC Endpoint Types: Master = 0
*****************************************************
Object Type: link
Operation : format data, Scan State : first time
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
Virtual link
Link ID=30, Link type=x.25 virtual
XLIU Link ID=0
PVC Enpoint Types: Slave = 0
*************************************************
Object Type : dn
Operation : format data, Scan State : finished
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
dn = 6135550106, ext byte = 0
extracted object index = 0
```

Usage example of the UPDATE command with PVC <pvc_ID> and <slave_point_info> options

```
update 0 x25 6135550106 b 6
This is a virtual link. PVC object associated with virtual links cannot be
changed.
```

PVCOBJCI

Usage example of the CPLOOKUP command with the <link_id> and <lcn> options

```
cplookup 12 5
*****************************************************
Object Type : pvc
Operation : format data, Scan State : finished
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
PVC Endpoint Types: Master = 0
*****************************************************
Object Type : link
Operation : format data, Scan State : first time
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
Virtual link
Link ID = 12, Link type = x.25 virtual
XLIU lid = 0
PVC Endpoint Types: Slave = 0
*****************************************************
Object Type : dn
Operation : format data, Scan State : finished
Operation : audit check, Scan State : first time
Operation : display    , Scan State : first time
dn = 6135550106, ext byte = 0
extracted object index = 0
PVC Object Internal ID: 0
```

QCOUNTS

Function

The QCOUNTS command is used to determine on an LTID or trunk basis, virtual call attempts and protocol counts. QCOUNTS sends a request to the XLIU to which the XSG is mapped, and displays protocol and protocol abnormality counts to the user.

The information displayed includes link level counts, packet level counts, link level protocol abnormality counts, and packet level protocol abnormality counts.

The QCOUNTS command is also used to query and reset protocol and protocol abnormality counts for open systems interconnection (OSI) levels 1, 2, and 3 of the X.25 and X.75 protocols.

Note: For USNBD, the QCOUNTS command is modified to add the option LCN for LTIDs and CLLIs of the LEA.

The LTID and LCN number for the LEA (or the CLLI and LCN number if the LEA is on a different switch) is entered to obtain OM information. If an LTID or CLLI not associated with a LEA is entered, an error message is generated.

The LCN option is not supported with the XSG parameter.

QCOUNTS

Command syntax

The following figure displays the QCOUNTS command syntax.

QCOUNTS command syntax

```
qcounts
Next par is: <selection> {LTID <ltgrp> STRING
                     <ltnum> {1 TO 1022}
                     <count level> {LINK,
                               PACKET,
                               ALL
                               LCN <lcn number> {0 TO 2048}},
                CLLI <clli> STRING
                  <extrknm> {0 TO 9999}
                  <count level> {LINK,
                            PACKET,
                            ALL,
                            LCN <lcn number> {0 TO 2048}},
                XSG <xsg number> {0 TO 749},
                 <xsg level> {BRD,
                         CHNL <chnl number> {1 TO 31},
                         OVLD}}
```

QCOUNTS

Usage examples

Usage example of the QCOUNTS command with a LEA LTID

```
qcounts ltid pkt 12 lcn 1
 LAYER 3 PROTOCOL COUNTS
 -----------------------
 Packets Received:
 VC,PVC:          0 RR:           0 RNR:         0 Data:          0
 Packets Transmitted:
 VC,PVC:          0 RR:           0 RNR:         0 Data:          0
 Virtual Call Attempts:
 Setup:          0 Originating:          0 Terminating:          0
 Unsuccessful Virtual Call Attempts:
 Blocking:                       0 Denied:                       0
 Clearing:                       0 Overload:                     0
 LAYER 3 PROTOCOL ABNORMALITY COUNTS
 -----------------------------------
 Restart Packets:
 Sent:                           0 Received:                     0
 Reset Packets:
 Sent:                           0 Received:                     0
 Clear Packets:
 Sent:                           0 Received:                     0
 Diagnostic Packets:
 Sent:                           0 Received:                     0
 LAYER 3 SERVICE DISRUPTION COUNTS
 ---------------------------------
 Reset Packets Transmitted:      0
 Clear Packets Transmitted:      0
 LAYER 3 OVERLOAD COUNTS
 -----------------------
 Dynamic Window Congestion:
 Local:                          0 Remote:                       0
 Packets dropped due to Layer 3 congestion:
 Link:                           0 VC:                           0
 Packets dropped due to:
 Layer 2:                        0 RNR:                          0
 Layer 3 link queue congestion: 0
 VC_Q Congestion:                0
```

QCOUNTS

Usage example of the QCOUNTS command with a LEA CLLI

```
qcounts clli pl1x750g lcn 1
 LAYER 3 PROTOCOL COUNTS
 -----------------------
 Packets Received:
 VC,PVC:          0 RR:           0 RNR:         0 Data:          0
 Packets Transmitted:
 VC,PVC:          0 RR:           0 RNR:         0 Data:          0
 Virtual Call Attempts:
 Setup:          0 Originating:          0 Terminating:          0
 Unsuccessful Virtual Call Attempts:
 Blocking:                       0 Denied:                       0
 Clearing:                       0 Overload:                     0
 LAYER 3 PROTOCOL ABNORMALITY COUNTS
 -----------------------------------
 Restart Packets:
 Sent:                           0 Received:                     0
 Reset Packets:
 Sent:                           0 Received:                     0
 Clear Packets:
 Sent:                           0 Received:                     0
 Diagnostic Packets:
 Sent:                           0 Received:                     0
 LAYER 3 SERVICE DISRUPTION COUNTS
 ---------------------------------
 Reset Packets Transmitted:      0
 Clear Packets Transmitted:      0
 LAYER 3 OVERLOAD COUNTS
 -----------------------
 Dynamic Window Congestion:
 Local:                          0 Remote:                       0
 Packets dropped due to Layer 3 congestion:
 Link:                           0 VC:                           0
 Packets dropped due to:
 Layer 2:                        0 RNR:                          0
 Layer 3 link queue congestion: 0
 VC_Q Congestion:                0
```

QPHF

Function

The QPHF command displays information about how a particular XSG is configured. The DMS PH keeps a representation of its provisioning data in a structure called a management information tree (MIT). The MIT consists of object types such as XSGs, channels, DNs, PVCs, and X.75 links. The QPHF command displays information about how the MIT is configured and what the parameters are for each object.

QPHF options are used to query information about packet handler services related to the queried entity like DN, LTID, XSG and so on.

Note: Only the changes associated with USNBD are included in this command description.

The QPHF command provides the following options:

- With the XSG parameter, displays information specific to the XSG, and indicates which channels are connected to it.

  >QPHF XSG xsg_number

  Note: Note: If the XSG specified in a command has a CALEA link provisioned on it, then this command displays VLINK_ID for the CALEA lLINK and link type as VIRTUAL LINK.

- With the XSG and ALL parameters, displays information specific to the XSG and all link objects associated with it.

  >QPHF XSG xsg_number ALL

  Note: For a CALEA virtual link, this command displays the string VLINK DATA, and displays the number of active calls on a the virtual link.

- With the LTID parameter, displays information about link level parameters for a particular X.25 terminal, and indicates what DNs are supported by this terminal. The logical terminal's associated channel and XSG are also displayed.

  >QPHF LTID ltgrp ltnum

  Note: This command will not function with USNBD, because no DNs are associated with virtual links (VLINK).

QPHF

- With the DN parameter, displays information about packet level parameters associated with a particular DN. This command also queries which, if any, PVCs are connected to the DN, and which, if any, CUGs it belongs to. The DN's associated logical terminal channel and XSG are also displayed.

  >QPHF DN dn_num

  Note: This command will not function with USNBD, because no DNs are associated with virtual links (VLINK).

Usage examples

Usage example of the QPHF command with XSG option

```
>qphf xsg 100

XSG INFORMATION
---------------
XSG EXT INDEX: 100         CURRENT NUMBER OF LINKS: 10
XLIU INDEX: 0              MAXIMUM NUMBER OF CHANNELS: 30
XSG 100 IS AVAILABLE FOR USE BY AUTO RESOURCE ASSIGNMENT
NUMBER OF ECHO STATION : 1 NUMBER OF virtual LINKS : 1

MAPPING
-------
CHANNEL:  1  X.25 Bd
CHANNEL:  2  X.25 Bd
CHANNEL:  3  X.25 PB
CHANNEL:  5  X.25 Bd
CHANNEL:  6  X.25 Bd
CHANNEL:  7  X.25 Bd
CHANNEL:  8  X.25 Bd
CHANNEL:  9  X.75 B
CHANNEL: 10  X.75 B
CHANNEL: 11  X.25 PB
CHANNEL: 12  X.25 PB
CHANNEL: 13  X.25 PB
CHANNEL: 14  X.25 PB
CHANNEL: 15  X.25 PB
LTID: PKT 25    ECHO STATION
VLINK_ID : 0    virtual LINK
```

QPHF

Usage example of the QPHF command with XSG-ALL option

```
>qphf xsg 100 all

MAPPINGS FOR XSG 100
--------------------
CHANNEL:   1 LTID: NI2 201  DN: 6135550201   DN: 6135550205
             No active call(s) on this LTID.
             LTID: NI2 203  DN: 6135550206
             No active call(s) on this LTID.
CHANNEL:  2  LTID: NI2 202  DN: 6135550202   DN: 6135550204
             No active call(s) on this LTID.
CHANNEL:  3
CHANNEL:  5
CHANNEL:  6
CHANNEL:  7  LTID: PKT   4  DN: 6135551004
             No active call(s) on this LTID.
CHANNEL:  8  LTID: PKT   3  DN: 6135551003
             No active call(s) on this LTID.
CHANNEL:  9
CHANNEL: 10
CHANNEL: 11  LTID: PKT 103  DN: 6135550103
             No active call(s) on this LTID.
CHANNEL: 12  LTID: PKT 104  DN: 6135550104
             No active call(s) on this LTID.
CHANNEL: 13  LTID: PKT 105  DN: 6135550105
             No active call(s) on this LTID.
CHANNEL: 14  LTID: PKT 106  DN: 6135550106
             No active call(s) on this LTID.
CHANNEL: 15  LTID: PKT 107  DN: 6135550107
             No active call(s) on this LTID.
ECHO DATA:   LTID: PKT  25  DN: 6135551222
             No active call(s) on this LTID.

Virtual Link DATA:  VLINK_ID: 0
>No active call(s) on this virtual link
```

UNPERMIT

UNPERMIT

Function

Use the unpermit command to discontinue a userid and prevent access to the DMS switch. To gain access to the DMS switch, a user must be issued a permit command with all attributes. This is one of a set of six user access/user message commands, including LOGIN, PERMIT, UNPERMIT, MSG, LOGOUT, and FORCEOUT.

Command syntax

Command	Parameters
unpermit	username password
username	This variable specifies the name of a DMS switch user. The user cannot be logged in while using this command. The valid length of the user name is 8 to 16 characters.
password	This variable specifies a valid password associated with the user name. If the enhanced password control feature is activated, the user's current password must be specified.

Qualifications

When attempting to delete a user with the unpermit CI command when the user is also a USNBD user, the UNPERMIT command fails, and the user is not deleted.

UNPERMIT

Usage examples

The following table provides an example of the UNPERMIT command.

Example of the UNPERMIT command

Example	Task, response, and explanation	
>unpermit fred ø *where* fred	specifies the name of the user	
	Task	Remove a user from the system when the enhanced password control feature is not active
	Response	UNPERMIT: USER MUST BE DELETED FROM USNBD USER LIST BEFORE BEING UNPERMITTED
	Explanation	This command fails, and user id is not discontinued because the user id also appears in the USNBD users list.

Usage responses

The following table provides explanations of system responses to the UNPERMIT command:

Responses for the UNPERMIT command

MAP output	Meaning and action
USER LOGGED IN	
	Meaning: The user was logged in when the command was attempted. **Action:** Request that the user log off and repeat the command.
USER NOT FOUND	
	Meaning: The system did not recognize the name entered as valid. **Action:** Notify the user that the user ID no longer is valid.

UNPERMIT

Responses for the UNPERMIT command (Continued)

MAP output	Meaning and action
`USER MUST BE DELETED FROM USNBD USER LIST BEFORE BEING UNPERMITTED`	
	Meaning: The user to be deleted is in the USNBD user list and cannot be deleted. **Action:** Completion of the command is denied. Contact the USNBD administrator.

XPSCI

Function

XPSCI commands are used after accessing an XLIU using REMLOGIN, and display the state of Finite State Machines (FSM) running under the X.25/X.75 Process System (XPS), the UDA data of the FSM associated with the link, and the CCUDA information.

XPSCI commands are also used to display the links allocated in the XLIU and the associated states of the three layers. Available options include LINKS, CCUDA, and UDA.

> ***Note:*** The only change associated with USNBD is the display of the X.25 virtual link.

>DISPLAY pvc <pvc_id>

Usage examples

Usage example of the CPLOOKUP command with the <link_id> and <lcn> options

```
links

     LLID GLID LCHNL GCHNL  L1 L2 L3 (0=down, 1=up)
       0    30    -     -    -   -  1
       1    31    -     -    -   1  1
       2    10   11  6411    1   0  0
       3    11   12  6412    1   0  0
       4    27    3  6403    1   0  0
       5    12   13  6413    1   0  0
       6     2    8  6408    1   0  0
       7     3    7  6407    1   0  0
       8    13   14  6414    1   0  0
       9    20    1  6401    1   0  0
      10    21    2  6402    1   0  0
      11    22    1  6401    1   0  0
      12    14   15  6415    1   0  0
      13    25    5  6405    1   1  1
      14    26    6  6406    1   1  1
      15    29     5  6405    1  0  0
```

XPSCI

Error responses

The following section provides a list of error responses that USNBD can display when either the USNBD administrator or a USNBD user enters a USNBD-specific command. The syntax of an error response is

```
<command> FAILED: <message>
```

where

command	is any one of the USNBD commands
message	is any one of the responses listed in the table that follows

For example, `CCR ADD FAILED: BOTH CCR DNS ARE THE SAME.`

Note: The error responses are listed in alphabetical order.

Error responses for USNBD commands

MAP output	Meaning and action
A CDC IS ASSOCIATED WITH THE SPECIFIED SURVEILLANCE	
	Meaning: The command failed because a CDC is already associated with the specified surveillance. **Action:** Contact the LEA to discuss further action. If required, disassociate the CDC using the CDC DISASSOC command and re-enter the command.
AGENCY FAILED: UNAUTHORIZED COMMAND.	
	Meaning: User is not authorized to use AGENCY command. **Action:** None.
AGENCY FAILED: USNBD IS NOT ACTIVE.	
	Meaning: USNBD SOC is IDLE. **Action:** Turn the USNBD SOC ON.
AGENCY FAILED: USNBD RECOVERY IN PROGRESS, PLEASE TRY AGAIN LATER.	
	Meaning: After a RESTART (cold or reload), USNBD performs some initialization. The AGENCY command cannot be used during that short period of time. **Action:** Try again few seconds later.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
AGENCY FAILED: USNBD DATA TRANSFER IN PROGRESS, PLEASE TRY AGAIN LATER.	
	Meaning: A load application is in progress. The AGENCY command is not allowed while USNBD data is being transferred. **Action:** Try again later, when the load application is completed.
AGENCY ADD FAILED: INTERNAL ERROR.	
	Meaning: USNBD is not able to claim FLAG for executing AGENCY ADD command. **Action:** Try again later.
AGENCY ADD FAILED: STS NOT FOUND IN TABLE HNPACONT	
	Meaning: STS specified in the AGENCY ADD command does not exist in table HNPACONT. **Action:** Verify that the user assigned the correct STS value with the agency through AGENCY command. If the current agency STS is correct, it should be validated that the value does not exist in the table HNPACONT. The user should invoke the operating company procedure to add the missing datafill to the table. Then re-issue the AGENCY ADD command.
AGENCY ADD FAILED: PRETRANSLATOR NOT FOUND IN TABLE STDPRTCT	
	Meaning: PRETRANSLATOR specified in the AGENCY ADD command does not exist in table STDPRTCT. **Action:** Verify that the user assigned the correct PRETRANSLATOR value with the agency using AGENCY ADD command. If the current agency PRETRANSLATOR is correct, confirm that the value does not exist in table STDPRTCT. The user should invoke the operating company procedure to add the missing datafill to the table. Then re-issue the AGENCY ADD command.
AGENCY ADD FAILED: LCANAME NOT FOUND IN TABLE LCASCRCN OR LCA INFO.	
	Meaning: LCANAME specified in the AGENCY ADD command does not exist in table LCASCRCN or LCA. **Action:** Verify that the user assigned the correct LCANAME value with the agency via AGENCY command. If the current agency LCANAME is correct, confirm that the value does not exist in table LCASCRCN or LCA. The user should invoke the operating company procedure to add the missing datafill to the table. Then re-issue the AGENCY ADD command.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
AGENCY ADD FAILED: BILLING NUMBER MUST BE OF 10 DIGITS.	
	Meaning: 10 digit bill number is not specified in the AGENCY ADD command. **Action:** Re-issue the AGENCY ADD command with proper 10 digit bill number.
AGENCY ADD FAILED: AGENCY CAPACITY EXCEEDED FOR SWITCHED ISUP CCCS.	
	Meaning: User is trying to add 9th agency with switched ISUP CCC feature. **Action:** None.
AGENCY ADD FAILED: AGENCY ALREADY EXISTS.	
	Meaning: User is trying to add agency data with similar agency name that already exists. **Action:** None.
AGENCY DEL FAILED: INTERNAL ERROR.	
	Meaning: USNBD is not able to claim FLAG for executing AGENCY DEL command. **Action:** Try again later.
AGENCY DEL DONE.	
	Meaning: Agency data used for translation pertaining to specified agency is deleted. **Action:** None.
AGENCY DEL FAILED: NO MATCHING AGENCY FOUND	
	Meaning: Agency specified in the AGENCY DEL command does not exist. **Action:** Verify that the agency exists using AGENCY LIST command.
AGENCY LIST FAILED: INTERNAL ERROR.	
	Meaning: USNBD is not able to claim FLAG for executing AGENCY LIST command. **Action:** Try again later.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
ANOTHER NBD APPLICATION ALREADY ACTIVE	
	Meaning: The command failed because another network broadcast delivery (NBD) application is active. **Action:** Contact your next level of support.
BOTH CCCS ARE THE SAME	
	Meaning: The command failed because the two CCCs entered refer to the same CCC. **Action:** Verify the DN of the line or CLLI and trunk member of the line or trunk to be used as the CCC and re-enter the command.
BOTH CCR DNS ARE THE SAME	
	Meaning: The command failed because you entered the same DN for each of the CCCs of a separated CCR. **Action:** Re-enter the command and ensure you enter the correct DN for each CCC, which must be different from one another.
CANNOT DELETE THE ONLY REMAINING ADMINISTRATOR	
	Meaning: The command failed because the user to be deleted is the only remaining administrator. **Action:** At least one USNBD administrator must be defined at all times.
CANNOT ESTABLISH SVC ON CDC	
	Meaning: The command failed because USNBD could not establish a switched virtual circuit (SVC) on the specified CDC. **Action:** Verify the CDC information in table MPCLINK, as well as the X.25 connection. If required, contact the LEA to discuss further action.
CANNOT FIND DN	
	Meaning: The command failed because the DMS was unable to get the DN from the CPID. **Action:** Re-enter the command and ensure the DN you enter for the surveillance is a valid DN.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
CCC1 AND CCC2 ARE BUSY	
	Meaning: The command failed because USNBD was unable to establish communication with both CCCs. **Action:** Verify the CCC line or trunk state and the equipment. If required, contact the LEA to discuss further action.
CCC1 IS BUSY, NO ANSWER FROM CCC2	
	Meaning: The command failed because USNBD was unable to establish communication with both CCCs. **Action:** Verify the CCC line or trunk state and the equipment. If required, contact the LEA to discuss further action.
CCCn ALREADY USED	
	Meaning: The command failed because the DN or CLLI name you specified for the CCC (CCC1 or CCC2) is already in use. **Action:** Re-enter the command and ensure you enter the correct DN or CLLI name. If this message is displayed again, verify the datafill for the line or trunk. If required, contact the LEA to discuss further action.
CCCn CLLI INVALID	
	Meaning: The command failed because the CLLI specified for the CCC (CCC1 or CCC2) does not exist in the switch. **Action:** Re-enter the command and ensure you enter the correct CLLI name. If this message is displayed again, verify the datafill in table CLLI.
CCCn DN INVALID FOR THIS SWITCH	
	Meaning: The command failed because the DN you specified for the CCC (CCC1 or CCC2) is not a 10-digit DN. **Action:** Re-enter the command using the correct 10-digit DN for the CCC. If required, contact the LEA to discuss further action.
CCCn DN MUST BE ASSIGNED TO A LEN	
	Meaning: The command failed because the DN you specified for the CCC (CCC1 or CCC2) is not assigned to a line equipment number (LEN). **Action:** Re-enter the command and ensure you enter the correct DN. If this message is displayed again, verify the datafill for the DN. If required, contact the LEA to discuss further action.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
CCCn HAS UNSUPPORTED FEATURES	
	Meaning: The command failed because the DN you specified for the CCC (CCC1 or CCC2) has one or more non-monitorable features assigned to it. **Action:** Re-enter the command and ensure you enter the correct DN. If this message is displayed again, verify the datafill for the DN. If required, contact the LEA to discuss further action.
CCCn IS BUSY	
	Meaning: The command failed because USNBD was unable to establish communication with the specified CCC. **Action:** Verify the CCC line or trunk state and the equipment. If required, contact the LEA to discuss further action.
CCCn IS UNDER SURVEILLANCE	
	Meaning: The command failed because monitoring on the specified CCC (CCC1 or CCC2) is in progress. **Action:** Contact the LEA that requested the surveillance on the CCC. Deactivate and delete the surveillance.
CCCn LINE DATA IS CORRUPTED	
	Meaning: The command failed because the DN of the specified CCC (CCC1 or CCC2) has corrupted data. **Action:** Contact your Nortel representative.
CCCn LINE MUST BE POTS 1FR, POT 1MR, OR RES	
	Meaning: The command failed because the DN you specified for the CCC (CCC1 or CCC2) is not associated with a POTS 1FR, POTS1MR, or RES line. **Action:** Verify that the line type associated with the DN is 1FR, 1MR, or RES. Re-enter the command.
CCCn TRUNK MEMBER INVALID	
	Meaning: The command failed because the trunk member specified by the given CLLI group and external trunk name does not exist (for CCC1 or CCC2). **Action:** Verify the CLLI and trunk number and re-enter the command.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
`CCR ADD FAILED: SWITCHED CCC DN MUST BE OF 10 OR 11 DIGITS`	
	Meaning: CCC DN(s) specified in the CCR ADD command for switched access type of CCR are not 10 to 11 digits long. **Action:** Find a new valid remote CCC DN. Replace the local directory number originally entered by the new one. Re-issue the CCR ADD subcommand with the new parameters.
`CCR ADD FAILED: SWITCHED CCC DN <DN> PRESENT ON THE HOST SWITCH.`	
	Meaning: With switched access, CCC DN given as a parameter in the CCR ADD subcommand should not be a local DN. **Action:** Find a new valid remote CCC DN. Replace the local directory number originally entered by the new one. Re-issue the CCR ADD subcommand with the new parameters.
`CCR AGENCY NOT SAME AS SURVEILLANCE AGENCY`	
	Meaning: The agency of the CCR is different from the agency of the surveillance. To associate a CCR, the agency of the CCR and surveillance must be the same. **Action:** None.
`CCR ALREADY ASSOCIATED`	
	Meaning: The command failed because the CCR you specified is already associated with a surveillance. **Action:** Re-enter the command and ensure you enter the correct CCR and SIN. If required, contact the LEA to discuss further action.
`CCR ASSOCIATED WITH A SURVEILLANCE`	
	Meaning: The command failed because the CCR you specified is currently associated with a surveillance. **Action:** Re-enter the command and ensure you enter the correct CCR and SIN. If required, contact the LEA to discuss further action.
`CCR CAPACITY EXCEEDED FOR THIS SURVEILLANCE`	
	Meaning: The command failed because the maximum number of CCRs allowed for the specified surveillance has been reached. **Action:** Contact the LEA that requested to have the CCR associated with the surveillance to discuss further action.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
CCR DOES NOT EXIST	
	Meaning: The command failed because the CCR you specified does not exist. **Action:** Re-enter the command and ensure you enter the correct CCR index. If required, contact the LEA to discuss further action.
CCR NOT ASSOCIATED	
	Meaning: The command failed because the CCR you specified is not associated with any surveillances. **Action:** Re-enter the command and ensure you enter the correct CCR index. If required, contact the LEA to discuss further action.
CCRS ARE STILL PRESENT	
	Meaning: The command failed because some CCRs are still present in the USNBD data. **Action:** Contact the LEAs to determine whether the CCRs are still required. If the CCRs are no longer required, delete each of the remaining CCRs using the CCR DEL command, and re-enter the command.
CDC AGENCY NOT SAME AS SURVEILLANCE AGENCY	
	Meaning: The agency of the CDC is different from the agency of the surveillance. When associating a CDC to a surveillance, the agency must be the same. **Action:** None.
CDC ASSOCIATED WITH A SURVEILLANCE	
	Meaning: The command failed because the CDC you specified is associated with at least one surveillance. **Action:** Re-enter the command and ensure you enter the correct CDC and SIN. If required, contact the LEA to discuss further action.
CDC MESSAGES STILL WAITING TO BE SENT, PLEASE TRY AGAIN LATER	
	Meaning: The command failed because the CDC message queue still contains some CDC messages, which need to be sent. **Action:** Re-enter the command at a later time.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
CDCS ARE STILL PRESENT	
	Meaning: The command failed because some CDCs are still present in the USNBD data. **Action:** Contact the LEAs to determine whether the CDCs are still required. If the CDCs are no longer required, delete each of the remaining CDCs using the CDC DEL command, and re-enter the command.
DMS RESOURCES NOT AVAILABLE (FTRQ)	
	Meaning: The command failed because no feature queue (FTRQ) is available to be associated with the surveillance. **Action:** Re-enter the command at a later time.
DMS RESOURCES NOT AVAILABLE (MAILBOX)	
	Meaning: The command failed because no mailboxes were available upon request. **Action:** Re-enter the command at a later time.
DN IS EXISTING CCR	
	Meaning: The command failed because the DN you specified for the surveillance corresponds to a CCC. **Action:** If the DN corresponds to a CCC, contact the LEA to discuss further action.
DN IS UNDEFINED OR DOES NOT UNIQUELY IDENTIFY A SUBJECT	
	Meaning: The command failed because the DN you specified is not assigned to a line equipment number (LEN) or does not correspond to a unique LEN or key. **Action:** Re-enter the command and ensure you enter the correct DN. If required, contact the LEA to discuss further action.
DN MUST BE 10 DIGITS	
	Meaning: The command failed because the DN you specified for the surveillance is not a 10-digit DN. **Action:** Re-enter the command and ensure the DN you enter for the surveillance is a 10-digit DN.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
HANDLE NOT SUPPORTED FOR THIS SUBJECT	
	Meaning: The command failed because the handle you specified to identify the subject is not supported for this type of subject. For example, an ISDN subject cannot be identified using the LEN handle. **Action:** Re-enter the command and ensure you specify the correct handle to identify the subject.
INDEX ALREADY IN USE	
	Meaning: The command failed because the index you specified for the CCR or CDC is already in use. **Action:** Display a list of unused CCR indexes using CCR LIST FREE or unused CDC indexes using CDC LIST FREE, and re-enter the command using a free index.
INTERNAL ERROR	
	Meaning: The command failed because an unexpected error occurred. **Action:** Capture any SWER logs and contact your Nortel representative.
INVALID ADDRESS	
	Meaning: The command failed because you specified and invalid address for the X.25 link. **Action:** Re-enter the command and ensure you specify the correct address. If required, contact the LEA to verify the address.
INVALID AGENCY NAME	
	Meaning: The agency name entered by the ADMIN exceeds the maximum allowed size of agency. Names should be no more than 16 characters long. **Action:** None.
INVALID MPC LINK	
	Meaning: The command failed because the MPC link you specified is either undefined or does not correspond to an existing X.25 link. **Action:** Re-enter the command and ensure you enter the correct MPC link number. If this message is displayed again, verify tables MPC and MPCLINK to ensure the MPC link is defined. If required, contact the LEA to discuss further action.
INVALID NEW USER NAME	

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
	Meaning: The command failed because the user name you specified is not a valid CI user name. **Action:** Re-enter the command and ensure you enter the correct user name and that the user name is a valid CI user name.
INVALID PROTOCOL	
	Meaning: The command failed because the protocol you specified for the MPC link is invalid. **Action:** Re-enter the command and ensure you enter the correct protocol. If this message is displayed again, contact the LEA to verify the protocol. (The only invalid protocol is 0 0 0 0.)
INVALID SIN	
	Meaning: The command failed because the SIN you specified contains more than 25 characters. **Action:** Re-enter the command using a SIN with a maximum of 25 characters.
LEN NOT ASSIGNED TO A DN	
	Meaning: The command failed because the LEN you specified for the surveillance is an unused line. **Action:** Re-enter the command and ensure the LEN you enter for the surveillance is for a valid working line.
MAXIMUM NUMBER OF USERS ALREADY REACHED	
	Meaning: The command failed because the maximum number of registered users has already been reached. **Action:** If required, delete a user with the USER DEL command, and add the new user with the USER ADD command.
NO ANSWER FROM CCCn	
	Meaning: The command failed because USNBD was unable to establish communication with the specified CCC. **Action:** Verify the CCC line or trunk state and the equipment. If required, contact the LEA to discuss further action.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
NO ANSWER FROM CCC1 AND CCC2	
	Meaning: The command failed because USNBD was unable to establish communication with both CCCs. **Action:** Verify the CCC line or trunk state and the equipment. If required, contact the LEA to discuss further action.
NO ANSWER FROM CCC1, CCC2 IS BUSY	
	Meaning: The command failed because USNBD was unable to establish communication with both CCCs. **Action:** Verify the CCC line or trunk state and the equipment. If required, contact the LEA to discuss further action.
NO CDC ASSOCIATED WITH THE SURVEILLANCE	
	Meaning: The command failed because no CDC is currently associated with the surveillance. **Action:** Re-enter the command and ensure you enter the correct SIN for the desired surveillance.
NOT ENOUGH MEMORY	
	Meaning: The command failed because not enough memory is available. **Action:** Re-enter the command at a later time. If this message is displayed again, contact the next level of support.
NO MATCHING AGENCY FOUND **AGENCY LIST DONE.**	
	Meaning: The translation data specific to the agency was not found. **Action:** None.
NO MATCHING USER FOUND	
	Meaning: No matching user found. No user belongs to the given agency. **Action:** None.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
RECORDING IS STARTED ONTO ANOTHER DEVICE	
	Meaning: The command failed because a recording link has been set up between devices. **Action:** Verify the status of terminal recording using the RECORD QUERY command, and stop recording using the command RECORD STOP. Re-enter the command after recording has been stopped.
SDN SUBJECT NOT SUPPORTED	
	Meaning: The command failed because the DN you specified corresponds to a secondary directory number (SDN), which is unsupported. **Action:** Contact the LEA to discuss further action. If required, re-enter the command using the primary directory number (PDN) for the SDN subject.
SIN ALREADY EXISTS	
	Meaning: The command failed because the surveillance identification number (SIN) you specified already exists. **Action:** Re-enter the command and ensure the correct SIN is entered. If required, display a list of all surveillances and their corresponding SIN using the SURV LIST ALL command.
SIN DOES NOT EXIST	
	Meaning: The command failed because the surveillance identification number (SIN) you specified does not exist. **Action:** Re-enter the command and ensure the correct SIN is entered. If required, display a list of all surveillances and their corresponding SIN using the SURV LIST ALL command to obtain the correct SIN for the desired surveillance.
SUBJECT AGENT UNEQUIPPED	
	Meaning: The command failed because the subject you specified corresponds to a line that is not datafilled in table LENLINES. **Action:** Re-enter the command and ensure you enter the correct LEN, DN, or KEY. If required, contact the LEA to discuss further action.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
SURVEILLANCE ALREADY ACTIVE	
	Meaning: The command failed because the surveillance you specified is already active. **Action:** Re-enter the command and ensure you specify the correct SIN for the desired surveillance.
SURVEILLANCE ALREADY INACTIVE	
	Meaning: The command failed because the surveillance you specified is already inactive. **Action:** Re-enter the command and ensure you specify the correct SIN for the desired surveillance.
SURVEILLANCE CAPACITY EXCEEDED	
	Meaning: The command failed because the maximum number of surveillances allowed on the switch has been reached. **Action:** Contact the LEAs to determine whether all their surveillances are still required. Delete any unnecessary surveillances using the SURV DEL command, and add the new surveillance using the SURV ADD command.
SURVEILLANCE IS ACTIVE	
	Meaning: The command failed because the surveillance you specified is active. **Action:** Re-enter the command and ensure you enter the correct SIN for the desired surveillance. If this message is displayed again, contact the LEA to determine whether the surveillance can be deactivated. If so, deactivate the surveillance using the SURV DEACT command, re-enter the command, and re-activate the surveillance.
SURVEILLANCE MUST HAVE AT LEAST ONE CCR OR CDC	
	Meaning: The command failed because a CCR nor a CDC is not associated with the specified surveillance. The command may also fail if trying to disassociate the last CCR or CDC from an active surveillance. **Action:** Contact the LEA(s) to discuss further action. If required, associate a CCR, a CDC, or both with the surveillance. Re-enter the command or deactivate the surveillance before attempting to delete the last CCR or CDC.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
`SURVEILLANCES ARE STILL PRESENT`	
	Meaning: The command failed because some surveillances are still defined. **Action:** Contact the LEAs to determine whether the surveillances are still required. If not, delete each of the remaining surveillances using the SURV DEL command, and re-enter the command.
`TEST_CALL_BILLNO ADD FAILED: BILLING NUMBER MUST BE OF 10 DIGITS.`	
	Meaning: The length of the specified TEST call billing number is invalid. **Action:** Enter proper 10 digit TEST call billing number.
`TEST_CALL_BILLNO REP FAILED: BILLING NUMBER MUST BE OF 10 DIGITS`	
	Meaning: The length of the specified TEST call billing number is invalid. **Action:** Enter proper 10 digit TEST call billing number.
`TEST FAILED: UNAUTHORIZED COMMAND`	
	Meaning: The user is not authorized to use the TEST command, or the user agency is not the same as CCR agency. **Action:** None.
`TEST FAILED: USNBD IS NOT ACTIVE`	
	Meaning: USNBD SOC is IDLE. **Action:** Turn the USNBD SOC ON.
`TEST FAILED: USNBD RECOVERY IN PROGRESS, PLEASE TRY AGAIN LATER.`	
	Meaning: After a RESTART (cold or reload), USNBD performs some initialization. The TEST command cannot be used during that short period of time. **Action:** Try again few seconds later.
`TEST FAILED: USNBD DATA TRANSFER IN PROGRESS, PLEASE TRY AGAIN LATER.`	
	Meaning: A load application is in progress. The TEST command is not allowed while USNBD data is being transferred. **Action:** Try again later after the load application is completed.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
`TEST FAILED: INTERNAL ERROR`	
	Meaning: USNBD is not able to claim FLAG for executing TEST command. **Action:** Try again later.
`TEST FAILED: CCR ALREADY ASSOCIATED.`	
	Meaning: The TEST command cannot be performed because the specified CCR is currently associated to surveillance. **Action:** Disassociate the CCR and then perform the test.
`TEST FAILED: CCR DOES NOT EXIST.`	
	Meaning: The specified CCR does not exist. **Action:** Verify that CCR is present using the CCR LIST command.
`TEST WARNING <DN>: INBAND SIGNALLING ENCOUNTERED.`	
	Meaning: At least one leg of the call has been routed over inband signaling trunks, resulting in extra delays in call setup for the specified CCR link. **Action:** None.
`TEST FAILED: CCC DN <DN> UNALLOCATED`	
	Meaning: The called party cannot be reached, or the specified number is not currently assigned. **Action:** Verify that the correct CCC DN is entered. Verify the DN with the agency.
`TEST FAILED: NO ROUTE TO CCC DN <DN>.`	
	Meaning: The network is unable to route the call to the requested destination. **Action:** Verify that the correct CCC DN is entered. Verify translation/routing tables using the TRAVER command. Verify the DN with the agency.
`TEST FAILED: CALL REJECTED BY CCC DN <DN>.`	
	Meaning: The remote switching equipment refused the call for the specified link. **Action:** Verify that the correct CCC DN is entered. Verify the DN with the agency.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
TEST FAILED: CCC DN <DN> IS OUT OF ORDER.	
	Meaning: The interface to the destination of the specified link is not functioning correctly. **Action:** Verify that the correct CCC DN is entered. Verify that the recorder interface is functioning for the agency. Verify the DN with the agency.
TEST FAILED: CCC DN <DN> CIRCUIT IS NOT AVAILABL	
	Meaning: There is no appropriate circuit currently available to handle the call for the specified link. **Action:** Verify that the correct CCC DN is entered. Verify that trunks are available (in IDLE state) in the required route(s) identified using the TRAVER command, then retry. Verify the DN with the agency.
TEST FAILED: NETWORK FOR CCC DN <DN> IS TEMPORARILY OUT OF ORDER.	
	Meaning: The specified link could not be established because the network is not functioning properly for an indefinite period of time. **Action:** Try again later.
TEST FAILED: NETWORK CONGESTION FOR CCC DN <DN>	
	Meaning: The specified link could not be established because the network is experiencing a period of high traffic. **Action:** Try again later.
TEST FAILED: TEST_CALL_BILLNO MISSING.	
	Meaning: The specified CCC DN TEST call is a billable call and there is no TEST_CALL_BILLNO parameter defined in UNB_OFCWIDE. **Action:** Verify that the call is intended to be billable. If billable, define a TEST_CALL_BILLNO using the UNB_OFCWIDE command. If not billable, find a valid non-billable DN and re-assign it to the current CCC.
TEST FAILED: EXTENSION BLOCK NOT AVAILABLE.	
	Meaning: There are no more NBD extension blocks available to make the connection for the specified CCC link. **Action:** None.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
TEST FAILED: DMS RESOURCES NOT AVAILABLE.	
	Meaning: Some DMS switch resources are not available to make the connection for the specified CCC link. **Action:** Examine AUD594 logs. Verify that no more VIDS are available.
TEST FAILED: COMMUNICATION PROBLEM, PLEASE TRY AGAIN.	
	Meaning: After issuing the TEST command, no response was received, within the maximum time allowed, to acknowledge the proper establishment of the specified CCC link. This should be a temporary situation. **Action:** Try again later.
TEST FAILED: TRANSLATIONS FAILED FOR CCC DN <DN>.	
	Meaning: The specified DN does not translate properly. **Action:** Verify that the correct CCC DN is entered. Verify the translation tables using the TRAVER command. Verify the DN with the agency.
TEST FAILED: ROUTING FAILED FOR CCC DN <DN>.	
	Meaning: A route cannot be found for the specified DN digits. **Action:** Verify that the correct CCC DN is entered. Verify the translation/routing tables using the TRAVER command. Verify the DN with the agency.
TEST FAILED: UNSUPPORTED TRUNK TYPE.	
	Meaning: The trunk type used to route to the specified DN is not supported. The trunk types should be ISUP trunks (TO, IT, T2). **Action:** Verify that the translations are correct using the TRAVER command. If necessary, change translations to route to a supported trunk type.
TEST FAILED: CCC DN <DN> IS BUSY.	
	Meaning: The specified DN is in Call Processing Busy state. **Action:** Verify that the correct CCC DN is entered. If it is a DN locally defined on the switch, post the DN at the MAP LTP level to determine the connected line or trunk and take any necessary steps to release the line. Contact the agency to verify if the recorder is off-hook and verify the DN.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
TEST FAILED: MESSAGING PROBLEM- DN <DN>.	
	Meaning: The connection to the specified DN cannot be made due to some USNBD messaging problem. **Action:** Verify if SWERR logs are being generated and refer them to your support group.
TEST FAILED: DISCONNECTED DURING CALL SETUP TO CCC DN <DN>.	
	Meaning: The link associated with the DN answered and then disconnected. **Action:** Verify that the correct CCC DN is entered. Verify that the recorder interface (to the line) with the agency is functioning. Verify the DN with the agency.
TEST FAILED: NO ANSWER FROM CCC DN <DN>.	
	Meaning: The link associated with the DN did not return an answer within the maximum time allowed. **Action:** Verify that the correct CCC DN is entered. Verify that the recorder interface (to the line) with the agency is functioning. Verify the DN with the agency.
TEST FAILED: NO CSIDE LINKS FOR CCC DN <DN>.	
	Meaning: The internal DMS linkage is out of service between the network and the Peripheral Module (PM) to which the specified link (DN) is assigned. **Action:** Refer problem to the maintenance personnel responsible for the DMS switch for corrective action.
TEST FAILED: UNKNOWN PROBLEM.	
	Meaning: Due to some unknown problem (not a resource or communication problem), the link could not be established for the specified DN. This should be temporary. **Action:** Examine LOSTXXX, PM180, and SWERR logs.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
TOO MANY SURVEILLANCES ON SUBJECT	
	Meaning: The command failed because the maximum number of surveillances on the subject has been reached. **Action:** Contact the LEAs to determine whether all surveillances on the subject are still required. Delete any unnecessary surveillances using the SURV DEL command, and add the new surveillance using the SURV ADD command.
UNABLE TO PREVENT OTHER DEVICES FROM RECORDING	
	Meaning: The command failed because recording cannot be disabled for the device on which a USNBD user is working; therefore, recording could be started onto another device. **Action:** Re-enter the command at a later time. If required, contact the next level of support.
UNAUTHORIZED COMMAND	
	Meaning: The command failed for one of the following reasons: • an unauthorized user attempted to access the USNBD command or its subcommands, which are only accessible to USNBD users • a USNBD user without administrator privileges entered the USNBD USER command, which is only accessible to USNBD users with administrator privileges • an unauthorized user or a USNBD user without administrator privileges attempted to enter the SOC commands related to USNBD, which can only be entered by a USNBD user with administrator privileges unless no administrator has ever been defined • an unauthorized user attempted to access logs UNB300, UNB301, UNB302, UNB303, or UNB304, which are only accessible to USNBD users (with or without administrator privileges) • an unauthorized user or a USNBD user without administrator privileges attempted to access log UNB305, which is only accessible to USNBD users with administrator privileges **Action:** If this response is displayed for a user who is not defined as a USNBD user, but needs access to USNBD, contact a USNBD administrator who can add USNBD users. It may be necessary to contact your Nortel representative if the last administrator was deleted and can no longer access USNBD.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
UNDEFINED CCR	
	Meaning: The command failed because the CCR you specified does not exist. **Action:** Re-enter the command and ensure you enter the correct index for the CCR. If required, contact the LEA to discuss further action.
UNDEFINED CDC	
	Meaning: The command failed because the CDC you specified does not exist. **Action:** Re-enter the command and ensure you enter the correct index for the CDC. If required, contact the LEA to discuss further action.
UNDEFINED LEN	
	Meaning: The command failed because the line equipment number (LEN) you specified is not defined on the switch. **Action:** Re-enter the command and ensure you enter the correct LEN. If required, contact the LEA to discuss further action
UNDEFINED LEN/KEY COMBINATION	
	Meaning: The command failed because the KEY you specified does not exist on the specified LEN, or the LEN does not exist. **Action:** Re-enter the command and ensure you enter the correct LEN and correct key. If required, contact the LEA to discuss further action.
UNDEFINED LTID	
	Meaning: The command failed because the logical terminal id (LTID) you specified is not defined on the switch. **Action:** Re-enter the command and ensure you enter the correct LTID.
UNSUPPORTED AGENT	
	Meaning: The command failed because the subject you specified either corresponds to a line that has one or more unsupported features, or to an unsupported line type. **Action:** Contact the LEA to discuss further action.

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
UNSUPPORTED TRUNK BEARER CAPABILITY ON CCCn	
	Meaning: The command failed because the CCCn trunk member specified (CCC1 or CCC2) has a bearer capability other than 64KDATA. **Action:** Select a trunk member with 64KDATA bearer capability and re-enter the command.
UNSUPPORTED TRUNK DIRECTION ON CCCn	
	Meaning: The command failed because the CCC trunk member specified (CCC1 or CCC2) has a direction other than OG (outgoing). **Action:** Verify the direction of the CLLI in table TRKGRP and re-enter the command, or select another CLLI and trunk member and re-enter the command.
UNSUPPORTED TRUNK TYPE ON CCCn	
	Meaning: The command failed because the CCC trunk member specified (CCC1 or CCC2) has a trunk type other than NU (nailed up). **Action:** Verify the entry for the Signal Data Selector in field SUBGRPVAR in table TRKSGRP for the CLLI and re-enter the command, or select another CLLI and trunk member and re-enter the command.
USER AGENCY NOT SAME AS CCR AGENCY	
	Meaning: The agency of the user executing the command is different from the agency of the CCR. The user must have the same agency as the CCR to perform this procedure. **Action:** None.
USER AGENCY NOT SAME AS CDC AGENCY	
	Meaning: The agency of the user executing the command is different from the agency of the CDC. **Action:** None.
USER AGENCY NOT SAME AS SURVEILLANCE AGENCY	
	Meaning: The agency of the user executing the command is different from the agency of the surveillance. **Action:** None.
USER ALREADY EXISTS	

Error responses for USNBD commands (Continued)

MAP output	Meaning and action
	Meaning: The command failed because the user name you specified already exists. **Action:** Re-enter the command and ensure you enter the correct user name.
USER NOT FOUND	
	Meaning: The command failed because the user you specified does not exist in the list of defined USNBD users. **Action:** Re-enter the command and ensure you enter the correct user id. If required, verify the list of users with the USER LIST command.
USNBD DATA TRANSFER IN PROGRESS, PLEASE TRY AGAIN LATER	
	Meaning: The command failed because a one-night process (ONP) or switch of activity (SWACT) is in progress. **Action:** Re-enter the command once the ONP or SWACT is complete or aborted.
USNBD IS NOT ACTIVE	
	Meaning: The command failed because USNBD is not active. **Action:** If required, activate USNBD through the SOC utility.
USNBD RECOVERY IN PROGRESS, PLEASE TRY AGAIN LATER	
	Meaning: The command failed because the USNBD recovery process is running. **Action:** Re-enter the command once the USNBD recovery process is complete.
YOU ARE ALREADY IN USNBD	
	Meaning: The user is attempting to reaccess USNBD while already in the USNBD directory. **Action:** All USNBD commands can be accessed from the current session.

Information-type messages

The following messages are generated to provide information to the user.

Information-type messages

MAP output	Meaning and action
`OTHER USERS ARE ACCESSING USNBD DATA. PLEASE WAIT...`	
	Meaning: The current user has attempted to administer a change which is temporarily delayed. The delay is because other users are performing changes, or an audit process is running that checks internal data consistency. The command will be completed when the data can be safely changed. **Action:** No action.
`WARNING: THERE IS NO USNBD ADMINISTRATOR DEFINED`	
	Meaning: All USNBD administrators have been deleted. If any USNBD users (without administrator privileges) exist, they can continue to provision surveillances. It is not possible to either create new USNBD users or change the state of the USNBD SOC option. **Action:** Contact your Nortel Networks representative for assistance.
`WARNING: THERE IS ONLY ONE USNBD ADMINISTRATOR DEFINED`	
	Meaning: Only one USNBD administrator is currently defined. **Action:** It is strongly recommended that another USNBD administrator be created as soon as possible. If the one and only USNBD administrator is deleted, new USNBD users cannot be created, nor can the USNBD SOC option be set to ON or IDLE.
`YOU HAVE BEEN DEFINED AS THE INITIAL USNBD ADMINSTRATOR`	
	Meaning: A user has activated USNBD for the first time through the SOC utility, which automatically makes that user the initial USNBD administrator. **Action:** No action is required. However, it is strongly recommended that another USNBD administrator be created as soon as possible. If the one and only USNBD administrator is deleted, new USNBD users cannot be created, nor can the USNBD SOC option be set to ON or IDLE.

Chapter 4: Operational measurements

This chapter describes the CF3P, EXT, FCNF, UNBCDC, UNBMISC, and XLIUL3 operational measurement (OM) groups used by the USNBD feature.

OM group CF3P

OM description

The registers in OM group CF3P provide information on the use of three-port conference circuits. The information includes the number of times the system seized a circuit, the number of times a circuit was not available, and the number of queue overflows and abandons.

The USNBD feature uses the registers in OM group CF3P to monitor the usage of three-way conference bridges used for combined CCRs.

Release history

OM group CF3P was introduced before BCS20.

Registers

The CF3P OM group registers display on the MAP terminal in a non-TOPS office as follows:

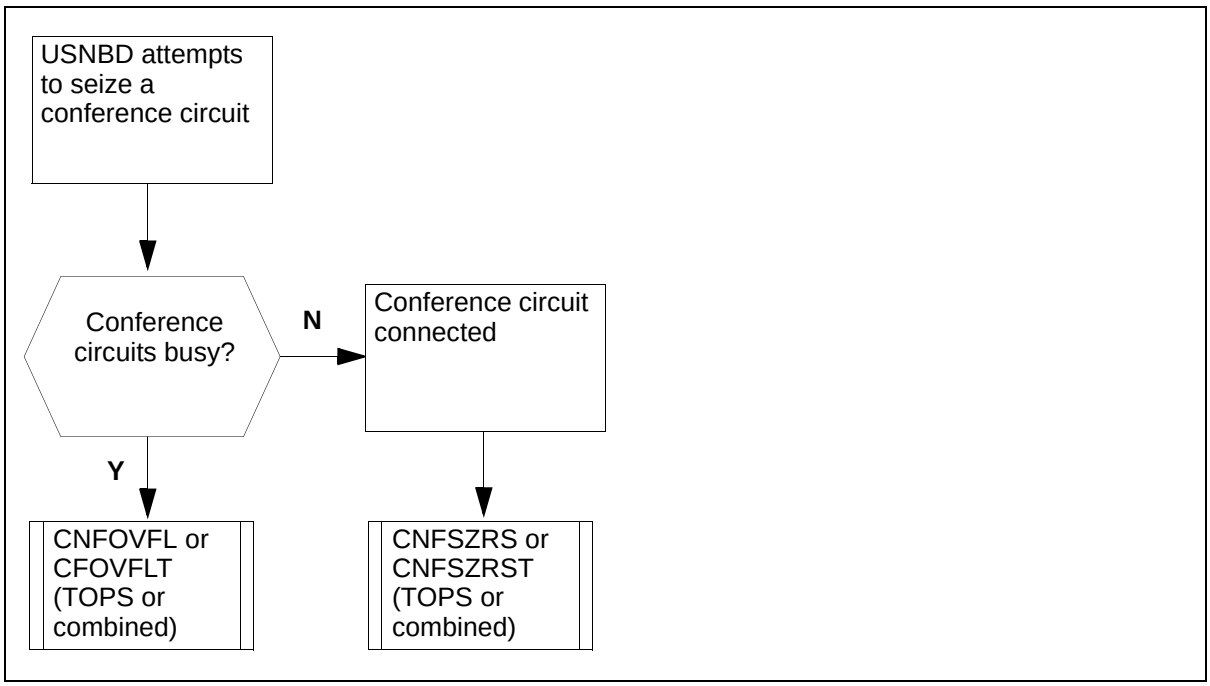
```
CNFSZRS     CNFOVFL      CNFQOCC     CNFQOVFL
CNFQABAN    CNFTRU       CNFSBU      CNFMBU
```

The CF3P OM group registers display on the MAP terminal in a TOPS office as follows:

```
CNFSZRST     CNFOVFLT      CNFQOCCT     CNFQOVFT
CNFQABNT    CNFTRUT       CNFSBUT      CNFMBUT
TOPSZRS    TOPSOVFL       TOPSTRU
```

OM group CF3P

OM group CF3P registers



Group structure

Key field: Common language name.
Info field: Conference member number.

Associated OM group

None

Associated functional groups

None

Associated functionality codes

None

OM group CF3P

Register CNFSZRS

Register CNFSZRS increases when the system assigns a circuit in response to a request, before an attempt to set up network paths to the three ports.

This register is used in non-TOPS environments.

Release history

Register CNFSZRS was introduced before BCS20.

Associated registers

None

Associated logs

None

Register type

Register CNFSZRS is a peg-type register.

Extension registers

None

Register CNFOVFL

Register CNFOVFL increases when the system cannot satisfy a request for a three-port conference circuit immediately because all conference circuits are busy.

This register is used in non-TOPS environments.

Release history

Register CNFOVFL was introduced before BCS20.

Associated registers

When register FCNFFAIL is pegged, one CNFOVFL is also pegged.

Associated logs

None

Register type

Register CNFOVFL is a peg-type register.

Extension registers

None

OM group CF3P

Register CNFQOCC

CF3P queue occupancy (CNFQOCC)

Register CNFQOCC is a usage register. Every 10 s, the system scans conference circuits and CNFQOCC records. The system scans if requests for a conference circuit are waiting in the queue. The queue consists of waiting service analysis and trunk test position requests only.

The system uses this register in non-TOPS environments.

Release history

Register CNFQOOC was introduced before BCS20.

Associated registers

There are no associated registers.

Associated logs

There are no associated logs.

Register CNFQOVFL

CF3P queue overflows (CNFQOVFL)

Register CNFQOVFL counts attempts to enter the wait queue when the queue is full. Only requests from trunk test or service analysis positions increase this register. Other requests do not attempt to wait.

The system uses this register in non-TOPS environments.

Release history

Regsiter CNFQOVFL was introduced before BCS20.

Associated registers

There are no associated registers.

Associated logs

The line maintenance subsytem generates log LINE 138 when the system routes a call to a treatment after being call processing busy.

The trunk maintenance subsystem generates log LINE 138 when the system routes a call to a treatment after being call processing busy.

OM group CF3P

Register CNFQABAN

Register CF3P queue abandons (CNFQABAN)

Register CNFQABAN counts circuit requests abandoned while the requests wait in the conference circuit queue.

The system uses this register in non-TOPS environments.

Release history

Register CNFQABAN was introduced before BCS20.

Associated registers

There are no associated registers.

Associated logs

The line maintenance subsystem generates the following logs when the system encounters problems during call processing: LINE104, LINE105, LINE109, and LINE204.

Register CNFTRU

CF3P traffic busy usage

Register CNFTRU is a usage register. Every 10 s, the system scans the conference circuits and CNFTRU records if the circuits are call processing busy, unloaded, or locked out.

The system uses this register in non-TOPS environments.

Release history

Register CNFTRU was introduced before BCS20. In BCS20, the register was modified to allow the system to record the usage count in deci-erlangs or CCS.

Associated registers

There are no associated registers.

Associated logs

There are no associated logs.

Register CNFSBU

CF3P system busy usage (CNFSBU)

OM group CF3P

Register CNFSBU is a usage register. Every 10 s, the system scans conference circuits. CNFSBU records if the conference circuits are remote busy, peripheral module busy, system busy, carrier failed, or unloaded. A conference request that originated in the system can place the conference circuits in these states.

The system uses this register in non-TOPS environments.

Release history

Register CNFSBU was introduced before BCS20. In BCS20, the register was modified to allow the system to record the usage count in deci-erlangs or CCS.

Associated registers

There are no associated registers.

Associated logs

The trunk maintenance subsystem generates log TRK106 when a diagnostic test on trunk equipment fails.

Register CNFMBU

CF3P manual busy usage (CNFMBU)

Register CNFMBU is a usage register. Every 10 s, CNFMBU scans the conference circuits. CNFMBU records the number of conference circuits that are in any of the following states during the last OM transfer period:

- manual busy
- seized
- network management procedures

Maintenance personnel can seize a circuit for diagnostic tests while working from the trunk test position at the MAP terminal. Personnel working the automatic trunk test (ATT) system can seize a circuit for diagnostic tests. A system audit on the conference ports can also seize a circuit for diagnostic tests.

The system updates the active register every 10 s with the number of CF3Ps that are in any of the previously listed states. For example, if one conference port is manual busy, the active register increases by 1 every 10s. The register will continue to increase for as long as the port is in this state. The register also increases if the system seizes one of the ports for a system audit. The system copies the accumulated count to the holding register (CNFMBU)

OM group CF3P

every 30 min (and erases the previous value). If no ports are in these busy states, CNFMBU will show a value that is not zero. Values that are not zero will only appear if the system counted a port during the last OM transfer period (30 min).

Non-TOPS environments use this register.

Release history

Register CNFMBU was introduced before BCS20. In BCS20, the register was modified to allow the system to record the usage count in deci-erlangs rather than CCS.

Associated registers

There are no associated registers.

Associated logs

There are no associated logs.

OM group EXT

OM group EXT

OM description

The EXT OM group records usage statistics for extension blocks. Extension blocks primarily store feature data on a per-call basis.

The USNBD feature uses the 126 FBSEXT entry, which monitors the extension blocks used by USNBD.

Release history

The EXT OM group was introduced before BCS20.

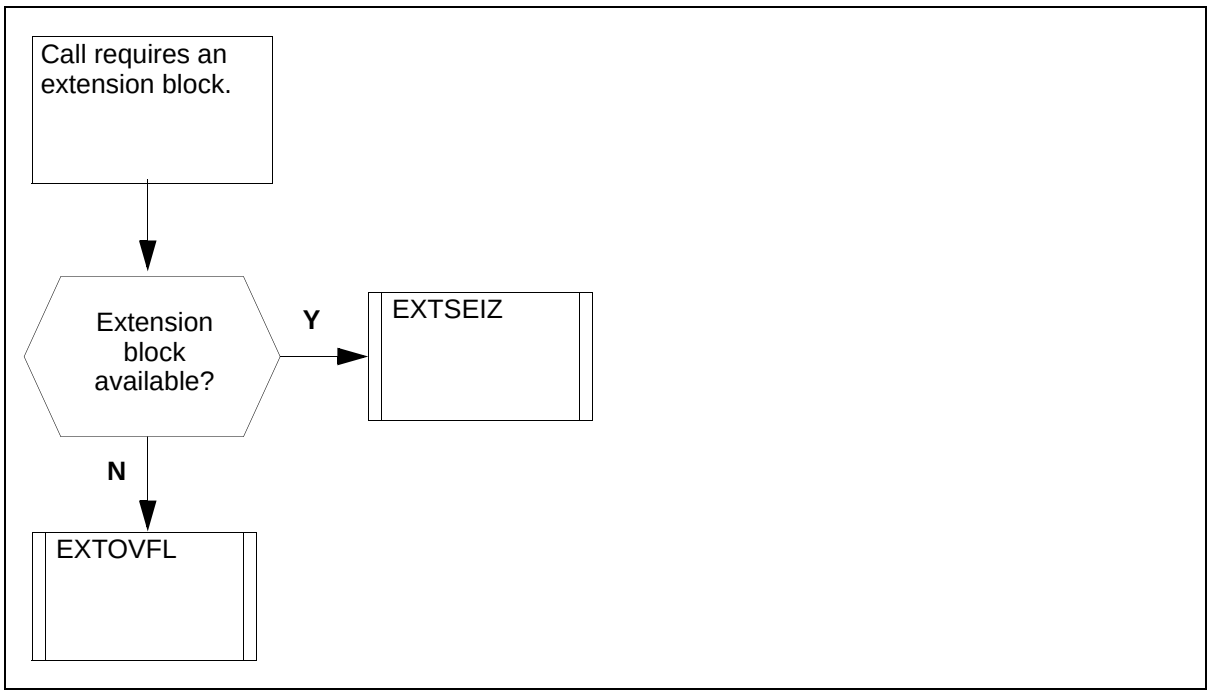
Registers

The EXT OM group registers display on the MAP terminal as follows:

```
> omshow ext active 126

EXT

CLASS: ACTIVE
START: 1998/08/08 08:00:00 SAT; STOP: 1998/08/08 08:08:41
SAT;
SLOW SAMPLES              6; FAST SAMPLES            52;

         KEY (EXT_FORMAT_CODE)
         INFO (EXTINFO)
          EXTSEIZ   EXTOVFL      EXTHI   EXTSEIZ2
           EXTHI2

  126 FBSEXT
             0
              0      0            0          0
               0
```

OM group EXT

OM group EXT registers



Group structure

Key field: EXT_FORMAT_CODE
EXT_FORMAT_CODE: 126 FBSEXT
Info field: EXTINFO indicates the number of blocks provisioned.

Associated OM group

None

Associated functional groups

None

Associated functionality codes

None

Register EXTSEIZ

Register EXTSEIZ monitors the number of requests for a particular type of extension block. EXTSEIZ increases when a request for a particular type of extension block is successful.

OM group EXT

Release history
Register EXTSEIZ was introduced before BCS20.

Associated registers
None

Associated logs
None

Register type
Register EXTSEIZ is a peg-type register.

Extension registers
EXTSEIZ2

Register EXTOVFL

Register EXTOVFL increases when the particular type of extension block requested for a call is not available. If call processing cannot allow the call to wait for a second attempt or if the occurrence is a second attempt failure, the call is routed to no-service-circuit (NOSC) treatment.

Release history
Register EXTOVFL was introduced before BCS20.

Associated registers
None

Associated logs
None

Register type
Register EXTOVFL is a peg-type register.

Extension registers
None

OM group EXT

Register EXTHI

Register EXTHI records the maximum number of extension blocks (of a specific type) that are in simultaneous use during the preceding OM transfer period (15 or 30 min.). To predict peak usage accurately, gather high water marks for the busiest hours of the busiest days of the year (following either the High Day Busy Hour or the Extreme Value Engineering provisioning concept). Use these data to calculate and adjust the provisioning of extension blocks, so that they are never more than about 80% utilized during the busiest times.

At the beginning of each transfer period, the active register initializes to the number of extension blocks that are currently in use. The active register updates continuously throughout the transfer period whenever the number of blocks that are currently in use exceeds the previously recorded value.

At the end of the transfer period (15 or 30 min.), the active register value transfers to the holding register (EXTHI) where it resides without change until it is overwritten at the end of the next transfer period.

True peak utilization can be predicted by taking the maximum value of all the high water marks observed during individual transfer periods during the busiest days of the year. An additional amount should be added to this value to ensure that the target 80% peak utilization of software resources is not exceeded, even during the busiest times. The calculated value is datafilled in the office parameter in table OFCENG for each particular type of extension block.

Release history

Register EXTHI was introduced in BCS23.

Associated registers

None

Associated logs

None

Register type

Register EXTHI is a peg-type register.

Extension registers

EXTHI2

OM group FCNF

OM group FCNF

OM description

The FCNF OM group is used to track successful and unsuccessful attempts to seize service circuits.

The USNBD feature uses the FCNFSUCC, FCNFFAIL, DTMFSUCC, DTMFFAIL, RCVRSUCC, and RCVRFAIL registers in the FCNF OM group to count the number of times USNBD makes a successful or unsuccessful attempt to seize a service circuit for combined call content resources (CCRs).

Release history

The FCNF OM group was introduced in NA005.

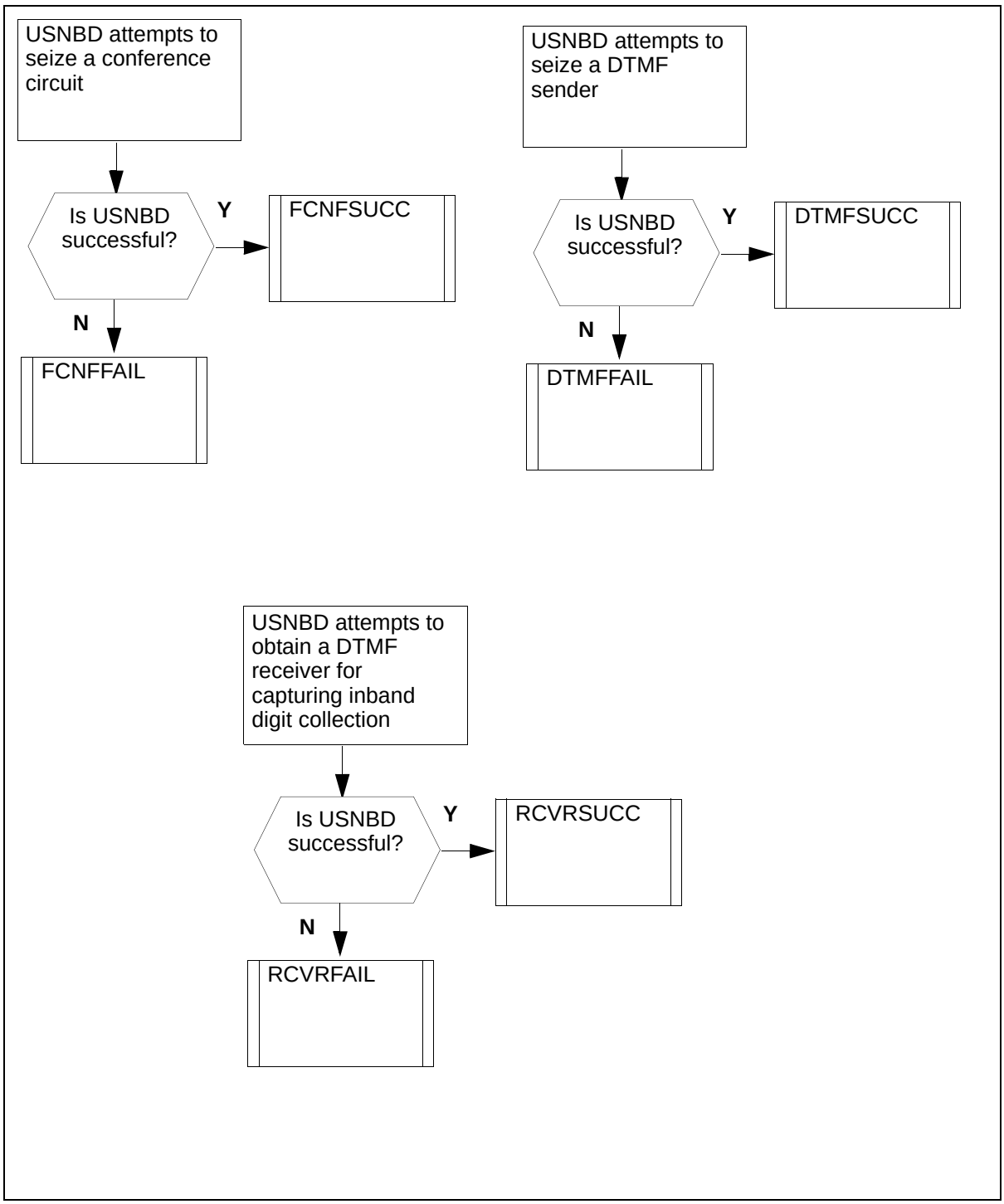
Registers

The FCNF OM group registers display on the MAP terminal as follows:

```
> omshow fcnf active

FCNF

CLASS: ACTIVE
START: 1996/02/08 08:00:00 THU; STOP: 1996/02/08 08:08:41
THU;
SLOW SAMPLES              3; FAST SAMPLES            24;

 FCNFSUCC FCNFFAIL DTMFSUCC DTMFFAIL RCVRSUCC RCVRFAIL

     0       0          0          0         0         0
```

OM group FCNF

OM group FCNF registers



OM group FCNF

Group structure

Key field: none
Info field: none

Associated OM group

None

Associated functional groups

None

Associated functionality codes

None

OM group FCNF

Register FCNFSUCC

Register FCNFSUCC is incremented when USNBD successfully seizes a conference circuit for a combined CCR.

Release history

Register FCNFSUCC was created in NA005.

Associated registers

Registers in group CF3P.

Associated logs

None

Register type

Register FCNFSUCC is a peg-type register.

Extension registers

None

Register FCNFFAIL

Register FCNFFAIL is incremented when USNBD fails to seize a conference circuit for a combined CCR.

Release history

Register FCNFFAIL was created in NA005.

Associated registers

Register CNFOVFL in group CF3P.

Associated logs

When USNBD fails to seize a conference circuit, log UNB300 is generated.

Register type

Register FCNFFAIL is a peg-type register.

Extension registers

None

OM group FCNF

Register DTMFSUCC

Register DTMFSUCC is incremented each time USNBD successfully obtains a DTMF sender.

Release history

Register DTMFSUCC was created in NA011.

Associated registers

When register DTMFSUCC is pegged, OM group SVCT register SVCSZRS is also pegged.

Associated logs

None

Register type

Register DTMFSUCC is a peg-type register.

Extension registers

None

Register DTMFFAIL

Register DTMFFAIL is incremented each time USNBD fails to obtain a DTMF sender.

Release history

Register DTMFFAIL was created in NA011.

Associated registers

When register DTMFFAIL is pegged, OM group SVCT register SVCQOVFL is also pegged.

Associated logs

When USNBD fails to seize a DTMF sender, log UNB300 is generated.

Register type

Register DTMFFAIL is a peg-type register.

Extension registers

None

OM group FCNF

Register RCVRSUCC

Register RCVRSUCC is incremented each time USNBD successfully obtains a DTMF receiver for capturing inband digits.

Release history

Register RCVRSUCC was added in NA014.

Associated registers

None

Associated logs

None

Register type

Register RCVRSUCC is a peg-type register.

Extension registers

None

Register RCVRFAIL

Register RCVRFAIL is incremented each time USNBD fails to obtain a DTMF receiver for capturing inband digits.

Release history

Register RCVRFAIL was added in NA014.

Associated registers

None

Associated logs

None

Register type

Register RCVRFAIL is a peg-type register.

Extension registers

None

OM group UNBCDC

OM group UNBCDC

OM description

The UNBCDC OM group records measurements on USNBD CDCs.

Release history

The UNBCDC OM group was introduced in NA012.

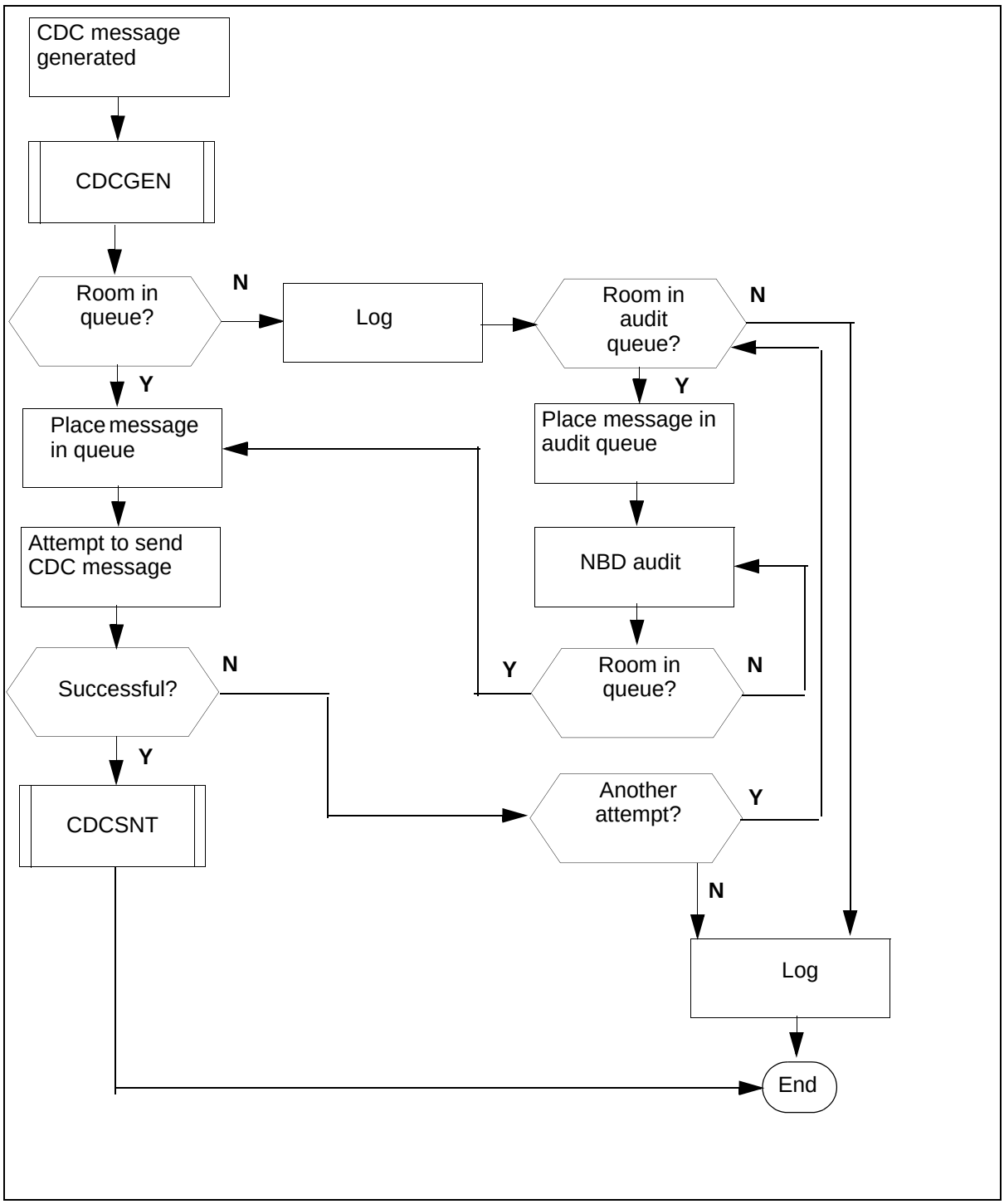
Registers

The UNBCDC OM group registers display on the MAP terminal as follows:

```
> omshow UNBCDC active

UNBCDC

CLASS: ACTIVE
START: 1998/08/08 08:00:00 SAT; STOP: 1998/08/08 08:08:41
FRI;
SLOW SAMPLES              4 ; FAST SAMPLES           35 ;

          KEY (UNB_CDC_SVC_TYPE)
              CDCGEN     CDCSNT

       1
                   3          2
       2
                   0          0
       3
                   0          0
       ...
```

OM group UNBCDC

OM group UNBCDC registers



OM group UNBCDC

Group structure

OM group UNBCDC provides up to 200 tuples, one for each defined CDC.

Key field: CDC Index Number, a number in the range 1 - 200, assigned at the CDC ADD command.
Info field: None

Associated OM group

OM groups MPCLINK2 and MPCLINK3 provide information on the traffic in links 2 and 3 respectively of the multiprotocol controller on which CDC messages are transmitted.

Associated functional groups

The Network Broadcast Delivery (NBD) functional group is associated with OM group UNBCDC.

Associated functionality codes

Functionality codes associated with OM group UNBCDC

Functionality	Code
NBD	NBD00003

OM group UNBCDC

Register CDCGEN

Register CDCGEN counts the number of CDC messages generated by USNBD.

Release history

Register CDCGEN was created in NA012.

Associated registers

CDCSNT, the number of messages successfully sent. CDCSNT is used with CDCGEN to calculate the percentage of generated messages actually sent.using the following formula:

$$\frac{\text{CDCSNT[i]}}{\text{CDCGEN[i]}} \times 100\% = \text{ Percent of requested CDC messages transmitted}$$

where i is the index number of a particular CDC

The number of messages lost within an OM collection is defined by the following formula:

CDCGEN - CDCSNT = Number of CDC messages lost

> ***Note:*** It is possible that during a given period CDCGEN may exceed CDCSNT even though no messages are lost. This condition occurs because the messages may be sent during the next OM collection period. CDCGEN may also be smaller than CDCSNT which may occur when messages generated during an earlier OM collection period were successfully sent during the current OM collection period.

Associated logs

UNB301

Register type

Register CDCGEN is a peg-type register.

Extension registers

None

OM group UNBMISC

Register CDCSNT

Register CDCSNT counts the number of USNBD CDC messages successfully sent over the X.25 link.

Release history

Register CDCSNT was created in NA012.

Associated registers

CDCGEN

Associated logs

UNB301

Register type

Register CDCSNT is a peg-type register.

Extension registers

None

OM group UNBMISC

OM description

The UNBMISC OM group 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.

Release history

The UNBMISC OM group was introduced in NA012.

OM group UNBMISC

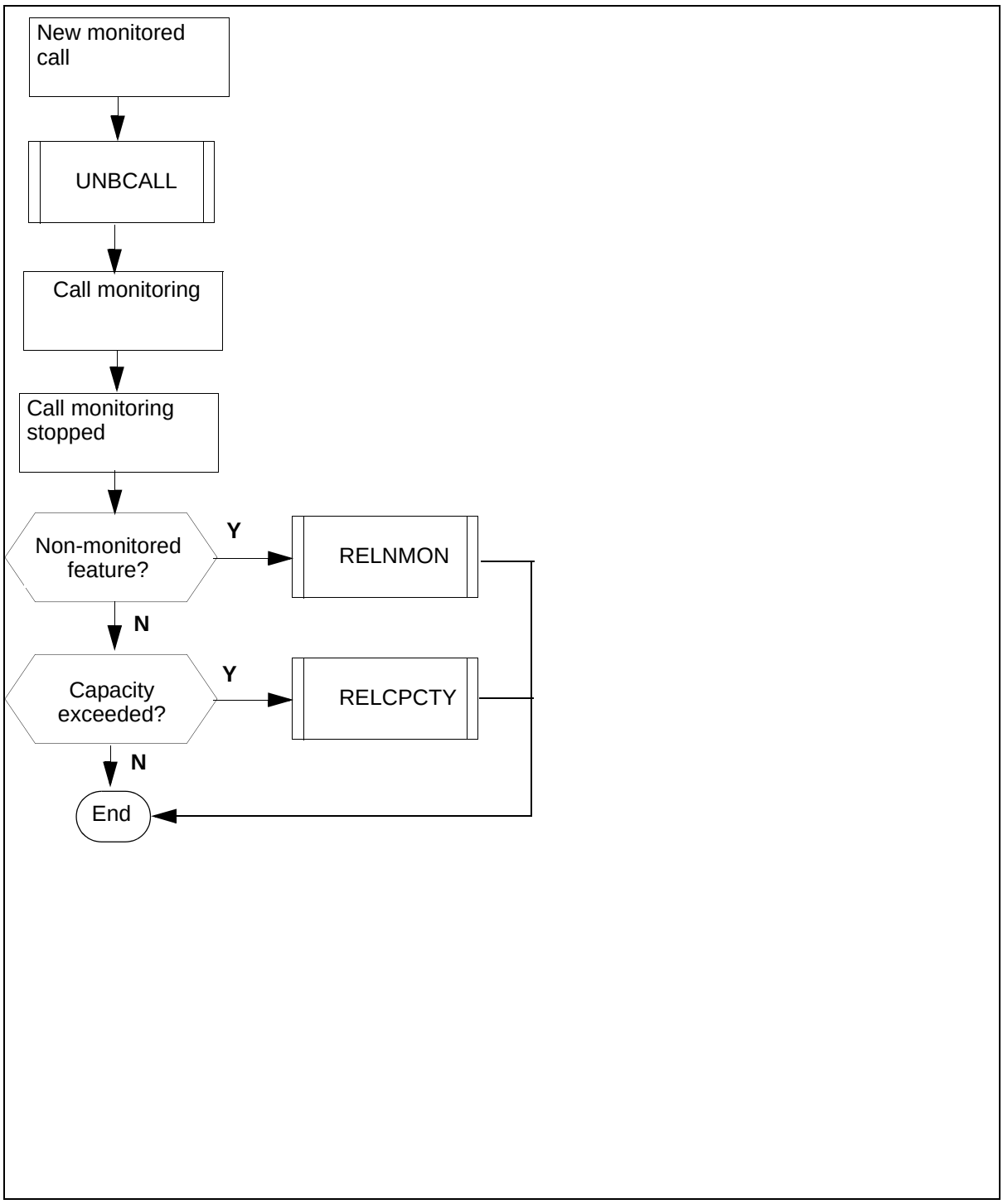
Registers

The UNBMISC OM group registers display on the MAP terminal as follows:

```
> omshow UNBMISC active

UNBMISC

CLASS: ACTIVE
START: 1998/08/08 08:00:00 SAT; STOP: 1998/08/08 08:08:41
FRI;
SLOW SAMPLES             16; FAST SAMPLES          152;

      UNBMCALL   RELNMON    RELCPCTY

   0        50         1           0
```

OM group UNBMISC

OM group UNBMISC registers



OM group UNBMISC

Group structure

OM group UNBMISC provides up to 200 tuples, one for each office.

Key field: None
Info field: None

Associated OM group

None

Associated functional groups

The Network Broadcast Delivery (NBD) functional group is associated with OM group UNBCDC.

Associated functionality codes

Functionality codes associated with OM group UNBCDC

Functionality	Code
NBD	NBD00003

Register RELCPCTY

Register RELCPCTY counts the number of monitored calls for which monitoring was stopped because USNBD defined capacity is exceeded.

Release history

Register RELCPCTY was created in NA012.

Associated registers

UNBMCALL, the number of USNBD monitored calls. UNBMCALL is used with RELCPCTY to calculate the percentage of calls for which monitoring was stopped because USNBD capacity is exceeded, using the following formula:

$$\frac{\text{RELCPCTY}}{\text{UNBMCALL}} \times 100\% = \text{Percent of calls released because capacity is exceeded}$$

Note: It is possible that during a given period RELCPCTY may exceed UNBMCALL. This condition occurs because monitoring could be stopped in the next OM collection period.

OM group UNBMISC

Associated logs
None

Register type
Register UNBMCALL is a peg-type register.

Extension registers
None

Register 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

Release history
Register RELNMON was created in NA012.

Associated registers
UNBMCALL

> ***Note:*** It is possible that during a given period RELNMON may exceed UNBMCALL. This condition occurs because monitoring could be stopped in the next OM collection period.

Associated logs
None

Register type
Register RELNMON is a peg-type register.

Extension registers
None

OM group UNBMISC

Register UNBMCALL

Register UNBMCALL counts the number of calls monitored by USNBD.

UNBMCALL is used to determine the real-time impact monitored calls make on the DMS switch. The impact is determined using the following formula:

$$\frac{\text{UNBMCALL} \times \text{average} \times \text{nmsubj}}{\text{omcp} \times \text{ncmcpu} \times \text{nasurv}} \times 100\% = \text{Percent of absolute increase in CPU occupancy}$$

where

average — is the average time added to monitored calls in milliseconds (the value 7.37 should be used in this formula)

nmsub — is the total number of monitored subjects on the DMS switch

Note: Since there may be up to five surveillances on the same subject, the value of NMSUBJ may be up to five less than the value of NASURV.

omcp — is the OM collection period in milliseconds, usually 15 min (900 000 ms), 30 min (1 800 000 ms), or 60 min (3 600 000 ms)

ncmcpu — is the number of CM CPUs on the DMS switch (always 1 unless an XA-Core processor is used)

nasurv — is the total number of active surveillances on the switch

Release history

Register UNBMCALL was created in NA012.

Associated registers

RELCPCTY and RELNMON

Associated logs

None

Register type

Register UNBMCALL is a peg-type register.

Extension registers

None

OM group XLIUL3

OM group XLIUL3

OM description

XLIU layer 3 OMs (XLIUL3)

OM group XLIUL3 counts the number of packets that the XLIU receives and transmits. OM group XLIUL3 also counts the number of originating, terminating, and not complete virtual call attempts.

The system can use these measurements to monitor packet traffic on the XLIU, and to indicate problems on XLIU links.

Release history

Registers PKTINT and PKTINT2 were added in NA014.

Registers DWCGST, DWCGST2, CALLCGST, CALLCGS2, PKTDROP, and PKTDROP2 were introduced in NA005.

The XLIUL3 OM group was introduced in NA002.

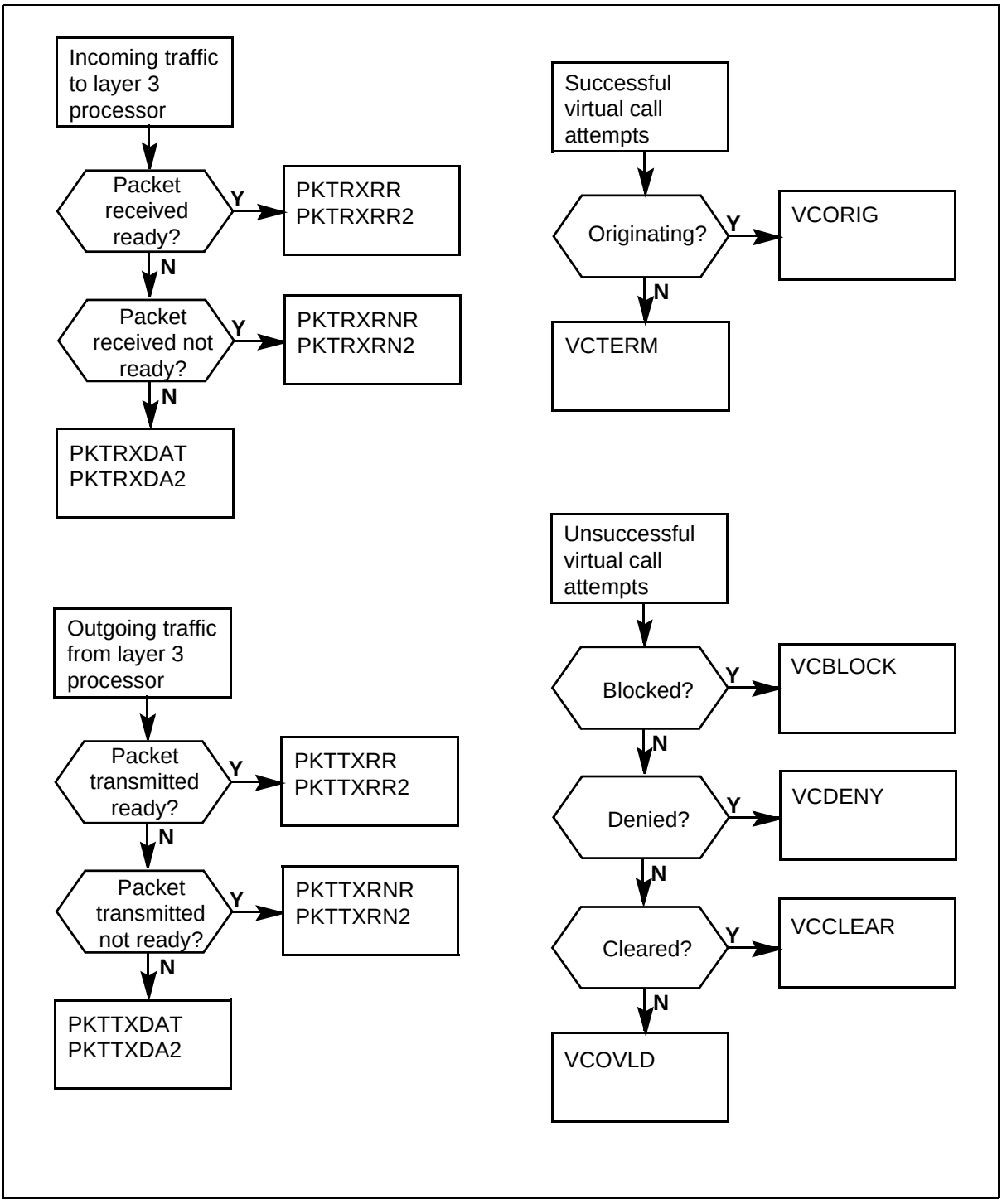
Registers

The XLIUL3 OM group registers display on the MAP terminal as follows:

```
PKTRXRR      PKTRXRR2     PKTRXRNR     PKTRXRN2
PKTRXDAT     PKTRXDA2     PKTTXRR      PKTTXRR2
PKTTXRNR     PKTTXRN2     PKTTXDAT     PKTTXDA2
VCORIG       VCTERM       VCBLOCK      VCDENY
VCCLEAR      VCOVLD       DWCGST       DWCGST2
CALLCGST     CALLCGS2     PKTDROP      PKTDROP2
PKTINT       PKTINT2
```

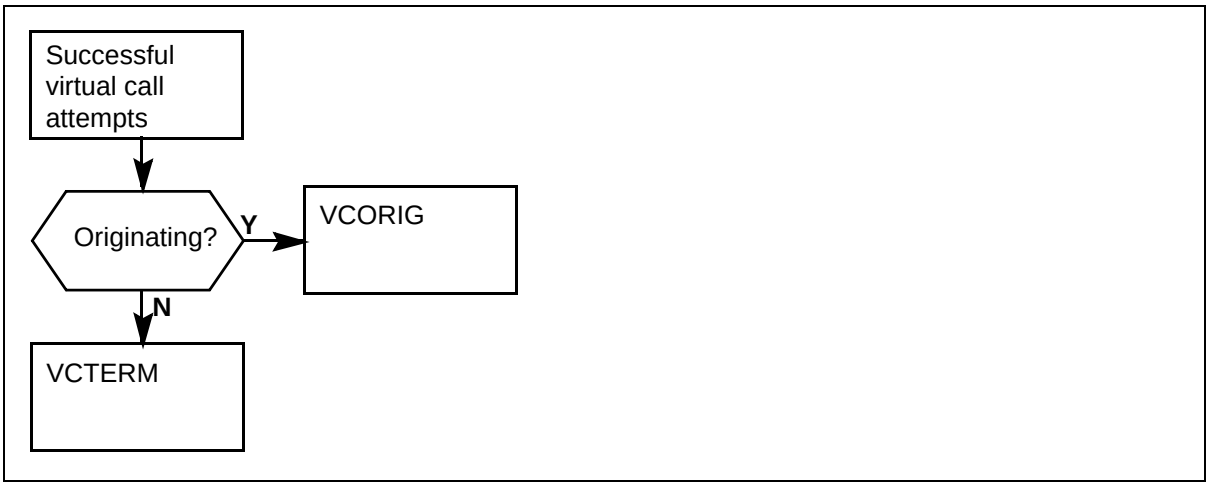
OM group XLIUL3

OM group XLIUL3 registers



OM group XLIUL3

OM group XLIUL3 registers (continued)



Group structure

Table XLIUL3 provides one tuple for each XLIU datafilled in table LIUINV.

Key field: Integer value, range 0 to total number of tuples minus one.
Info field: Node name and number. Node name is XLIU. Number ranges from 0 to 511.

Associated OM group

None

Associated functional groups

The DMS Packet Handler functional group is associated with OM group XLIUL3.

Associated functionality codes

Functionality codes associated with OM group XLIUL3

Functionality	Code
NI0 NI-1 Packet	NI000010

OM group XLIUL3

Register PKTINT

Register intercepted packets dropped: PKTINT

Register PKTINT is the total number of intercepted packets dropped due to congestion or overflow of VC_Q from virtual FSM.

Release history

Register PKTINT was created in NA014.

Associated registers

None

Associated logs

None

Register type

Register PKTINT is a peg-type register.

Extension registers

PKTINT2

Register PKTINT2

Register intercepted packets dropped: PKTINT2

To determine total intercepted packets dropped, multiply register PKTINT2 by 65 536 and add register PKTINT.

Release history

Register PKTINT2 was created in NA014.

Associated registers

None

Associated logs

None

Register type

Register PKTINT2 is a peg-type register.

Extension registers

None

OM group XLIUL3

Register PKTRXRR

Register packets received: RR (PKTRXRR)

Register PKTRXRR is the total number of Received Ready (ACK) packets that the layer 3 processor receives.

Release history

Register PKTRXRR was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTINT2 is a peg-type register.

Extension registers

PKTRXRR2

Register PKTRXRR2

Register packets received: RR (extension) (PKTRXRR2)

To determine total received packets, multiply register PKTRXRR2 by 65 536 and add register PKTRXRR.

Release history

Register PKTRXRR2 was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTRXRR2 is a peg-type register.

Extension registers

None

OM group XLIUL3

Register PKTRXRNR

Register packets received: RNR (PKTRXRNR)

Register PKTRXRNR is the total number of Received Not Ready (NACK) packets that the layer 3 processor receives.

Release history

Register PKTRXRNR was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTRXRNR is a peg-type register.

Extension registers

PKTRXRN2

Register PKTRXRN2

Register packets received: RNR (PKTRXRN2)

To determine total RNR received packets, multiply register PKTRXRN2 by 65 536 and add register PKTRXRNR.

Release history

Register PKTRXRN2 was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTRXRN2 is a peg-type register.

Extension registers

None

OM group XLIUL3

Register PKTTXDAT

Register packets transmitted: data (PKTTXDAT)

Register PKTTXDAT is the total number of data packets that the layer 3 processor transmits.

Release history

Register PKTTXDAT was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTTXDAT is a peg-type register.

Extension registers

PKTTXDA2

Register PKTTXDA2

Register packets transmitted: data (extension) (PKTTXDA2)

To determine total transmitted data packets, multiply register PKTTXDA2 by 65 536 and add register PKTTXDAT.

Release history

Register PKTTXDA2 was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTTXDA2 is a peg-type register.

Extension registers

None

OM group XLIUL3

Register PKTTXRR

Register packets transmitted: RR (PKTTXRR)

Register PKTTXRR is the total number of Received Ready (ACK) packets transmitted that the layer 3 processor transmits.

Release history

Register PKTTXRR was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTTXRR is a peg-type register.

Extension registers

Register PKTTXRR2

Register PCKTTXRR2

Register packets transmitted: RR (extension) (PKTTXRR2)

To determine total transmitted RR packets, multiply register PKTTXRR2 by 65 536 and add register PKTTXRR.

Release history

Register PKTTXRR2 was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTTXRR2 is a peg-type register.

Extension registers

None

OM group XLIUL3

Register PKTTXRNR

Register packets transmitted: RNR (PKTTXRNR)

Register PKTTXRNR is the total number of Received Not Ready (NACK) packets that the layer 3 processor transmits.

Release history

Register PKTTXRNR was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTTXRNR is a peg-type register.

Extension registers

PKTTXRN2

Register PKTTXRN2

Register packets transmitted: RNR (extension) (PKTTXRN2)

To determine total transmitted RNR packets, multiply register PKTTXRN2 by 65 536 and add register PKTTXRNR.

Release history

Register PKTTXRN2 was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTTXRN2 is a peg-type register.

Extension registers

None

OM group XLIUL3

Register PKTTXDAT

Register packets transmitted: data (PKTTXDAT)

Register PKTTXDAT is the total number of data packets that the layer 3 processor transmits.

Release history

Register PKTTXDAT was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTTXDAT is a peg-type register.

Extension registers

PKTTXDA2

Register PKTTXDA2

Register packets transmitted: data (extension) (PKTTXDA2)

To determine total transmitted data packets, multiply register PKTTXDA2 by 65 536 and add register PKTTXDAT.

Release history

Register PKTTXDA2 was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register PKTTXDA2 is a peg-type register.

Extension registers

None

OM group XLIUL3

Register VCORIG

Register virtual call attempts: originating (VCORIG)

Register VCORIG is the total number of call request packets that the layer 3 processor sends to the computing module (CM). This total includes call request packets that are both complete and not complete.

Release history

Register VCORIG was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register VCORIG is a peg-type register.

Extension registers

None

Register VCTERM

Register virtual call attempts: terminating (VCTERM)

Register VCTERM is the total number of call request packets the CM receives from the layer 3 processor. This total includes call request packets that are both complete and not complete.

Release history

Register VCTERM was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register VCTERM is a peg-type register.

Extension registers

None

OM group XLIUL3

Register VCBLOCK

Register unsuccessful virtual call attempts: blocking (VCBLOCK)

Register VCBLOCK is the total number of blocked call request packets for switched virtual circuits (SVC). This total includes:

- outgoing DTE call requests. No call slot and the system cannot assign LCN.
- incoming DTE call requests. The system cannot get User Data Area (UDA), cannot assign LCN, and extension byte does not match.

Release history

Register VCBLOCK was created in NA002.

Associated registers

None

Associated logs

None

Extension registers

None

Register VCDENY

Register unsuccessful virtual call attempts: denied (VCDENY)

Register VCDENY is the total number of denied call request packets for SVCs that the system clears. The system clears in direct response to the SVC call.

Release history

Register VCDENY was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register VCDENY is a peg-type register.

Extension registers

None

OM group XLIUL3

Register VCCLEAR

Register unsuccessful virtual call attempts: clearing (VCCLEAR)

Register VCCLEAR is the total number of call request packets for SVCs that the system clears. These are packets that a link clear message clears. The layer 3 processor generates the link clear message.

Release history

Register VCCLEAR was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register VCCLEAR is a peg-type register.

Extension registers

None

Register VCOVLD

Register unsuccessful virtual call attempts: overload (VCOVLD)

Register VCOVLD is the total number of call request packets that the system discards. The system discards the packets because of system overload for both SVCs and permanent virtual circuits (PVC).

Release history

Register VCOVLD was created in NA002.

Associated registers

None

Associated logs

None

Register type

Register VCOVLD is a peg-type register.

Extension registers

None

OM group XLIUL3

Register DWCGST

Register Mild XLIU Congestion (DWCGST)

Register DWCGST counts the number of times free buffer pools in layers 2 and 3 drop below the weak congestion threshold. This condition causes the dynamic window algorithm to take effect. The dynamic window algorithm reduces the layer 3 processor window size to throttle the traffic rate.

Release history

Register DWCGST was created in NA005.

Associated registers

None

Associated logs

None

Register type

Register DWCGST is a peg-type register.

Extension registers

DWCGS2

Register DWCGS2

Register Mild XLIU Congestion (extension) (DWCGS2)

To determine the total number of times free buffer pools drop below the weak congestion threshold, perform the following calculation. Multiply register DWCGS2 by 65 536 and add register DWCGST. The free buffer pools are in layers 2 and 3.

Release history

Register DWCGS2 was created in NA005.

Associated registers

None

Associated logs

None

Extension registers

None

OM group XLIUL3

Register CALLCGST

Register Call Congestion (CALLCGST)

Register CALLCGST counts the number of times the system delays a call in congestion. The system delays the calls because packets in the XLIU layer 3 wait for reception by the data terminal equipment (DTE).

Register CALLCGST release history

Register CALLCGST was introduced in NA005.

Associated registers

There are no associated registers.

Associated logs

There are no associated logs.

Extension register

CALLCGS2

Register CALLCGS2

Register Call Congestion (extension) (CALLCGS2)

To determine total number of times the system delays a call in congestion because packets must wait for reception, perform the following calculation. Multiply reigster CALLCGS2 by 65 536 and add register CALLCGST.

Register PKTTXDA2 release history

Register CALLCGS2 was introduced in NA005.

Associated registers

There are no associated registers.

Associated logs

There are no associated logs.

Extension registers

There are no extension registers.

OM group XLIUL3

Register PKTDROP

Register Packets Dropped Due to Congestion (PKTDROP)

Register PKTDROP counts the number of packets that the system drops at layer 3 because of XLIU congestion. Congestion in the XLIU can have the following causes:

- excessive incoming traffic
- traffic congestion in the layer 2 processor
- traffic that the system drops because the DTE transmits an RNR

Register PKTDROP release history

Register PKTDROP was introduced in NA005.

Associated registers

There are no associated registers.

Associated logs

There are no associated logs.

Extension registers

PKTDROP2

Register PKTDROP2

Register Call Congestion (extension) (PKTDROP2)

To determine the total number of packets that the system drops at layer 3 because of XLIU congestion, perform the following calculation. Multiply register PKTDROP2 by 65 536 and add register PKTDROP.

Register PKTTXDA2 release history

Register PKTDROP2 was introduced in NA005.

Associated registers

There are no associated registers.

Associated logs

There are no associated logs.

Extension registers

There are no extension registers.

Chapter 5: Log reports

This chapter describes the logs used by the USNBD feature, which are:

- TRIG600
- TRIG700
- UNB300
- UNB301
- UNB302
- UNB303
- UNB304
- UNB305
- UNB306

Access to UNB logs is provided only to USNBD users (with or without administrator privileges) through the LOGUTIL;OPENSECRET UNB command. No password is required.

Log TRIG600 indicates that an UNB300, UNB301, UNB302, UNB303, or UNB304 log has been generated. These logs are service-affecting. Log TRIG700 indicates that an UNB305 or UNB306 information-only log has been generated.

UNB300

UNB300

Explanation

The UNB300 log report is generated when an error exists with a shared resource, which makes it unavailable to USNBD.

Feature data blocks (FDB), feature queue blocks (FTRQ), and conference circuits are shared resources that USNBD uses, and it is essential that these resources be available for the proper operation of USNBD. The DTMF sender is also a shared resource that is essential to the transmission of the CCC Tag on the CCR at the end of the call content delivery. See UNB303 logs for more information.

These logs are generated when there is a problem with DTMF receivers. The generation of these logs indicates a problem with the DTMF receivers and a problem in capturing inband digits.

Format

The format for log report UNB300 follows:

```
UNB 300 mmmdd hh:mm:ss ssdd INFO
<problem>
<result>
[SIN: <sin>]
```

Example

An example of log report UNB300 follows:

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

Field descriptions

The following table explains each of the fields in the log report.

Field	Value	Description
problem	Can be any one of the following: • Conference circuit has been made busy • Conference circuit unavailable • DTMF receiver is unavailable • DTMF receiver is lost • Feature data block unavailable • FTRQ16WPERMS block unavailable	This field indicates the problem USNBD encountered with a shared resource.
result	Can be any one of the following: • Call cannot be monitored • Call content cannot be delivered • Inband digits may have been lost • Inband digits have not been captured • Surveillance cannot be activated • CCC tag was not delivered	This field indicates the consequence of the problem.
sin	alphanumeric	This field indicates the surveillance identification number of the affected surveillance. If surveillance information is not available, this field is not present.

Action

The action to be taken depends on the problem indicated in the <problem> field.

If the <problem> field indicates...	then...
Conference circuit has been made busy	Inform the LEA if required.
Conference circuit unavailable	Inform the LEA if required. Install more conference circuits if this log is often generated.

UNB300

If the <problem> field indicates...	then...
DTMF receiver is unavailable	Inform the LEA if required. Install more DTMF receivers if this log occurs often.
DTMF receiver is lost	Inform the LEA if required, and contact your Nortel Networks representative to determine further action.
Feature data block unavailable	Inform the LEA if required, and contact your Nortel Networks representative to determine further action.
FTRQ16WPERMS block unavailable	Inform the LEA if required, and contact your Nortel Networks representative to determine further action.

Associated OM registers

Register FCNFFAIL in OM group FCNF is pegged when USNBD fails to seize a conference circuit for combined CCRs because none are available. Register DTMFFAIL in OM group FCNF is pegged when USNBD fails to obtain a DTMF sender.

The RCVRFAIL OM register is pegged to indicate the number of times USNBD failed to obtain a DTMF receiver.

Additional information

None

UNB301

UNB301

Explanation

The UNB301 log report is generated when a problem occurs with the CDC link, the CDC message queue, or the CDC audit queue. Any problems with switched remote FSK CDCs are also reported in this log.

Format

The format for log report UNB301 follows:

```
UNB 301 mmmdd hh:mm:ss ssdd INFO
<cdc_problem>
<result>
CDC: <cdc_index>
[NUMBER OF CDC MESSAGES LOST: <nb>]
[CDC_DEFINITION: <mpc> <link> <address> <protocol>]
```

Example

An example of log report UNB301 follows:

```
UNB 301 JUN05 15:33:23 7300 INFO
CDC QUEUE FULL
CDC MESSAGE HAS BEEN PUT IN THE CDC AUDIT QUEUE
CDC: 1
```

UNB301

Field descriptions

The following table explains each of the fields in the log report.

Field	Value	Description
cdc_problem	Can be any one of the following: • CDC audit queue full • CDC has become invalid • CDC queue full • Maximum number of transmission attempts reached • SVC failed • Cannot route to CDC • CDC down • CDC has become invalid • CDC in bad state	This field indicates the problem encountered with the CDC.
result	Can be any one 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	This field indicates the consequence of the problem.
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, and 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, and is only provided when the result field is “CDC has been deleted”.

UNB301

Field	Value	Description
address	1 through 15 decimal digits	This field indicates the MPC address defined for the X.25 CDC that was deleted, and is only provided when the result field is “CDC has been deleted” and the CDC used X.25.
protocol	4 decimal digits of 0 through 255	This field indicates the protocol defined for the X.25 CDC that was deleted, and is only provided when the result field is “CDC has been deleted” and the CDC used X.25.
IP address	4 decimal digits of 0 through 255	This field indicates the IP address defined for the IP CDC that was deleted, and is only provided when the result field is “CDC has been deleted” and the CDC used IP.
port	0 through 32767	This field indicates the port defined for the IP CDC that was deleted, and is only provided when the result field is “CDC has been deleted” and the CDC used IP.
access	DE, SL, or SR	This field indicates the access defined for the FSK CDC that was deleted, and is only provided when the result field is “CDC has been deleted” and the CDC used FSK.
DN	10-digit DN	This field indicates the DN defined for the FSK CDC that was deleted, and is only provided when the result field is “CDC has been deleted” and the CDC used FSK.

UNB301

Action

The action to be taken depends on the problem with the CDC indicated in the <cdc_problem> field.

If the <cdc_problem> field indicates...	then...
CDC audit queue full	Determine whether the NBDAUDIT process is running using the command QUERY PROCESS NBDAUDIT. If the process is not running, recreate it by performing a warm or cold maintenance SWACT. If the process is running, verify all X.25, IP, and FSK links of the USNBD CDCs. If all links are functional, contact your Nortel representative to determine further action. Inform the LEA.
CDC has become invalid Unsupported line class for CDC Unsupported line format for CDC	Verify the MPC link information in tables MPC and MPCLINK. If required, contact the affected LEA. Correct the problem and re-add the CDC. Check for UNB304 logs to determine to which surveillances the CDC was associated (if any), and reactivate those surveillances.
CDC queue full	Determine whether the FBSX25 process is running using the command QUERY PROCESS FBSX25. If the process is not running, recreate it by performing a warm or cold maintenance SWACT. If the process is running, contact your Nortel representative.
Maximum number of transmission attempts reached	Verify the datalink of the specified CDC. Inform the LEA.
SVC failed	Verify the X.25 datalink of the specified CDC. If required, contact the LEA to discuss further action.
CDC down	Verify the FSK CDC line state. If required, contact the LEA. Disassociate the FSK CDC and reassociate it.
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.

UNB301

Associated OM registers

None

Additional information

Before a CDC is deleted, it is first disassociated from all its surveillances if any. Log UNB304 is generated for each affected surveillance.

UNB302

UNB302

Explanation

The UNB302 log report is generated when one of the processes that USNBD requires cannot be started, or ends unexpectedly. (See “DMS switch processes used for USNBD” on page 1-24 for details about the processes.)

Format

The format for log report UNB302 follows:

```
UNB 302 mmmdd hh:mm:ss ssdd INFO
<process_problem> <process_name>
<result>
```

Example

An example of log report UNB302 follows:

```
UNB 302 JUN05 15:33:23 7300 INFO
FAILURE TO START FBSX25
CDC MESSAGES WILL NOT BE SENT
```

Field descriptions

The following table explains each of the fields in the log report.

Field	Value	Description
process_problem	Can be any one of the following: • Abnormal death of • Failure to start	This field indicates the problem that the process encountered.
process_name	Can be any one of the following: • FBSX25 • NBDAUDIT • NBDRCVRY	This field identifies the process that encountered the problem.

UNB302

Field	Value	Description
result	Can be any one of the following: • CDC messages will be queued but not sent • The USNBD audit will not run • Process will be recreated • USNBD recovery will not be performed	This field indicates the consequence of the problem.

Action

The action to be taken depends on which process has the problem.

If the <process_name> field indicates...	then...
FBSX25 or NBDAUDIT	Determine whether the affected process is running using the command QUERY PROCESS <process_name>. 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 representative to determine further action.
NBDRCVRY	Determine whether SWERs or TRAPs related to USNBD were generated. If SWERs or 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 representative to determine further action. If no SWERs or TRAPs were generated, no action is required.

Associated OM registers

None

Additional information

None

UNB303

UNB303

Explanation

The UNB303 log report is generated when a problem is encountered with a CCR.

Format

The format for log report UNB303 follows:

```
UNB 303 mmmdd hh:mm:ss ssdd INFO
<ccr_problem>
<result>
CCR: <ccr_index>[ CCC: <ccc_index>]
[CCR DEFINITION: <type> <ccr_id> <ccc_tag>]
```

Example

An example of log report UNB303 follows:

```
UNB 303 JUN05 15:33:23 7300 INFO
UNSUPPORTED TRUNK SIGNALING FOR CCC
CCR HAS BEEN DELETED
CCR: 10 CCC: 1
CCR_DEFINITION: PAIRED TRUNK TG1 1 TG1 2
```

UNB303

Field descriptions

The following table explains each of the fields in the log report.

Field	Value	Description
ccr_problem	Can be any one of the following: • Cannot route to CCC • CCC down • CCC has become invalid • CCC in bad state • ISUP link released • Lost integrity on CCC • Missing billing number • No answer from CCC • Network connection unavailable • Insufficient resources • Connection setup failed • Problem outpulsing the correlation tag • Unsupported line class for CCC • Unsupported line format for CCC • Unsupported trunk bearer capability for CCC • Unsupported trunk direction, trunk signaling, or trunk type for CCC • Call content inaccessible - bearer channel behind private network	This field indicates the problem that the CCR encountered.

UNB303

Field	Value	Description
result	Can be any one of the following: • Call content cannot be delivered • CCR has been deleted • Correlation tag may not have been entirely delivered • Switched ISUP CCC call cannot be billed	This field indicates the consequence of the problem.
ccr_index	1 through 500	This field indicates the index number of the CCR that encountered the problem.
ccc_index	1 or 2	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.
type	combined or paired	This field indicates whether the CCR is a combined or paired CCR.
ccr_id	LINE <dn1> [<dn2>] <signaling> TRUNK <tg1> <tn1> [<tg2><tn2>]	Specifies the type of CCC (line or trunk) and the CCC through four subfields depending on the type of CCR and whether they are lines or trunks.
signaling	Y or N	Specifies if signaling is enabled on the CCC(s).
tg1	String	Specifies the CLLI of the trunk group containing the first CCC of the CCR.
tn1	Integer 0 to 9999	Specifies the trunk number of the first CCC of the CCR.
tg2	String	Specifies the CLLI of the trunk group containing the second CCC of the CCR.
tn2	Integer 0 to 9999	Specifies the trunk number of the second CCC of the CCR.
dn1 or dn2	10-digit DN	This field indicates the 10-digit DN of CCC1 (combined) or CCC1 and CCC2 (paired).

UNB303

Action

The action to be taken depends on the problem indicated in the ccr_problem field.

If the ccr_problem field indicates...	**then...**
CCC down CCC in bad state No answer from CCC	Verify the CCC line state. If required, contact the LEA. Disassociate the CCR and reassociate it.
CCC has become invalid Unsupported line class for CCC Unsupported line format for CCC Unsupported trunk signaling for CCC Unsupported trunk type for CCC Unsupported trunk direction for CCC Unsupported trunk bearer capability for CCC	Verify which changes have been made to the CCR datafill and why. If required, contact the LEA to determine the problem. Correct the problem and recreate the CCR. Check UNB304 logs to determine to which surveillances the CCR was associated (if any), and reactivate those surveillances.
Insufficient resources	Verify that BCT resources are set correctly. If the problem still occurs, inform your next level of support.
Lost integrity on CCC Connection setup failed	Inform your next level of support.
Problem outpulsing the correlation tag	If required, inform the LEA.

UNB303

If the ccr_problem field indicates...	then...
Network connection unavailable	Verify the JNET or ENET.
Call content inaccessible - bearer channel behind private network	If Private Network Interception is disabled and the USNBD software has determined that both agents on a monitored call are served by a private network, call content for the call is not delivered over the CCR – even if a CCR has been provisioned against this surveillance. If the surveillance also has a CDC associated, the log message indicates that call content for this call is inaccessible. Cut-through digits are collected only if the call traverses to the public network.

Associated OM registers

Register DTMFFAIL in OM group FCNF.

Additional information

Before a CCR is deleted, it is first disassociated from its surveillance. Log UNB304 is generated for the affected surveillance.

UNB304

Explanation

The UNB304 log report is generated to report events and problems that affect surveillances and to report surveillance activation and deactivation. The following events will trigger this log:

- the surveillance has been activated or deactivated
- a subject has been deleted
- the surveillance has become unsupported due to non-monitorable features
- no CCRs are available to a call because none are free, or no CCRs match the bearer capability of the monitored call

Format

The format for log report UNB304 follows. Agency information is displayed only for the USNBD administrative user when the surveillance is deleted. When the surveillance is deleted, subject information is displayed only if the user's agency is the same as the surveillance agency or if the user has USNBD administrative rights.

```
UNB 304 mmmdd hh:mm:ss ssdd INFO
<surv_event>
<result>
SIN: <sin>
[agency <agency>]
[SURV DEFN.: <subject> <caseid> <mrp> <clgdlvry>]
[CDC: <cdc_index> ] [CCR[s]: <ccr_list>]
[COMMAND ENTERED BY: <user>]
```

Example

An example of log report UNB304 for both USER and ADMIN follows. Surveillance has been activated.

```
UNB 304 JUN05 15:33:23 7300 INFO
SURV ACT COMMAND SUCCESSFULLY PROCESSED
SURVEILLANCE HAS BEEN ACTIVATED
SIN: 111
COMMAND ENTERED BY: USER23
```

UNB304

An example of log report UNB304 for ADMIN follows. Subject has been OUTed:

```
INDY1CDN10BO      UNB304 JUN19 06:01:10 2000 INFO
SUBJECT HAS BEEN DELETED
SURVEILLANCE HAS BEEN DELETED
SIN: SIN1
Agency: AGENCY2
SURV. DEFN.: DN 4164771051 A Y Y N
CCR: 1
CDC: 1
```

An example of log report UNB304 for USER follows. The user agency and surveillance agency are the same. Subject has been OUTed:

```
INDY1CDN10BO      UNB304 JUN19 06:01:10 2000 INFO
SUBJECT HAS BEEN DELETED
SURVEILLANCE HAS BEEN DELETED
SIN: SIN1
SURV. DEFN.: DN 4164771051 A Y Y N
CCR: 1
CDC: 1
```

An example of log report UNB304 for USER follows. The user agency is different from the surveillance agency. Subject has been OUTed:

```
INDY1CDN10BO      UNB304 JUN19 06:01:10 2000 INFO
SUBJECT HAS BEEN DELETED
SURVEILLANCE HAS BEEN DELETED
SIN: SIN1
CCR: 1
CDC: 1
```

Field descriptions

The following table explains each of the fields in the log report.

Field	Value	Description
agency	1 to 16 characters	This field identifies the agency of the surveillance.

UNB304

Field	Value	Description
surv_event	Can be any one of the following: • CCR has become invalid • CDC has become invalid • No free usable CCR • Subject has become unsupported • Subject has been deleted • SURV ACT command successfully processed • SURV DEACT command successfully processed	This field identifies the event encountered.
result	Can be any one 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	This field indicates the consequence of the problem.
sin	alphanumeric	This field indicates the surveillance identification number of the affected surveillance.
subject	handle and subject subfields	This field identifies the subject of the affected surveillance.

UNB304

Field	Value	Description
caseid	alphanumeric	This field identifies the case id of the affected surveillance
mrp	Y or N	This field indicates whether a monitored replacement party (MRP) was allowed for the affected surveillance.
clgdlvry	Y or N	This field indicates whether delivery of the calling party number was allowed for the affected surveillance.
cdc_index	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.
ccr_list	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.
user	alphanumeric	This field identifies the user who performed the action. ***Note:*** This field is optional and is only provided when the event is a surveillance activation or deactivation.

UNB304

Action

The action to be taken depends on the problem indicated in the surv_event field.

If the surv_event field indicates...	then...
No free usable CCR	Inform the LEA of the problem. Ensure that sufficient CCRs are provisioned for the type of calls that the subject can originate or receive. The problem may be due to the HELDMON feature being on. HELDMON specifies that a CCR stays with the CONF and another CCR is requested for the second leg. Because no second CCR is available, the log is generated.
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.
Subject has become unsupported	Verify what changes were made to the subject's service. Contact the LEA to discuss further action.
Subject has been deleted	Verify whether the subject's service was moved to another DN, LEN, KEY, or LTID. Contact the LEA to discuss further action.

Associated OM registers

None

Additional information

None

UNB305

UNB305

Explanation

The UNB305 log report is generated to report any problems that affect USNBD administration data and to report user/administrator creations and deletions.

Format

The format for log report UNB305 follows:

```
UNB 305 mmmdd hh:mm:ss ssdd INFO
<user_event>
<result>
USERNAME: <user_id>
[COMMAND ENTERED BY: <user>]
```

Example

An example of log report UNB305 follows:

```
UNB 305 JUN05 15:33:23 7300 INFO
USER ADD COMMAND SUCCESSFULLY PROCESSED
USNBD USER HAS BEEN ADDED
USERNAME: USER1
COMMAND ENTERED BY: USER23
```

Field descriptions

The following table explains each of the fields in the log report.

Field	Value	Description
user_event	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	This field identifies the event encountered.

UNB305

Field	Value	Description
result	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 ***Note***: When this result appears in the log message, a major alarm is raised in the office.	This field identifies the consequence of the event encountered.
user_id	alphanumeric	This field identifies the CI user name that was added or deleted.
user	alphanumeric	This field identifies the user who performed the action. ***Note:*** This field is optional and is only provided when the event is the successful processing of a command.

Action

The action to be taken depends on the information indicated in the result field.

If the result field indicates...	then...
USNBD administrator has been deleted; no administrator left	Contact your Nortel Networks representative for further action.

Associated OM registers

None

Additional information

None

UNB306

UNB306

Explanation

The UNB306 log report is generated to report when an STS, PRETRANSLATOR, LCANAME, PIC, or LATA assigned to an USNBD agency is deleted from tables HNPACONT, STDPRTCT, LCASCRCN, OCCNAME, or LATANAME respectively. The log indicates that datafill existed when the agency was entered in USNBD; however, in the interim, datafill was removed from the table.

The datafill must exist in the appropriate tables when monitoring sessions are activated in order for USNBD to monitor the target's calls. For example, without the STS and pretranslator datafill, USNBD cannot set up the agency recording links to record the target's calls. Without the LCANAME datafill, USNBD cannot determine if a switched connection to a remote agency's recording device is billable.

The log report identifies the agency whose datafill is deleted. Only USNBD users belonging to this agency can view this log report.

Format

The format for log report UNB305 follows:

```
UNB 306 mmmdd hh:mm:ss ssdd INFO
UNB AGENCY <datafill-type> DELETED FROM TABLE <table-
name>
AGENCY = <agency-name>
```

Example

An example of log report UNB305 follows:

```
UNB 306 Jun1 10:00:00 6700 INFO
UNB AGENCY STS DELETED FROM TABLE HNPACONT
AGENCY = AGENCY 1
```

UNB306

Field descriptions

The following table explains each of the fields in the log report.

Field	Value	Description
date	month-date	This field represents the date of generation of log.
time	time	This field represents the time of generation of log.
datafill-type	The possible values are: • STS • PRETRANSLATOR • LCANAME • PIC • LATA	This field identifies the type of datafill which has been removed from the data table.
table-name	The possible values are: • HNPACONT • STDPRTCT • LCASCRCN • OCCNAME • LATANAME	This field identifies the table from which datafill has been deleted.
agency-name	1 to 16 alphanumeric characters	This field identifies the USNBD agency whose recording links cannot be established.

Action

The USNBD user for the affected agency should 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 through 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.

UNB306

Associated OM registers

None

Additional information

None

Chapter 6: Data schema

This chapter contains details of data schema tables used with USNBD.

A virtual link subfield, VIRT, is added to table PVCINFO.

The output display for table LIDINFO is modified to show virtual links.

Typical trunk datafill for CCRs is contained in “Appendix A: Surveillance checklists”.

Tables MPC and MPCLINK are described in “Appendix B: Sample USNBD X.25 connections”.

Table PVCINFO

Table name

Permanent Virtual Circuit Information Table

Functional description

Table PVCINFO functions as a look-up table to determine permanent virtual circuit (PVC) service parameters for use with the DMS packet handler (DMS-PH). A PVC is a permanent logical connection between two network endpoints. One endpoint is designated as the master end and the other endpoint is designated as the slave end.

Fields KEY and SLVEND contain a directory number (DN) from table DNCHNL or a common language location identifier (CLLI) from table X75INFO. The endpoints can use a DN/LCN combination, or a CLLI/LCN combination.

Datafill

The following table lists USNBD datafill for table PVCINFO. Only the fields that have been added or modified by USNBD are shown.

Field description

Field	Subfield	Entry	Explanation and action
KEY	VIRT	see subfields	*Virtual link* Enter VIRT and datafill subfields LINK_ID and LCN.
	LINK_ID	0 to 32,767	*Link id assigned* Enter the link id number for the link assigned to the LEA.
	LCN	1 to 4095	*Logical channel number* Enter the number for the logical channel assigned to the LEA. ***Note:*** The system automatically assigns the LCN when the CCR ASSOC command is entered.

Table PVCINFO

Datafill example

The following example shows sample datafill for table PVCINFO.

MAP display example for table PVCINFO

```
KEY SLVEND PVCOPTNS
_____________________________________________________________________
VIRT 2 1 X25 613550104 V 2 (SENDTC 9600) (RECVTC 9600)
(SENDWAS 2) (RECVWS 2) (SENDPS 128) (RECVPS 128) (LATA INTRA)
(BILLING Y NORMAL)$
```

Note: The MAP display example shown here may not reflect the exact MAP display shown on your MAP terminal, since other fields may have been removed or added by other features following the introduction of USNBD. Therefore, it is recommended that you consult the DMS-100 documentation suite associated with the software release that is running on your switch for the most up-to-date information.

Table LIDINFO

Table LIDINFO

Table name

Link Identification Information

Functional description

Table LIDINFO is used to transfer link objects to the inactive side during an ONP. Table LIDINFO creates an empty link object (a link object whose fields are initialized with NIL values) at the inactive side, when tuples in table LIDINFO are transferred with the same CM and XLIU link ids. Values are entered into the link object when tables KSETINV, KSETLINE, DNCTINFO, and DNCHNL are transferred to the inactive side.

Note: The only change to this table for USNBD is the display of virtual links shown in the datafill example.

Table LIDINFO

Datafill

Datafill example

The following example shows sample datafill for table LIDINFO.

MAP display example for table LIDINFO

```
LIDKEY  XLIULID  LINKAREA
_____________________________________________________
0       004      LT_X25D   8  1
1       005      LT_X25D   8  2
2       006      LT_X25D   8  3
3       007      LT_X25D   8  4
4       000      LT_X25B   8  5
5       000      LT_X25B   8  6
6       000      LT_X25B   8  7
7       000      LT_X25B   8  8
8       000      LT_X25B   8  101
9       001      LT_X25B   8  102
10      002      LT_X25B   8  103
11      003      LT_X25B   8  104
12      005      LT_X25B   8  105
13      008      LT_X25B   8  106
14      00C      LT_X25B   8  107
15      000      LT_X25B   8  108
16      000      LT_X25B   8  109
17      000      LT_X25B   8  110
18      000      LT_X25D   8  9
19      000      LT_X25D   8  10
20      009      LT_X25D   3  201
21      00A      LT_X25D   3  202
22      00B      LT_X25D   3  203
23      000      LT_X25B   8  25
24      001      LT_X25D   3  112
25      000      LT_X25D   3  100
26      002      LT_X25B   8  60
27      001      LT_X25B   8  26
28      004      LT_X25B   8  61
29      00D      LT_X25B   8  62
30      00E      LT_X25B   8  63
31      000      LT_X25B   8  64
32      000      LT_X25B   8  65
33      001      LT_X25_VIRTUAL
```

Note: The MAP display example shown here may not reflect the exact MAP display shown on your MAP terminal, since other fields may have been removed or added by other features following the introduction of USNBD. Therefore, it is recommended that you consult the DMS-100 documentation suite associated with the software release that is running on your switch for the most up-to-date information.

Table LIDINFO

Chapter 7: Provisioning USNBD

Calculating hardware requirements

To determine the hardware requirements for USNBD, complete the table in the section below, then proceed to “Hardware and circuit calculations” on page 7-2.

Input data

Enter the values for your switch in the following table. (Consider the capacity limits provided in the section “Capacity” on page 1-12.)

The letters (A, B, C...) in the following table are used in the calculation formulas starting on the next page.

Provisioning data reference table for USNBD

Surveillances	Value
Total number of surveillances expected on the switch (maximum 400)	(A)
Percentage of surveillances that require call content delivery	(B)
Average number of CCCs per surveillance (maximum 5)	(C)
Call content channel delivery Percentage of loop-start lines	(D)
Percentage of ground-start lines	(E)
Percentage of non-signaling trunks	(F)
Percentage of separated CCRs	(G)
Percentage of combined CCRs	(H)
Inband digit collection Percentage of surveillances that require inband digit collection	(I)
Acceptable DTMF receiver blocking percentage	(J)

Provisioning data reference table for USNBD (Continued)

Average DTMF receiver holding time in minutes	(K)
Total number of lines on DMS switch	(L)
Total number of busy hour call attempts on DMS switch	(M)
Inband signaling to LEA Percentage of CCRs requiring inband signaling to LEAs	(N)

Hardware and circuit calculations

Complete the calculations that follow this table to determine the hardware and circuit requirements for USNBD, and enter the value beside the corresponding card in this table.

PEC	Function	Quantity
NT1X81AA or NT3X67AA	3-port conference circuit for combined CCRs	
NT6X17AC or NT6X17BA	type-A line card for CCC circuits	
NT6X50AB	DS1 card for non-signaling trunks	
NT6X18AA or NT6X18BA	type-B line card for CCC circuits	
NT1X89BA, NT1X89BB or IOM equivalent	multiprotocol controller (MPC) card, or enhanced MPC (EMPC) card for X.25 datalinks	
NT3X68AB	DTMF senders for inband digits to be reported to LEAs in a CDC message	
NT2X48AB	DTMF receivers for inband digit collection	

Calculating the number of conference circuits

To determine the number of conference circuits required for USNBD, use the following formula:

$(A \times B \times C \times H) \div 2 =$ number of NT3X67AA cards

or

$(A \times B \times C \times H) \div 10 =$ number of NT1X81AA cards

Calculating the number of X.25 links

Call Data Channels (CDC) communicate with LEAs using X.25 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 MPC card can support either two 19.2 Kbps low-speed X.25 facilities, or one 56/64 Kbps high speed facility.

A minimum of two X.25 facilities is required for each switch. The maximum number of facilities is 25.

Nortel 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.

Calculating the number of DTMF senders

To determine the number of DTMF senders required for USNBD, use the following formula (assume a maximum sender holding time of 750 milliseconds):

$[((N \times A \times B \times C) \div L) \times M \times 0.75] \div 100 =$ *DTMF Sender traffic*

Determine the number of DTMF senders required using the *DTMF Sender traffic* value with a DTMF Sender blocking value of 0.001 in a Service Circuit Capacity Poisson table.

Divide the number of senders by 4 to obtain the quantity of NT3X68AB cards required.

Calculating the number of DTMF receivers

To determine the number of DTMF receivers required for USNBD, use one of the following formulae:

- When blocking (value of J) = 0, use

  $(A \times I) \div 4 =$ number of NT2X48AB cards

- When blocking (value of J) is other than 0, use

  $[((A \times I) \div L) \times K \times M \times 60] \div 100 =$ *DTMF Receiver traffic*

Determine the number of DTMF receivers required using the DTMF Receiver traffic value with the DTMF Receiver blocking value (J) in a Service Circuit Capacity Poisson table.

Divide the number of receivers by 4 to obtain the quantity of NT2X48AB cards required.

Calculating the number of CCC circuits

To determine the number of type-A line cards required for USNBD, use the following formula:

$[(H \times D) + 2(G \times D)] \times A \times B \times C$ = number of NT6X17AC cards

To determine the number of type-B line cards required for USNBD, use the following formula:

$[(H \times D) + 2(G \times E)] \times A \times B \times C$ = number of NT6X18AA cards

To determine the number of DS-1 trunk cards required for USNBD, use the following formula:

$[[(H \times D) + 2(G \times F)] \times A \times B \times C] \div 24$ = number of NT6X50AB cards

Provisioning surveillances

To provision and set up surveillances, follow the advice in “Appendix A: Surveillance checklists”.

Chapter 8: USNBD administrator and user procedures

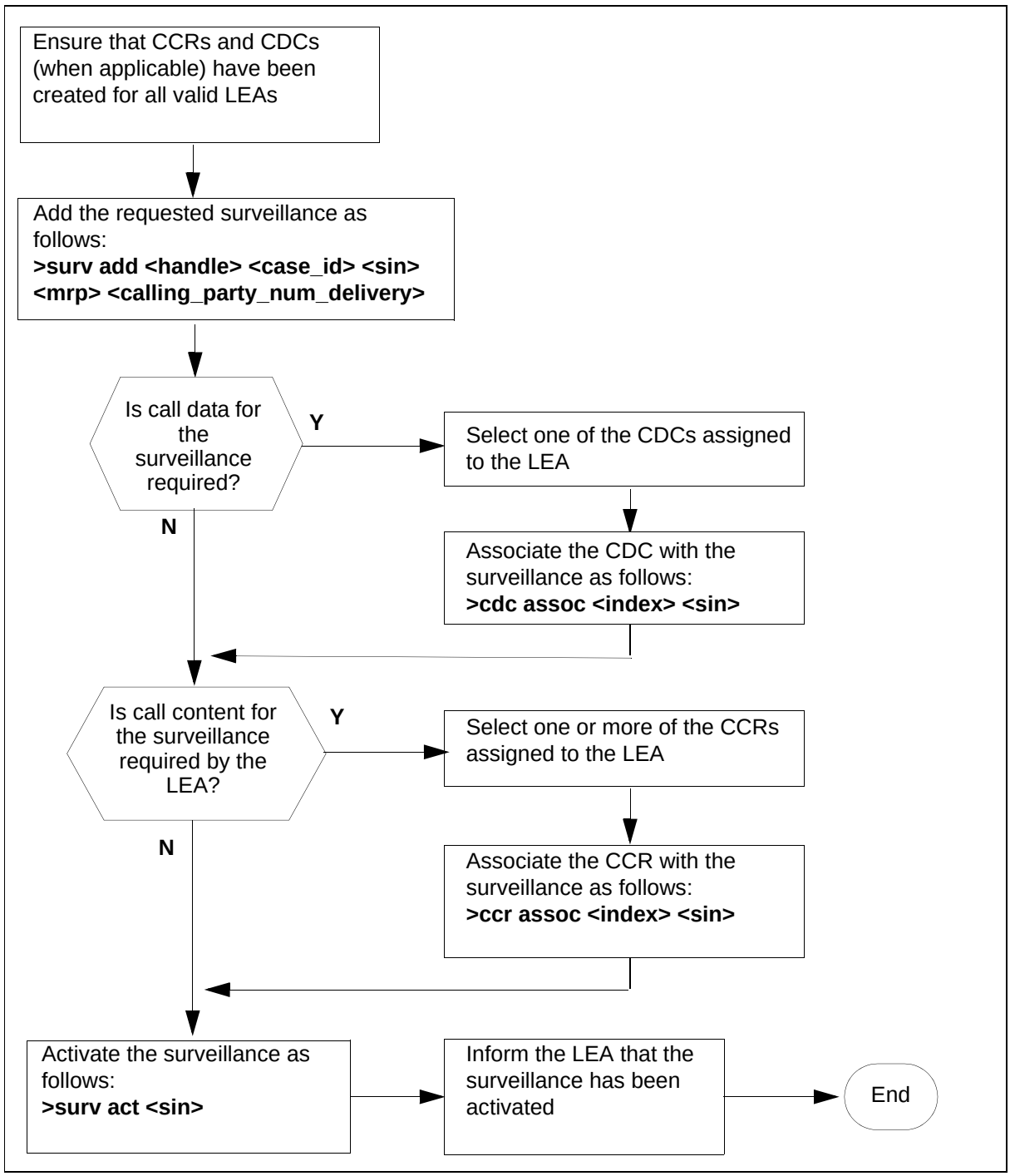
This chapter contains the procedures that USNBD administrators and USNBD users can perform. The procedures are:

- "Activating SOC option NBD00003" on page 8-3
- "Adding USNBD users" on page 8-7
- "Adding an agency" on page 8-11
- "Creating CCRs" on page 8-15
- "Creating a CDC" on page 8-21
- "Adding a surveillance" on page 8-26
- "Associating a CDC with a surveillance" on page 8-31
- "Associating a CCR with a surveillance" on page 8-36
- "Activating a surveillance" on page 8-41
- "Determining status of Held Conference" on page 8-45
- "Ensuring inband digits delivery" on page 8-49
- "Deactivating a surveillance" on page 8-54
- "Taking down a surveillance" on page 8-58
- "Deleting a CCR" on page 8-63
- "Deleting a CDC" on page 8-67
- "Deleting USNBD agencies" on page 8-71
- "Deleting USNBD users" on page 8-75
- "Deactivating SOC option NBD00003" on page 8-78

Summary of surveillance setup commands

The following figure contains a flowchart of the commands required to set up and activate a surveillance.

Summary of commands required to set up and activate a surveillance



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 after the software load that includes the USNBD feature is added to the switch, and it is required to activate USNBD.

Prerequisites

The user performing this procedure must have access to the USER command of USNBD and to the appropriate SOC commands. Therefore, prior to performing this procedure,

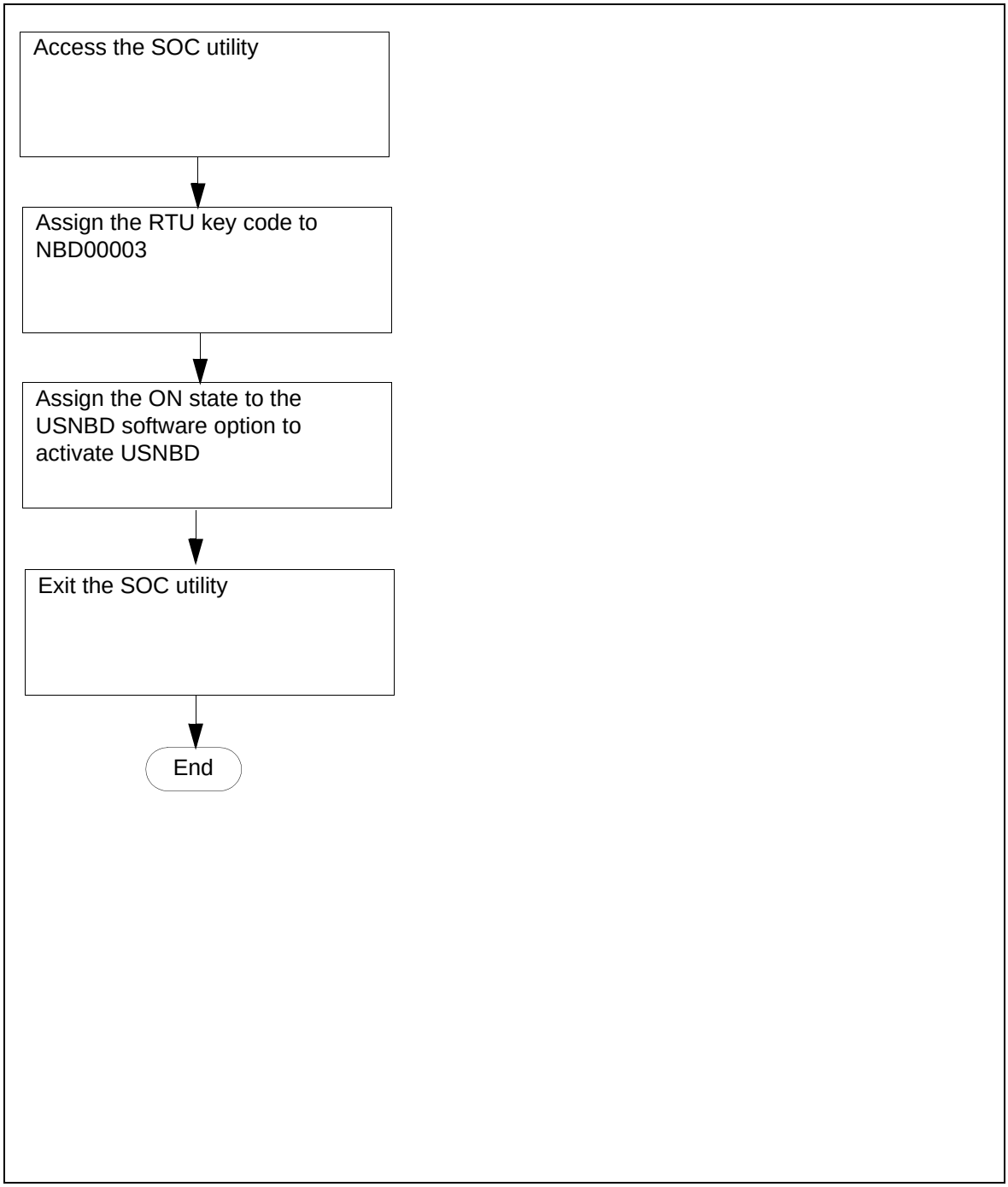
- it is recommended that you create a privilege class specific to USNBD using the PRIVCLAS command, and to assign the USNBD privilege class to authorized users using the PERMIT command
- obtain the right-to use (RTU) key code (password) from your Nortel Networks representative to activate SOC option NBD00003

Action

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

Activating SOC option NBD00003

Summary of Activating SOC option NBD00003



Activating SOC option NBD00003

Step	Action

At the CI level of the MAP

1 Access the SOC utility by typing:

```
> soc
```

MAP response:

```
SOC:
```

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

```
> select option nbd00003
```

MAP response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00003 NANBD     N  IDLE   -     -       -     98/05/10
```

3 Assign the right-to-use (RTU) key code to the USNBD software option by typing:

Note: The RTU key code (password for NBD00003) is obtained from your Nortel Networks representative.

```
> assign rtu <key_code> to nbd00003
```

where

key_code	is the password obtained from your Nortel Networks representative

MAP response:

```
Done.
```

Note: For security reasons, it is strongly recommended to assign the ON state to the USNBD software option immediately after having assigned the right-to-use (RTU) key code to SOC option NBD00003.

Activating SOC option NBD00003

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

```
> select option nbd00003
```

MAP response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00003 NANBD     Y  IDLE   -    -      -     98/05/10
```

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

```
> assign state on to nbd00003
```

MAP response:

```
Done.

You have been defined as the initial USNBD
administrator.
```

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

```
> select option nbd00003
```

MAP response:

```
GROUP: RES
OPTION NAME       RTU STATE USAGE LIMIT UNITS LAST_CHG
-------------------------------------------------------
NBD00003 NANBD     Y  ON   -    -      -     98/05/10
```

7 Exit the SOC utility by typing:

```
> quit
```

8 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 who has 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. It is recommended to have at least two USNBD users with administrator privileges at all times.

Prerequisites

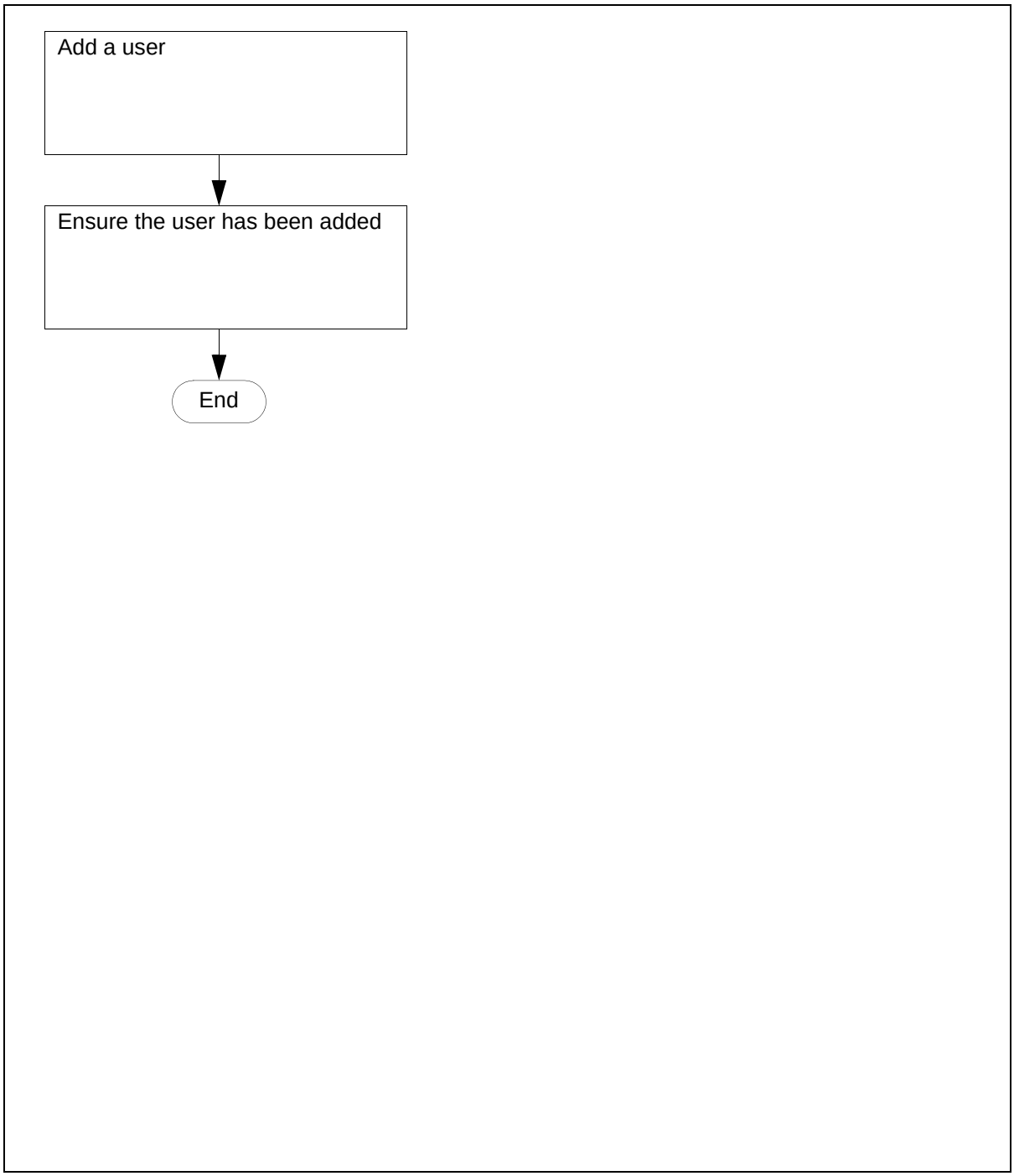
The administrator or user to be added must have a valid CI user id.

Action

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

Adding USNBD users

Summary of Adding USNBD users



Adding USNBD users

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

2 Add a user by typing:

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

where

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

Example input:

```
> user add user1 n agency1
```

MAP response:

```
USER ADD DONE:
```

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

Adding USNBD users

4 Ensure the users have been added by typing:

```
> user list
```

Example of a MAP response:

```
user list USER   ADMIN AGENCY
         ------------------------------
         USER1   N     nanbdadm1
         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 who has 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 CCRs.

Prerequisites

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

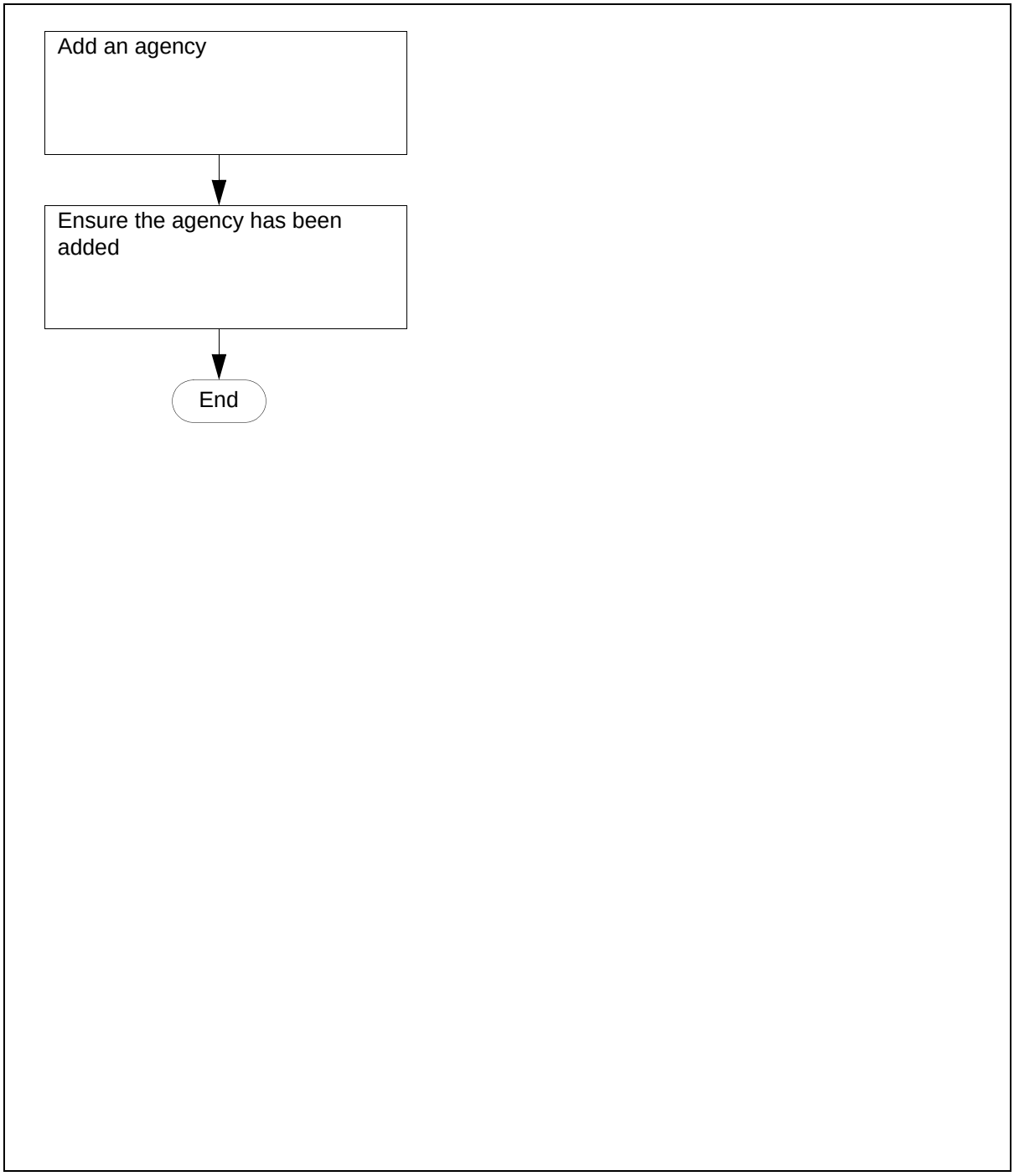
- the agency name to be used in USNBD (1 to 16 characters)
- the Serving Translation Scheme (STS)
- the pretranslator name
- the Local Calling Area Screening name (LCA)
- for switched access or FSK switched remote access using Equal Access trunks, the 10-digit billing number used for generating billing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

Adding an agency

Summary of Adding USNBD agencies



Adding an agency

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP 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>
```

where

agency_name	is the agency having access to switched ISUP CCCs to their remote recording device
STS	is the Serving Translation Scheme
pretranslator	is the PRETRANSLATOR Name
lca	is the Local Calling Area Screening Name
billno	is the 10-digit billing number used to generate billing records for the SWITCHED ISUP CCC or FSK SR CDC call pertaining to the specified agency
pic	is the PIC to use for switched CCRs or FSK SR CDCs using equal access dialing to the LEA. If equal access is not required, enter NILC.
lata	is the LATA to use for switched CCRs or FSK SR CDCs using equal access dialing to the LEA. If equal access is not required, enter NILLATA.

Adding an agency

Example input:

```
> agency add agency1 613 p621 l667 1234567890 epic
newlata
```

MAP 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
```

Example of a MAP response:

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

Note: You can add up to eight USNBD agencies with switched ISUP CCC access.

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.

Prerequisites

The USNBD user who is performing this procedure requires the following information:

- the LEA's preferred delivery method; combined or paired
- the directory number of each line to be used as a CCC circuit or the CLLI and external trunk number of each trunk to be used as a CCC circuit

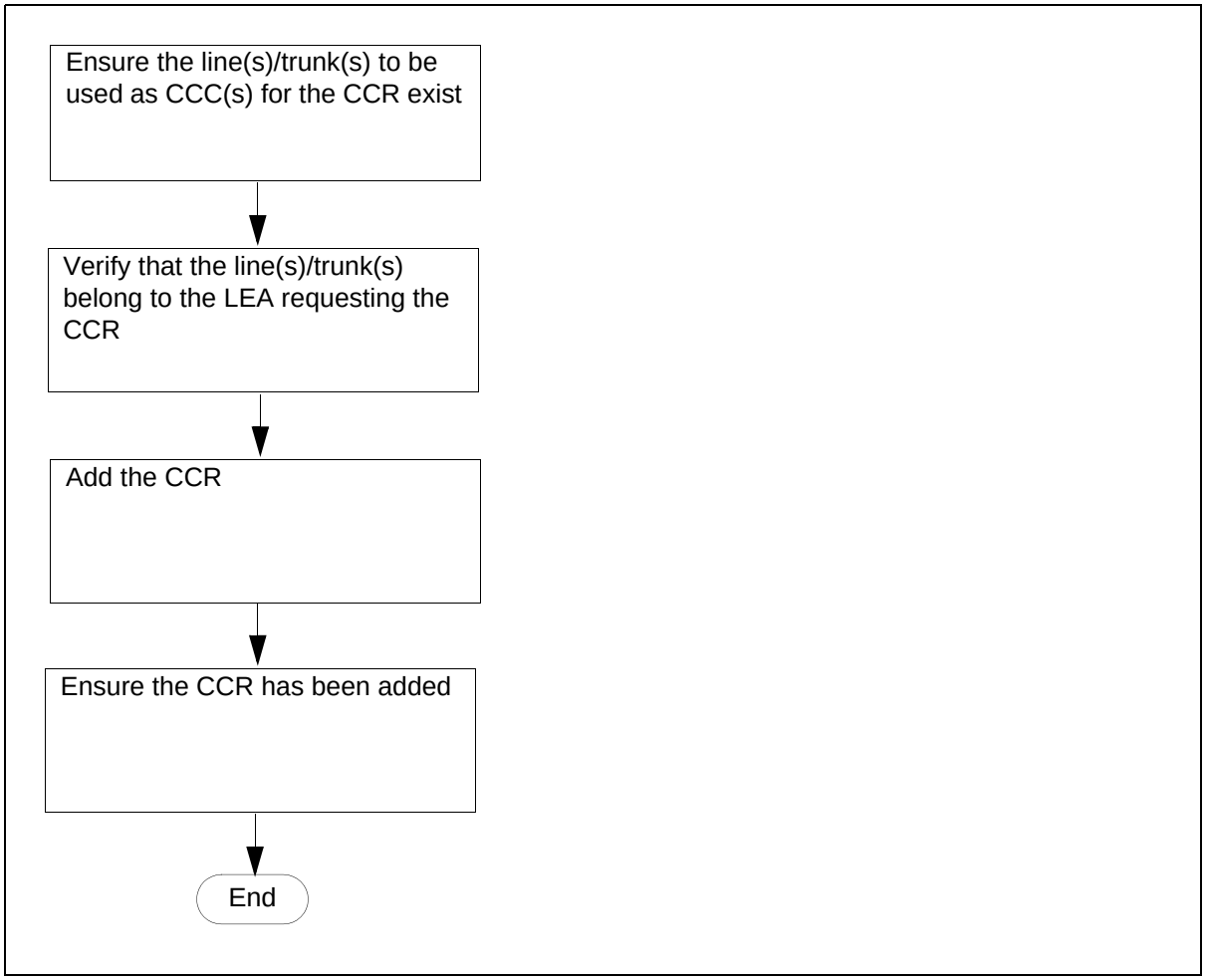
The USNBD user performing this procedure also must be associated with the same agency as the CCR or have USNBD administrative rights.

Action

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

Creating CCRs

Summary of Creating CCRs



Creating CCRs

Step	Action

1 Ensure the line(s) or trunk(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
- must be of type “single party line”
- must have a line class code (LCC) of 1FR, 1MR, or RES
- can only be assigned the following options:
  - COD
  - DGT
  - NAME
- cannot be assigned any RES options
- can make use of any office options

To use a line as a switched CCC circuit, the line

- for the DN must be remote from the host switch
- from the host switch must be across an ISUP trunk

2 Verify that the line(s) or trunk(s) belong to the LEA requesting the creation of the CCR(s).

At the USNBD level of the MAP

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

```
> ccr list free
```

Example of a MAP response:

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

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

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

Creating CCRs

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

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

where

index	is the CCR index number obtained in step 3 (1 through 500) that identifies the CCR
signaling	is Y to indicate signaling is enabled on the CCC(s) or N to indicate signaling is not enabled on the CCC(s)
ccr_content	is VOICE <ccr_definition> or PACKET <ccr_id>
ccr_definition for VOICE	is COMBINED <ccr_id> or is PAIRED <ccr_id>
ccr_definition for PACKET	is LINE, the PVC1 and PVC2 10-digit DNs to specify LCN or is TRUNK, the CLLI and the associated trunk number that are the endpoints to PVC1 and PVC2
ccr_id (COMBINED)	is LINE, the 10-digit DN of the CCC circuit and the signaling indicator or is TRUNK, the CLLI and the associated trunk number
ccr_id (PAIRED)	is LINE, the two 10-digit DNs of the CCC circuits, and the signaling indicator or is TRUNK and the two CLLIs and trunk numbers for the CCC circuits
access	is the access type of the CCR. For switched access, type SW. For dedicated access, type DE.
ccc_tag	is Y to have the CCC tag delivered for the CCR or N when delivery of the CCC tag for the CCR is not required

Creating CCRs

where

agency	is the agency of the CCR. This parameter is prompted 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 CCR agency and the user is not prompted for this parameter.

Example input:

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

Note: The example input above is for an administrative user. The example below is for a non-administrative user.

Example input:

```
> ccr add 11 combined trunk de myclli 5 Y
```

MAP response:

```
CCR ADD DONE.
```

5 Ensure the CCR(s) have been added by typing:

```
> ccr list all
```

Example of a MAP response:

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

CCR LIST DONE
```

Note: An administrative user will be given CCR information for all agencies (see MAP response above). A non-administrative user will see information only for those CCRs associated with the user's agency (see MAP response below).

Creating CCRs

Example of a MAP response:

```
Index Content CCRtype Acc CCRid CCC1/PVC1    [CCC2/PVC2]
 [Sig] [Tag]    [Sin]
-----------------------------------------------------
1 PACKET PAIRED LINE DE  9059631003        19059631003

33 VOICE COMBINED LINE DE 6135510102
  N    Y
```

Once a CCR has been added, it can be associated with a surveillance. See procedure “Associating a CCR with a surveillance” on page 8-36.

6 If a switched CCR is used, perform a test using the USNBD test command.

7 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 LEAs.

Prerequisites

The USNBD user who is performing this procedure requires the following information:

- the index number of the MPC or EMPC card from table MPC
- the MPC link number from table MPCLINK
- if you are using X.25 links for CDCs, the address and protocol of the X.25 node
- if you are using FSK links for CDCs, the access type (switched local, switched remote, or dedicated) and the 10- or 11-digit DN (see next paragraph)

A line used as an FSK SL or DE CDC circuit must have a non-ambiguous, 10-digit DN associated with it. A line used as an FSK SR CDC circuit may have a 10- or 11-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 only be assigned the following options:
  - COD
  - DGT
  - NAME
- cannot be assigned any RES options
- can make use of any office options
- the 10- or 11-digit string must terminate to an SS7 trunk of the following type: ATC with EA dialing, IT with or without EA dialing, TO, or T2

Creating a CDC

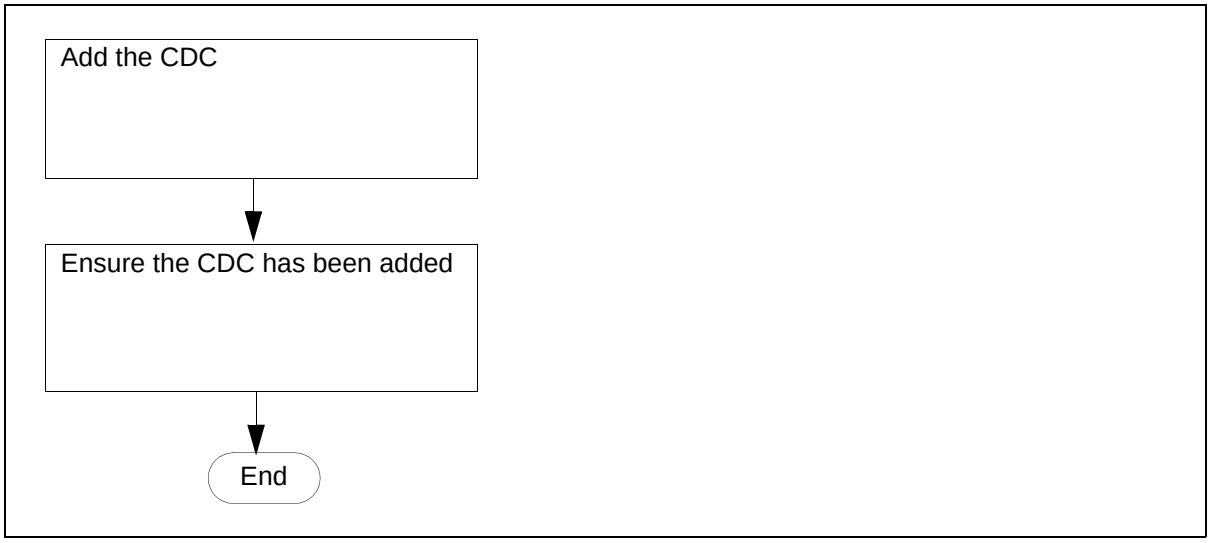
- the 10- or 11-digit string must not reside on the same switch as the surveillance
- the CDC circuit must be routed through an in-service CMR card hosted in an LGC or LTC XPM running load QLI17AY1 or higher

The USNBD user performing this procedure also must be associated with the same agency as the CDC will be 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 Creating a CDC



Step	Action

1 Ensure the link to be used as a CDC exists, and the translations datafill is set up correctly to terminate to a trunk.

At the USNBD level of the MAP

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

```
> cdc list free
```

Creating a CDC

Example of a MAP response:

```
4-200
CDC LIST DONE.
```

3 Administrative users add the requested CDC by typing:

```
> cdc add <index> <transport_protocol> <MPCIndex>
<MPCLinkNumber> <address> <protocol1> <protocol2>
<protocol3> <protocol4> <agency>
```

Non-administrative users add the requested CDC by typing:

```
> cdc add <index> <transport_protocol> <MPCIndex>
<MPCLinkNumber> <address> <protocol1> <protocol2>
<protocol3> <protocol4>
```

where

index	is the CDC index number (1 through 200) obtained in step 2 that identifies the CDC
transport_protocol	is the protocol. The transport_protocols used are X25, IP, and FSK. The IP transport protocol indicates that the CDC is using SCTP/IP association for its connection. Refer to the Lawful Intercept Product and Technology Fundamentals document (NA) NN10190-113. For FSK, complete fields access and 10- or 11-digit DN.
MPCIndex	is the index number of the EMPC or MPC card specified in table MPC
MPCLinkNumber	is the number of the MPC link specified in table MPCLINK
address	is the address of the X.25 node
protocol1, protocol2, protocol3, protocol4	is the protocol to use for the CDC

Creating a CDC

where

access	is the FSK access method required by the LEA: dedicated (DE), switched local (SL), or switched remote (SR)
10- or 11-digit DN	is the 10- or 11-digit DN used for the FSK SL or DE CDC circuit. For FSK switched remote access, the 10- or 11-digit DN must translate to a trunk.
agency	is 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 input:

```
> cdc add 1 x.25 0 3 11111111 3 1 128 0 agency1
```

MAP response:

```
CDC ADD DONE.
```

Note: The example input above is for an administrative user. The example below is for a non-administrative user.

Example input:

```
> cdc add 1 x.25 7 2 22222222 3 1 128 0
```

MAP response:

```
CDC ADD DONE.
```

4 Ensure the CDC has been added by typing:

```
> cdc list all
```

Example of a MAP response:

```
Index Type Access CDC DN      Agency
     [Associated SINs]
-----------------------------------------------------
    1  X.25 7 2   22222222        3 1 128 0
```

Creating a CDC

```
     SIN1 SIN2 SIN3 SIN8    AGENCY1
    2  X.25 6 2   22222222        3 1 128 0
     SIN4 SIN5 SIN6 SIN7    AGENCY2

CDC LIST DONE.
```

Note: An administrative user will be given CCR information for all agencies (see MAP response above). A non-administrative user will see infomation only for those CCRs associated with the user's agency (see MAP response below).

Example of a MAP response:

```
Index Type Access CDC DN      Agency
     [Associated SINs]
-----------------------------------------------------
    1  X.25 7 2   22222222        3 1 128 0
     SIN1 SIN2 SIN3 SIN8

CDC LIST DONE.
```

5 Test the CDC by typing:

```
> test cdc <index>
```

where

index — is the cdc index number added in step 3

Example input:

```
> test cdc 3
```

Example of a MAP response:

```
SUCCESSFUL TEST CALL FOR CDC DN 8197661234
```

If the test call is made for an FSK SR CDC and a modem is answering the call, remember to force the modem to release the connection after the test command is completed; otherwise, the line can be left in a lockout PLO state (left offhook after the trunk has been released when the test call is taken down).

After a CDC has been added and tested, you can associate it with one or more surveillances. See procedure "Associating a CDC with a surveillance" on page 8-31.

6 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.

Prerequisites

The USNBD user who is 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
- whether a monitored replacement party (MRP) can be provided for a monitored call
- whether inband digit collection should be performed
- whether the call content and inband digits of calls made within private networks will be intercepted
- whether the number of the calling party can be delivered to the LEA
- whether the feature status message should be delivered and how often
- whether the surveillance status should be delivered and how often

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

Adding a surveillance

Summary of Adding a surveillance

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

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

```
> surv add <handle> <case_id> <sin> <mrp>
<calling_party_num_delivery> <inband_delivery>
<feature_status_periodic> <feature_status_interval>
<surveillance_status_periodic>
<surveillance_status_interval> <PNI> <agency>
```

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

```
> surv add <handle> <case_id> <sin> <mrp>
<calling_party_num_delivery> <inband_delivery>
```

Adding a surveillance

```
<feature_status_periodic> <feature_status_interval>
<surveillance_status_periodic>
<surveillance_status_interval> <PNI>
```

where

handle	is one of the following: • DN with <subject_dn> • LEN with <site> <frame> <unit> <drawer> <circuit> • KEY with <site> <frame> <unit> <drawer> <circuit> <key> • LTID with <ltgrp> <ltnum> ***Note:*** Refer to the SURV ADD command Usage notes on 3-46 for guidelines on what to use to identify the subject.
case_id	is the identification of the surveillance provided by the LEA (1 through 16 alphanumeric characters)
sin	is the surveillance identification number (SIN), which uniquely identifies the surveillance (1 through 25 alphanumeric characters)
mrp	is Y or N to indicate whether an MRP can be provided for a monitored call
calling_party_num_delivery	is Y or N to indicate whether the calling party DN can be delivered to the LEA
inband_delivery	is Y or N to indicate if inband delivery is applicable
feature_status_periodic	is Y or N to indicate whether a feature status periodic message should be generated for the surveillance
feature_status_interval	is a time parameter in minutes (15 to 1440 in increments of 15) to indicate the amount of time between periodic messages

Adding a surveillance

where

surveillance_status_periodic	is Y or N to indicate whether a surveillance status periodic message should be generated for the surveillance
surveillance_status_interval	is a time parameter in minutes (60 to 1440 in increments of 15) to indicate the amount of time between periodic messages
PNI	is Y or N to indicate whether call content and inband digits (if a CCR is provisioned) of calls made on private networks will be intercepted
agency	is 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 of ADMIN user performing a SURV ADD and not using the defaults for feature_status_interval surveillance_status_periodic:

Example input:

```
> surv add dn 6137213456 case3 sin3 y y y y 45 y 75 n
Agency1
```

MAP response:

```
SURV ADD DONE.
```

Adding a surveillance

Example of ADMIN user performing a SURV ADD and using the defaults for feature_status_interval surveillance_status_periodic. Default is 1440.

Example input:

```
> surv add dn 6137213456 case3 sin3 y y y y y Agency1
```

MAP response:

SURV ADD DONE.

Example of non-ADMIN user performing a SURV ADD and not using the defaults for feature_status_interval surveillance_status_periodic:

Example input:

```
> surv add dn 6137213456 case3 sin3 y y y y 45 y 75 n
```

MAP response:

```
SURV ADD DONE.
```

Example of non-ADMIN user performing a SURV ADD and using the defaults for feature_status_interval surveillance_status_periodic. Default is 1440.

Example input:

```
> surv add dn 6137213456 case3 sin3 y y y y y
```

MAP 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 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” on page 8-21.

When to use this procedure

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

Prerequisites

The USNBD user who is 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
- whether monitoring information 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.

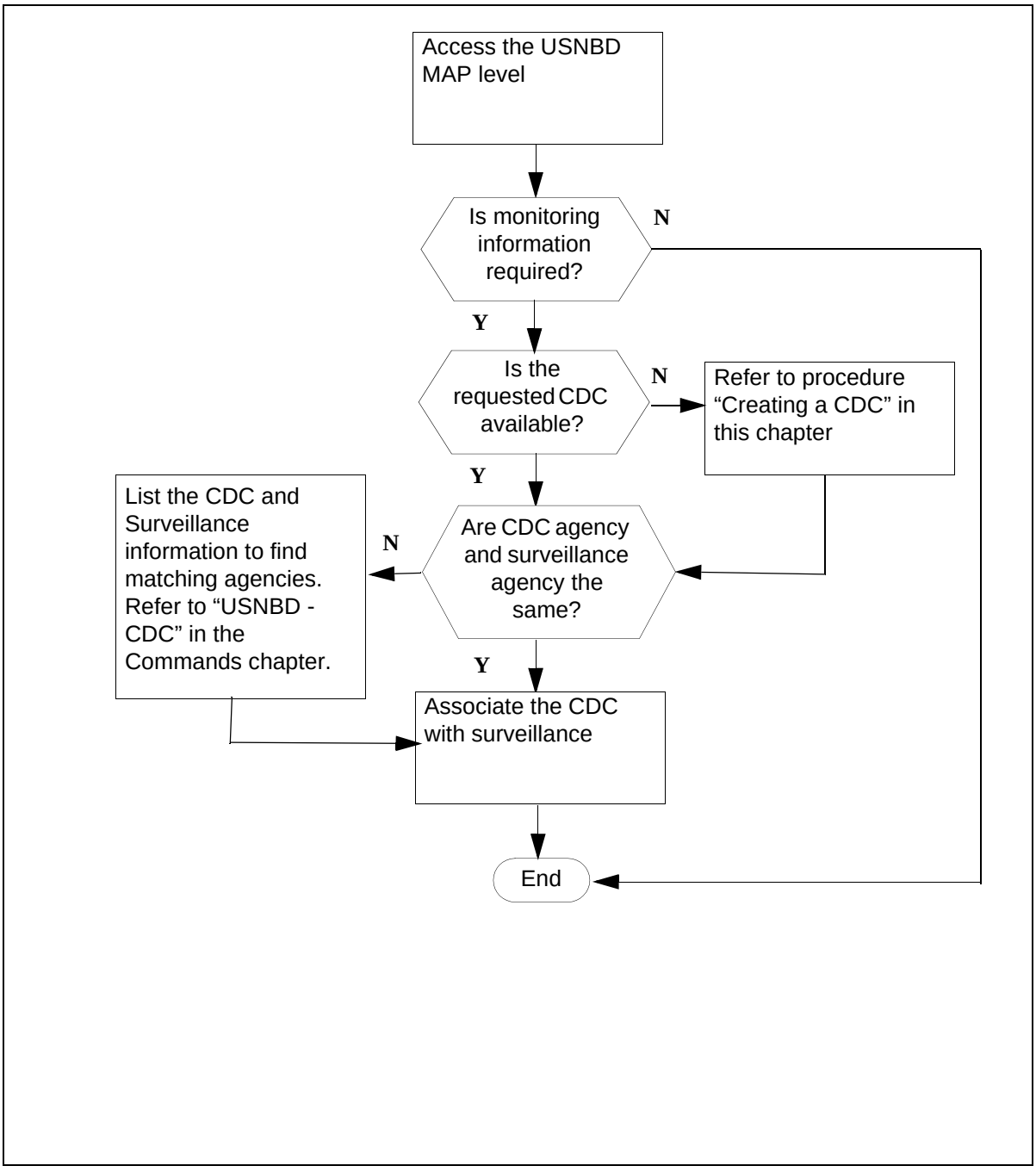
Users must enter agency data before FSK CDCs are associated with a surveillance.

Action

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

Associating a CDC with a surveillance

Summary of Associating a CDC with a surveillance



Associating a CDC with a surveillance

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

If the LEA	Then go to
requires monitoring information for the surveillance	step 2
does not require monitoring information for the surveillance	step 6

At the USNBD level of the MAP

2 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 will be shown. If the user has administrative rights, agency information will be shown for all CDCs. Display the list by typing:

```
> cdc list all
```

Example of a MAP response:

```
Index Type Access CDC DN       Agency
   [Associated SINs]
-------------------------------------------------------
    1  X.25 7 2   22222222        3 1 128 0
CDC LIST DONE.
```

Associating a CDC with a surveillance

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

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

3 Create the requested CDC using procedure “Creating a CDC” on page 8-21, then return to step 4 in this procedure.

4 Display a list of surveillances to find one with the same agency as the CDC. If the user does not have administrative rights, only surveillances for the user’s agency will be shown. If the user has administrative rights, agency information will be shown for all CDCs. Display the list by typing:

```
> surv list all
```

Example of a MAP response:

```
Subject       CaseID SIN MRP Clg_dlvry Feat_stat Int
Surv_stat Int               Status {Associated_CDC}
{Associated_CCRs}
-------------------------------------------------------
LTID ISDN2 1  CASE1 SIN1 Y Y Y 15 N 0             ACTIVE
{1} {8 6}
DN 6135520302 CASE2 SIN4 Y Y Y 15 Y 60
INACTIVE {1} {3}
```

5 Associate the requested CDC with the surveillance by typing:

```
> cdc assoc <index> <sin>
```

where

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

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

Associating a CDC with a surveillance

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 input:

```
> cdc assoc 1 sin1
```

MAP response:

```
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 associating the requested CCR(s) with the surveillance if call content is required for the surveillance.

When to use this procedure

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

Prerequisites

The USNBD user who is performing this procedure needs to 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.

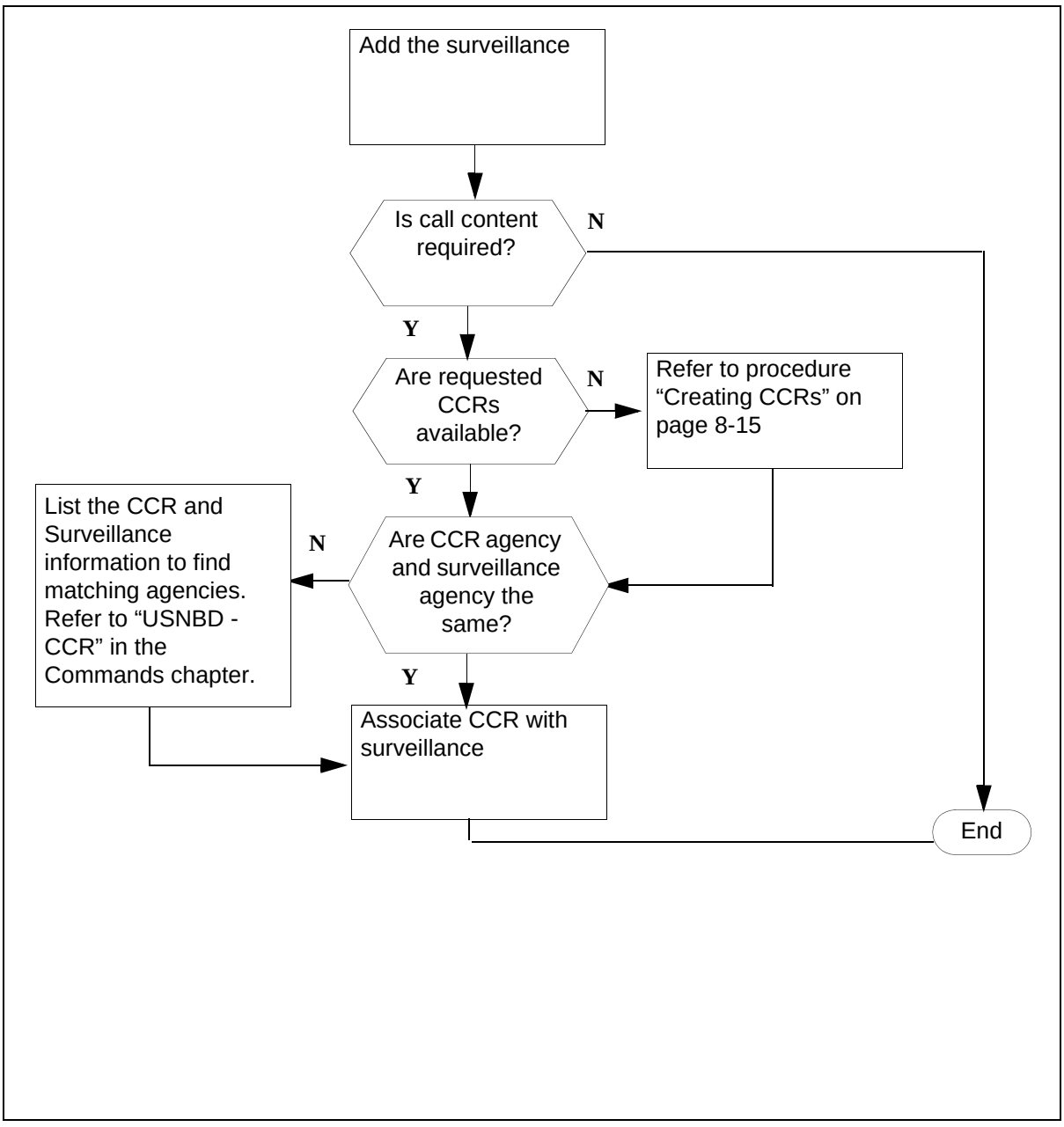
Agency data must be datafilled before switched ISUP CCCs or FSK switched remote CDCs can be associated with a surveillance.

Action

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

Associating a CCR with a surveillance

Summary of Associating a CCR with a surveillance



Associating a CCR with a surveillance

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

2 Determine if call content delivery is required.

If call content is	Then go to
required	step 3
not required	step 6

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

```
> ccr list all
```

Example of a MAP response:

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

CCR LIST DONE
```

Note: An administrative user will be given CCR information for all agencies (see MAP response above). A non-administrative user will see infomation only for those CCRs associated with the user's agency (see MAP response below).

Associating a CCR with a surveillance

Example of a MAP response:

```
Index Content CCRtype Acc CCRid CCC1/PVC1    [CCC2/PVC2]
 [Sig] [Tag]    [Sin]
-----------------------------------------------------
1 PACKET PAIRED LINE DE  9059631003        19059631003

33 VOICE COMBINED LINE DE 6135510102
  N    Y
```

Note: Look for the requested CCR(s) by their index number.

If the requested CCR(s) are	Then go to
not available	step 4
available	step 5

4 Create one or more CCRs using procedure “Creating CCRs” on page 8-11, then return to step 5 in this procedure.

5 Display a list of surveillances to find one with the same agency as the CCR. If the user does not have administrative rights, only surveillances for the user’s agency will be shown. If the user has administrative rights, agency information will be shown for all CCRs. Display the list by typing:

```
> surv list all
```

Example of a MAP response:

```
Subject       CaseID SIN MRP Clg_dlvry Inband_dlvry
(Feat_status Interval) (Surv_status Interval) PNI Agency
Status {Associated_CDC} {Associated_CCRs}
-----------------------------------------------------
LTID ISDN2 1  CASE1 SIN1 Y Y Y
              (N 15) (N 0) N CIA
              ACTIVE {1} {8 6}
DN 6135520302 CASE2 SIN4 Y Y Y
              (N 15) (Y 60) N NIL
              INACTIVE {1} {3}
```

Associating a CCR with a surveillance

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

```
> ccr assoc <index> <sin>
```

where

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

Example input:

```
> ccr assoc 10 sin1
```

MAP response:

```
CCR ASSOC DONE.
```

Note: When the subject of a surveillance is an ISDN NI1 terminal datafilled with PVC1 and the AFC or ACOU feature, the number of CCRs to associate with the surveillance must be in accordance with the number AFC keys. Multiple CCRs are required to ensure call content can be delivered for a second or subsequent call to or from the subject.

Once the CCR ASSOC command is entered for dedicated CCRs, a call is made to the CCC circuit(s) using standard translations and routing. When call setup is successful, 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 and the EXTOVFL register of key FBSEXT in the EXT operational measurement (OM) group is incremented.

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 an LEA requests that a surveillance be activated on a subject.

Prerequisites

The USNBD user who is performing this procedure requires the SIN of the surveillance to be activated.

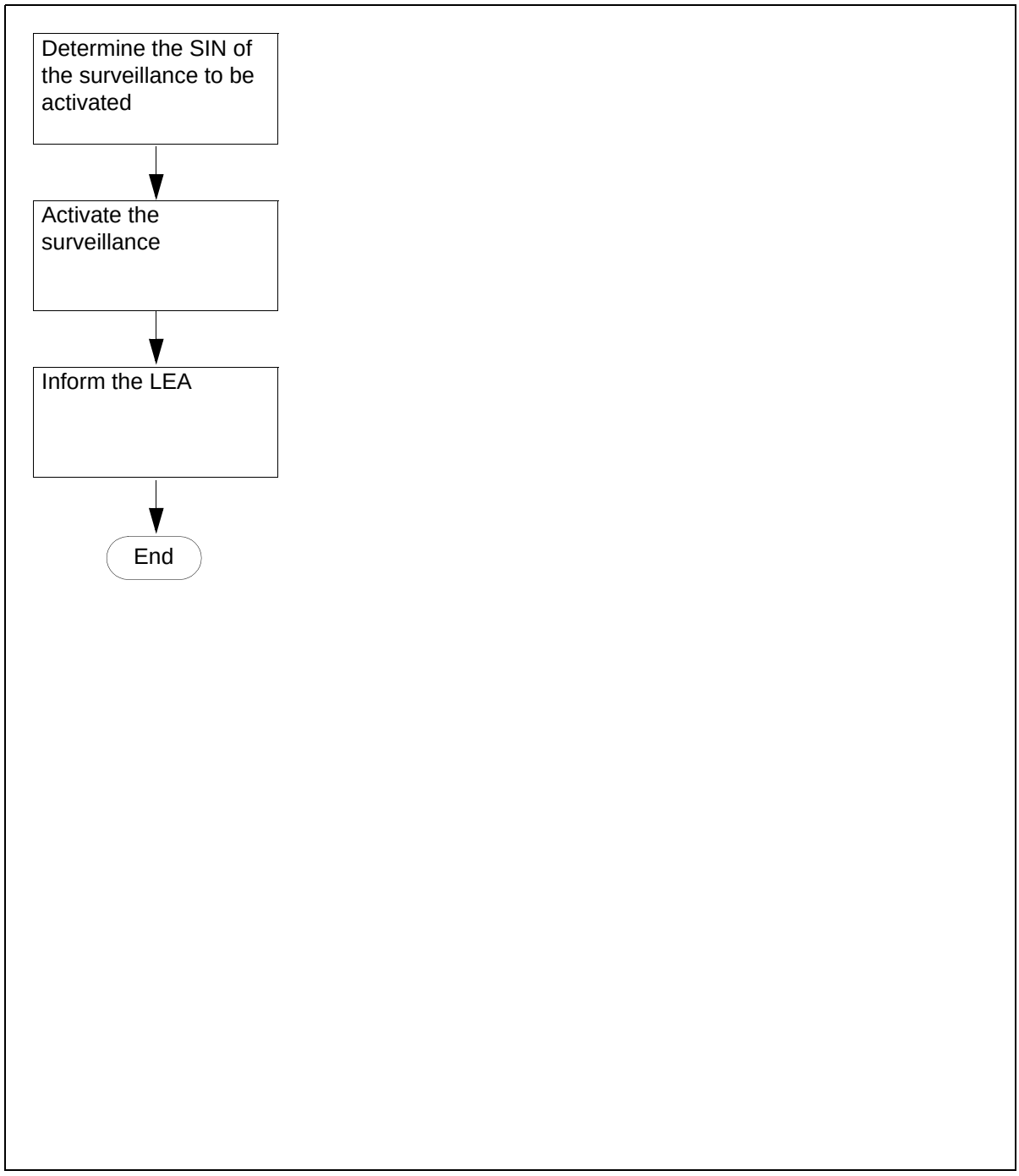
The USNBD user performing this procedure must be associated with the same agency as the surveillance will have or have USNBD administrative rights.

Action

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

Activating a surveillance

Summary of Activating a surveillance



Activating a surveillance

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

2 Display a list of inactive surveillances to obtain the surveillance identification number (SIN) that corresponds to the caseID of the surveillance to be activated by typing:

```
> surv list inact
```

Example of a MAP response:

```
Subject       CaseID SIN MRP Clg_dlvry Inband_dlvry
(Feat_status Interval) (Surv_status Interval) PNI Agency
Status {Associated_CDC} {Associated_CCRs}
-------------------------------------------------------
DN 6136211088  case1 sin1 Y Y N
               (N 0) (N 0) Y NIL
               INACTIVE {1} {10}
SURV LIST DONE.
```

Note: In the example above, the SIN of the surveillance is sin1.

Activating a surveillance

3 Activate the surveillance by typing:

```
> surv act <sin>
```

where

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

Example input:

```
> surv act sin1
```

MAP response:

```
SURV ACT DONE.
```

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

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

4 Inform the LEA that the surveillance has been activated.

5 You have completed this procedure.

Determining status of Held Conference

Purpose of this procedure

The purpose of this procedure is to enable USNBD to monitor the held conference call which has been established or caused by the subject's service.

> ***Note:*** The UNB_OFCWIDE command can only be accessed by administrative users.

When to use this procedure

Use this procedure when an LEA requests that a surveillance be activated on a subject.

Prerequisites

The USNBD user who is performing this procedure should contact the switch-provisioning group to ensure that sufficient conference circuits exist before turning HELDMON on. The need for conference circuits is determined by:

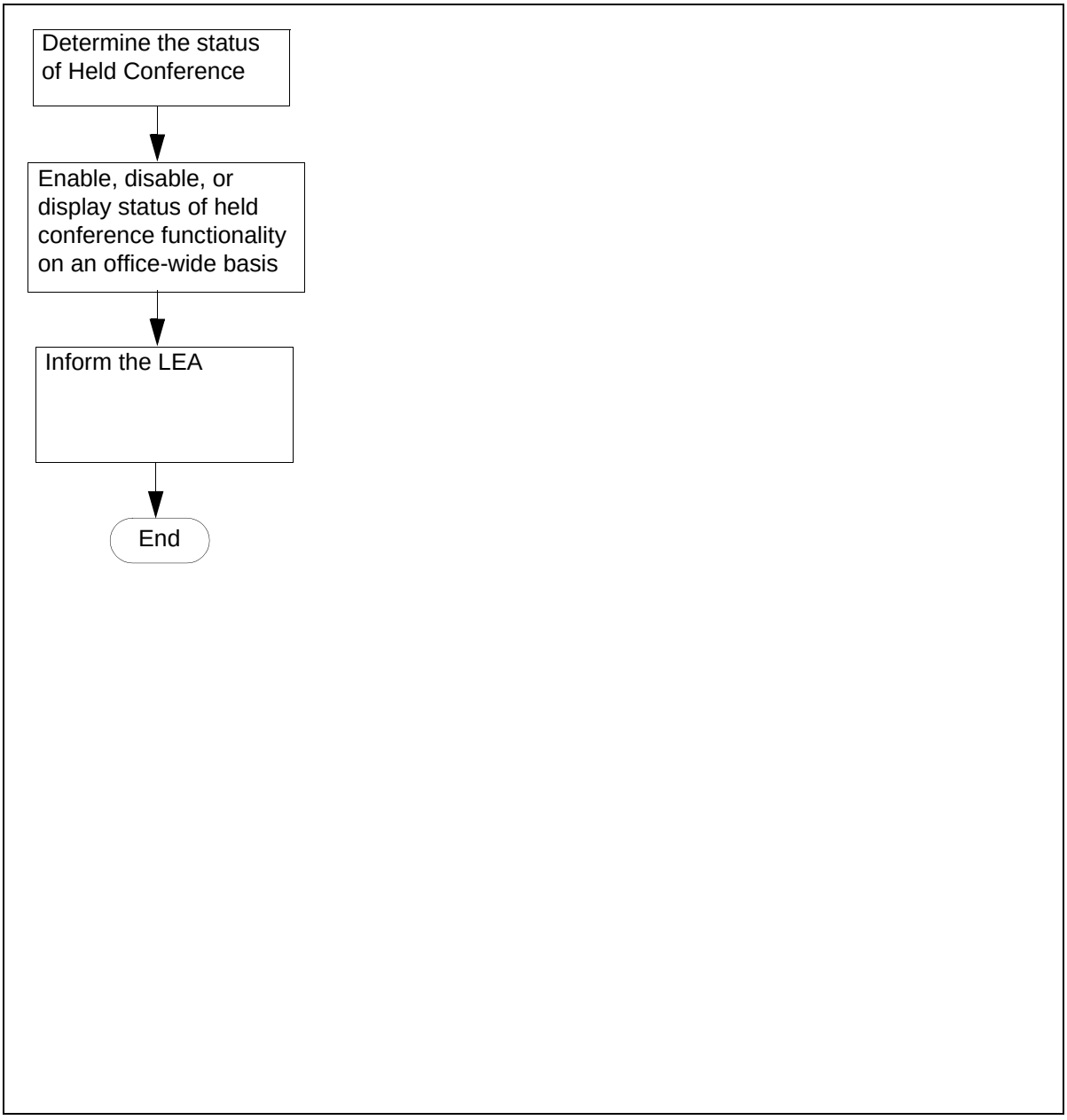
- HELDMON is set to ON
- the number of surveillances on the switch
- the number of combined CCRs existing on the switch

Action

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

Determining status of Held Conference

Summary of Determining the status of Held Conference



Determining status of Held Conference

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

2 Enter the Admin command by typing:

```
> unb_ofcwide
```

MAP response:

```
Next par is: <command> {HELDMON <heldmon_opts> {ON,
                                                 OFF,
                                                 STATUS}}
```

3 Enter the sub-command to enable, disable and display the status of content of held conference delivery, by typing:

```
> heldmon
```

MAP response:

```
Next par is: <command> {HELDMON <heldmon_opts> {ON,
                                                 OFF,
                                                 STATUS}}
```

Determining status of Held Conference

4 Enter a Heldmon option by typing ON, OFF, or STATUS:

where

ON	Activates the held conference functionality
OFF	Deactivates the held conference functionality
STATUS	Displays the status of held conference functionality on an office-wide basis

Example input:

```
> heldmon on
```

MAP response:

```
HELDMON ON DONE.
```

5 Return to the CI environment, by typing:

```
> quit
```

MAP response:

```
CI:
```

6 Inform the LEA of the status of held conference.

7 You have completed this procedure.

Ensuring inband digits delivery

Purpose of this procedure

The purpose of this procedure is to ensure inband digits delivery. This procedure uses a new exec_lineup which is a logical set of exec IDs which can be used as a group to perform tasks needed to originate, handle and supervise a call for a given peripheral type. Up to 254 exec IDs may be placed in a given exec_lineup.

Note: The new exec_lineup defined by this feature is MTM1EX.

When to use this procedure

The new exec_lineup needs to be downloaded to the MTMs as part of the USNBD setup process to ensure inband digits delivery functionality.

Note: This procedure should be performed in a low-traffic period, normally by switch maintenance personnel.

Prerequisites

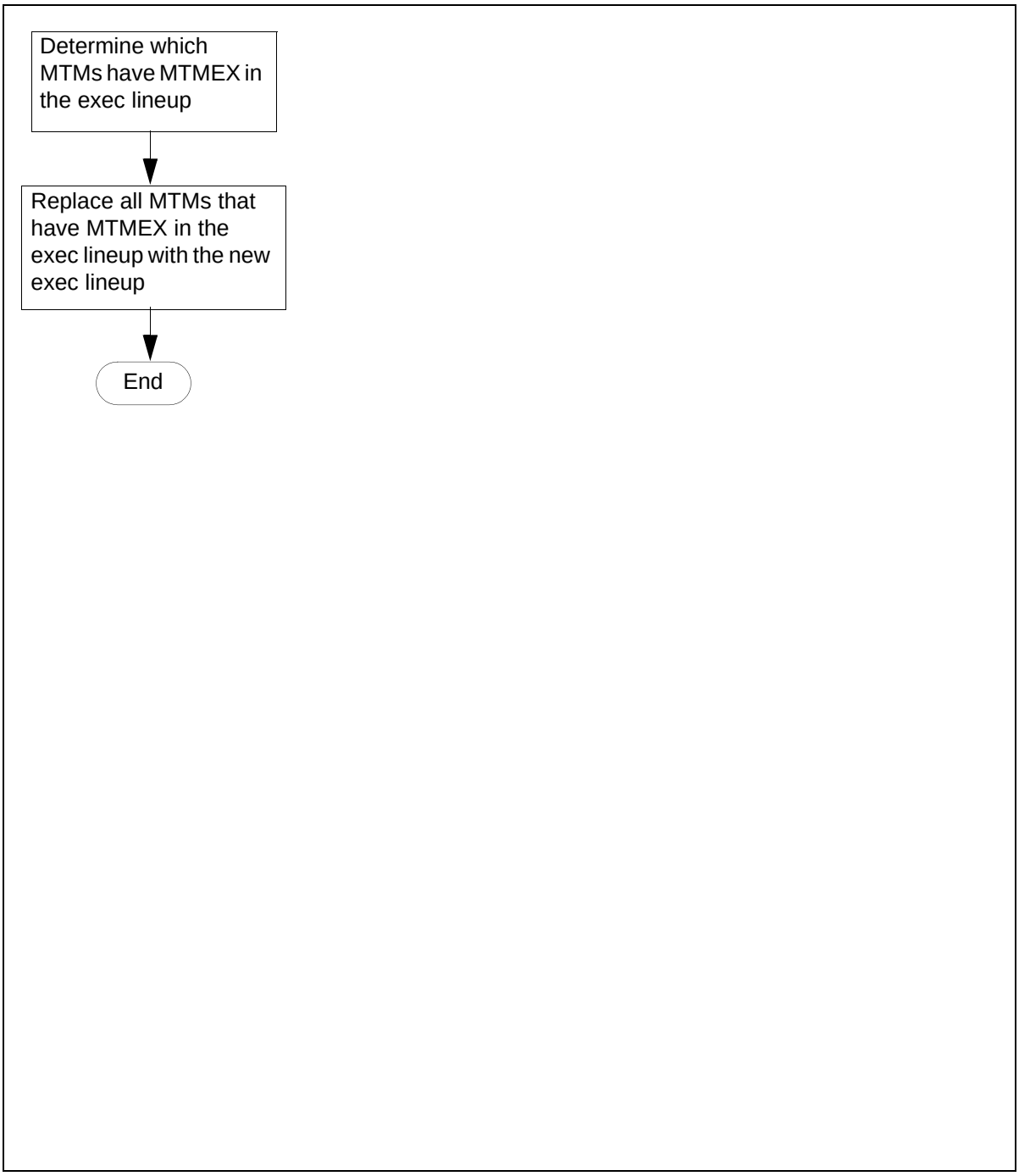
No prerequisites.

Action

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

Ensuring inband digits delivery

Summary of ensuring inband digits delivery



Ensuring inband digits delivery

Step	Action

At the CI level of the MAP

1 Access table TMINV by typing:

```
> table tminv
```

MAP response:

```
table tminv
```

2 To determine which MTMs have MTMEX in the exec lineup, list all the tuples in table TMINV by typing:

```
> list all
```

MAP response:

```
MTM 0 ISME 7 7 0 B 7 0 55 FX42AA MTMKA02 MTMEX SHELF
```

3 Replace each and every MTM, which has MTMEX as exec lineup, with the new exec lineup MTM1EX, by typing:

```
> REP MTM 0 ISME 7 7 0 B 7 0 55 FX42AA MTMKA02 MTM1EX
SHELF
```

MAP response:

```
MTM 0 ISME 7 7 0 B 7 0 55 FX42AA MTMKA02 MTM1EX SHELF
```

Ensuring inband digits delivery

To download the new exec lineup to the MTMs, use step 4 or step 5.

CAUTION
Partial Service Interruption

Both steps used below result in a partial service interruption. However, the impact is more severe in step 5 because all MTMs are loaded in parallel.

4 Return to the CI level of MAP, by typing:

```
> mapci;mtc;pm
```

For every MTM that has the exec lineup datafill changed, execute the following steps:

```
> post <MTM> 0
```

Busy the MTM by typing:

```
> bsy
```

Go to the DISKUT level by typing:

```
> diskut
```

List the volume which contains the load file for the PM. For example, if MTMKA02 is the load file and is available in volume S01DPMLOADS, the following command must be executed:

```
> lf s01dpmloads
```

Load the MTM with the new exec, by typing:

```
> loadpm
```

Once the load is complete, RTS the MTM, by typing:

```
> rts
```

Ensuring inband digits delivery

If step 4 above was not followed, proceed to step 5. Only one of these steps need be used.

5 Go to the SWACTCI level, by typing the following command at the CI level:

```
> bcsupdate; swactci
```

MAP response:

```
swactci
```

At the SWACTCI prompt, type:

```
> restorexecs tm
```

MAP response:

```
WARNING: a call processing outage will occur on
peripherals that will receive EXECs. Do you wish to
continue?
```

To restore the EXEC, confirm by typing YES or Y.

```
> yes
```

6 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 an LEA requests that a surveillance on a subject be deactivated.

Prerequisites

The USNBD user who is performing this procedure requires the caseID of the surveillance to be deactivated.

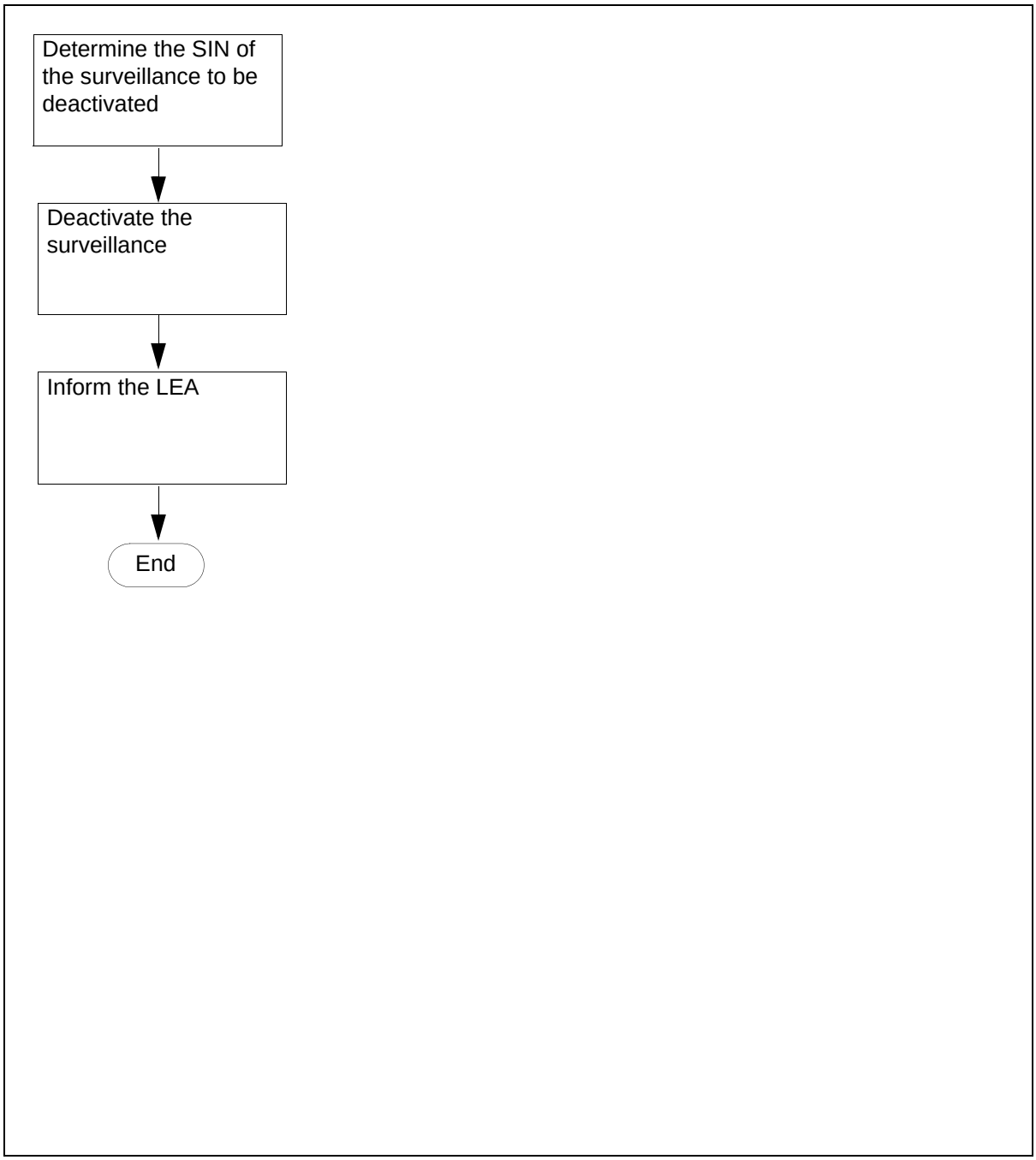
The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights.

Action

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

Deactivating a surveillance

Summary of Deactivating a surveillance



Deactivating a surveillance

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

2 Display a list of active surveillances to determine the surveillance identification number (SIN) that corresponds to the caseID of the surveillance to be deactivated by typing:

```
> surv list act
```

Example of a MAP response:

```
Subject       CaseID SIN MRP Clg_dlvry Inband_dlvry
(Feat_status Interval) (Surv_status Interval) PNI Agency
Status {Associated_CDC} {Associated_CCRs}
-------------------------------------------------------
DN 6136211088  case1 sin1 Y Y N
               (N 0) (N 0) N NIL
               ACTIVE {1} {10}
SURV LIST DONE.
```

Note: In the example above, the SIN of the surveillance is sin1.

3 Deactivate the surveillance by typing:

```
> surv deact <sin>
```

where

sin	is the surveillance identification number (SIN) of the surveillance to be deactivated

Example input:

```
> surv deact sin1
```

Deactivating a surveillance

MAP 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.

4 Inform the LEA that the surveillance has been deactivated.

5 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 an LEA requests that a surveillance on a subject be taken down.

Prerequisites

The USNBD user who is performing this procedure requires the following information:

- the SIN id 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

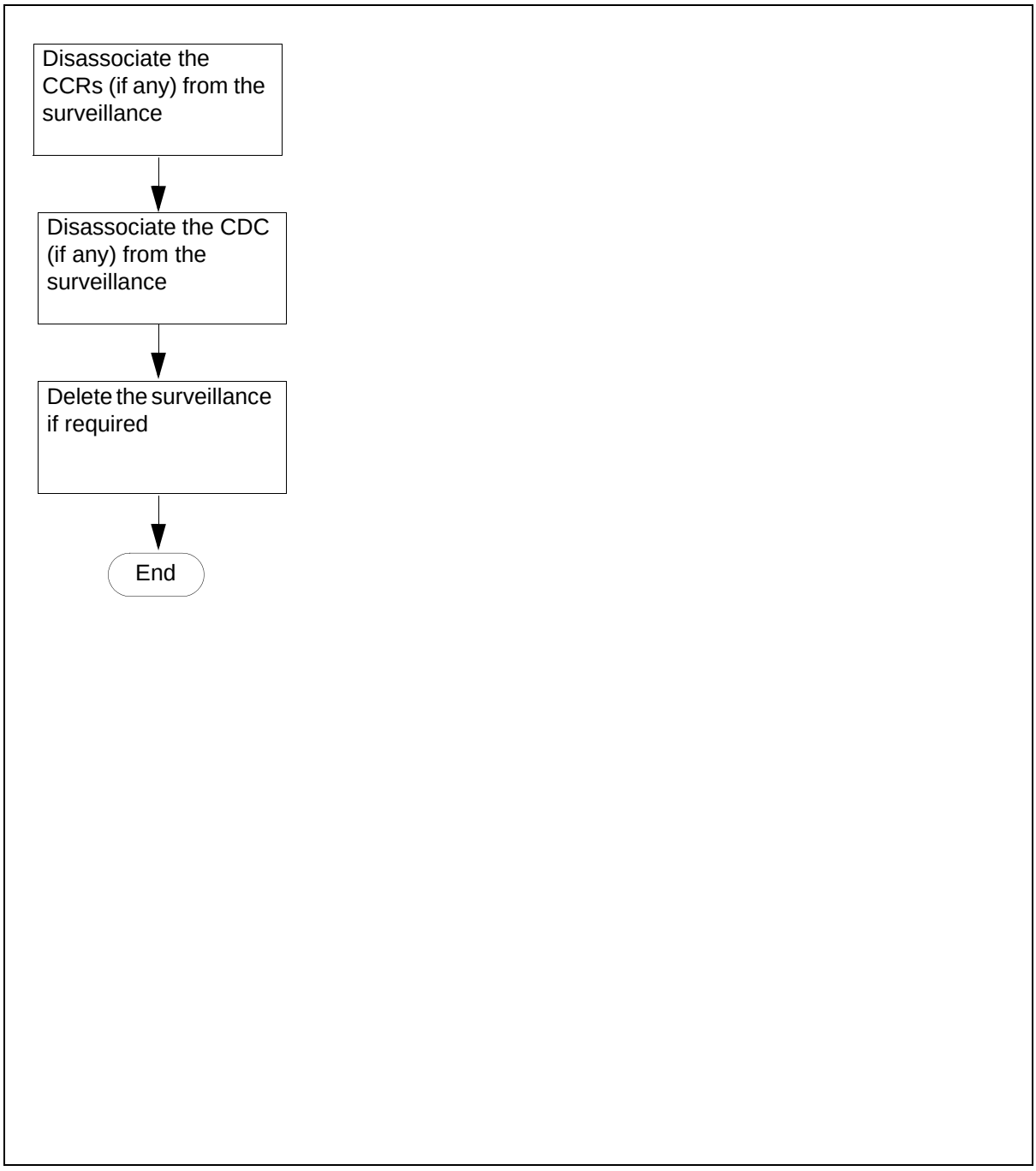
The USNBD user performing this procedure must be associated with the same agency as the surveillance or have USNBD administrative rights.

Action

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

Taking down a surveillance

Summary of taking down a surveillance



Taking down a surveillance

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

2 Display a list of inactive surveillances to obtain the surveillance identification number (SIN) that corresponds to the caseID of the surveillance to be taken down by typing:

```
> surv list inact
```

Example of a MAP response:

```
Subject       CaseID SIN MRP Clg_dlvry Inband_dlvry
(Feat_status Interval) (Surv_status Interval) PNI Agency
Status {Associated_CDC} {Associated_CCRs}
-------------------------------------------------------
DN 6136211088  case1 sin1 Y Y N
               (N 0) (N 0) N NIL
               INACTIVE {1} {10}
SURV LIST DONE.
```

Note: In the example above, the SIN of the surveillance is sin1.

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

If a CDC is	Then go to
associated with the surveillance	step 4
not associated with the surveillance	step 5

Taking down a surveillance

4 Disassociate the CDC from the surveillance by typing:

```
> cdc disassoc <sin>
```

where

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

Example input:

```
> cdc disassoc sin1
```

MAP response:

```
CDC DISASSOC DONE.
```

5 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	Then go to
associated with the surveillance	step 6
not associated with the surveillance	step 7

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

```
> ccr disassoc <index>
```

where

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

Example input:

```
> ccr disassoc 8
```

MAP response:

```
CCR DISASSOC DONE.
```

Taking down a surveillance

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

7 If required, delete the surveillance by typing:

```
> surv del <sin>
```

where

sin	is the surveillance identification number (SIN) of the surveillance to be deleted

Example input:

```
> surv del sin1
```

MAP response:

```
SURV DEL DONE.
```

If it is necessary to delete the	Then go to procedure
CCR(s)	"Deleting a CCR" on page 8-63
CDC	"Deleting a CDC" on page 8-67

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 kept and reused by other surveillances, therefore confirm with the LEA that the CCR really needs to be deleted.

Prerequisites

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

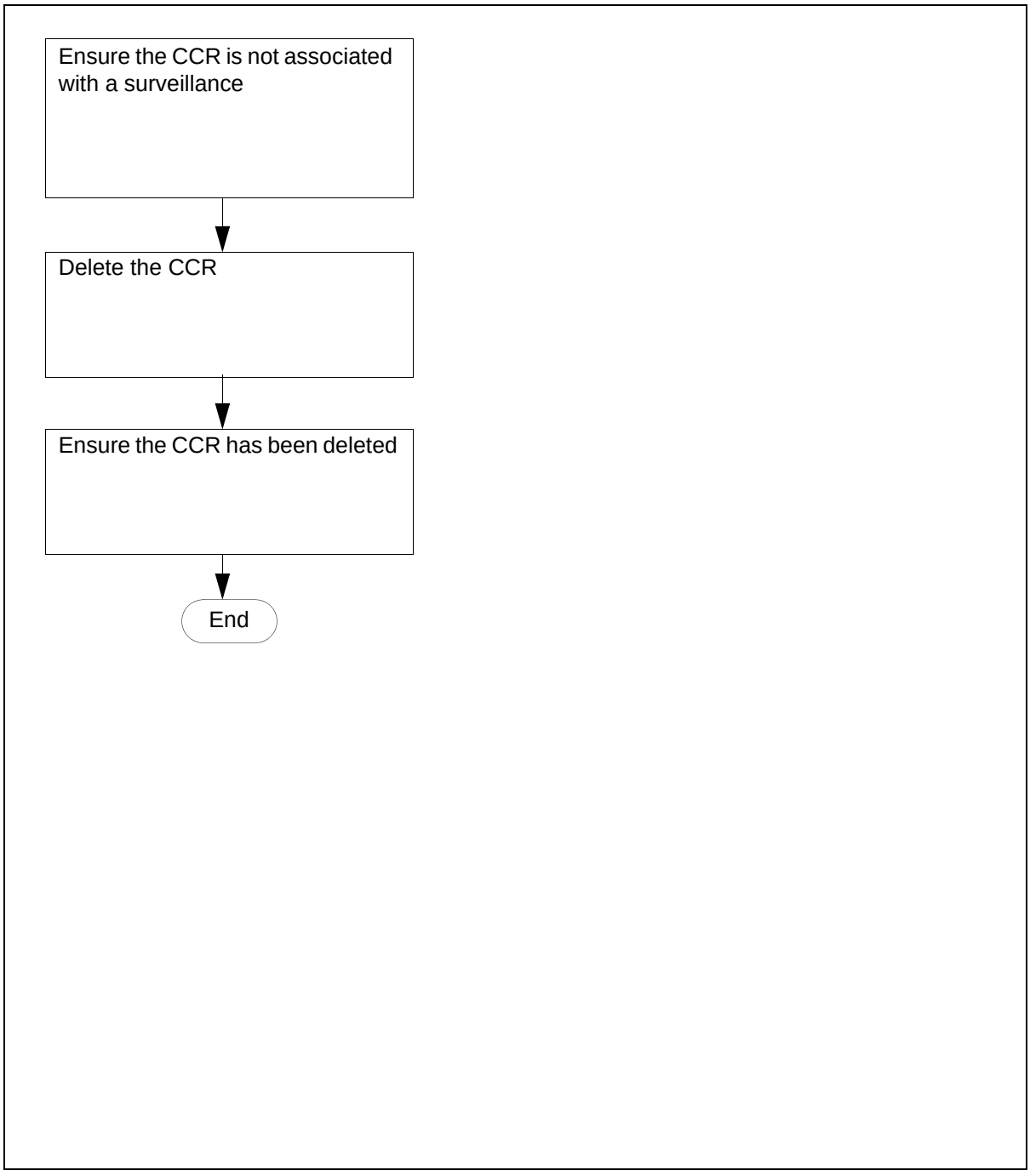
The USNBD user who disassociates the CCR from its surveillance must be associated with the same agency as the CCR or have USNBD administrative rights.

Action

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

Deleting a CCR

Summary of Deleting a CCR



Deleting a CCR

Step	Action

At the USNBD level of the MAP

1 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
```

Example of a MAP response:

```
Index Content CCRtype Acc CCRid CCC1/PVC1 [CCC2/PVC2]
[Sig] [Tag]    [Sin]     Agency
-------------------------------------------------
1 PACKET PAIRED LINE DE 9059631003        19059631003
                          AGENCY1
2 VOICE PAIRED LINE DE 6135519970            6135519971
  Y    Y                  DEFAULT
3 PACKET PAIRED TRUNK  PT1X75OG 1 1PT1X75OG 12
                          AGENCY2
CCR LIST DONE.
```

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

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

If the CCR is	Then go to
associated with a surveillance	step 2
not associated with a surveillance	step 3

2 Disassociate the CCR from the surveillance by typing:

```
> ccr disassoc <index>
```

where

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

Deleting a CCR

Example input:

```
> ccr disassoc 10
```

MAP response:

```
CCR DISASSOC DONE.
```

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

3 Delete the CCR by typing:

```
> ccr del <index>
```

where

index	is the index number (1 through 500) of the CCR to be deleted

Example input:

```
> ccr del 10
```

MAP response:

```
CCR DEL DONE.
```

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

4 Ensure that the CCR has been deleted by typing:

```
> ccr list all
```

Example of a MAP response:

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

5 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 kept and reused by other surveillances, therefore confirm with the LEA that the CDC really 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

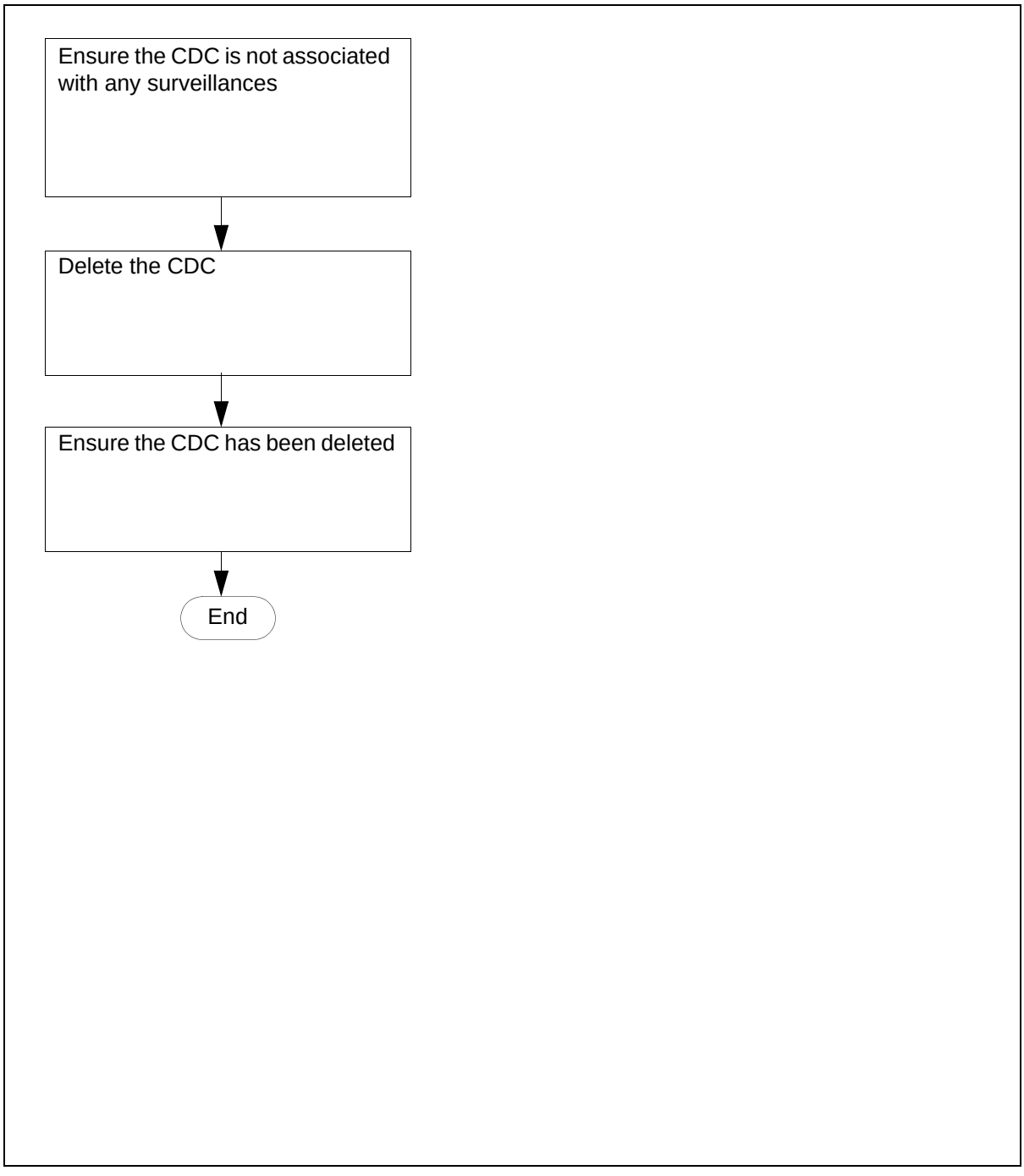
The USNBD user who disassociates the CDC from its surveillance must be associated with the same agency as the CDC or have USNBD administrative rights.

Action

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

Deleting a CDC

Summary of Deleting a CDC



Deleting a CDC

Step	Action

At the USNBD level of the MAP

1 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

Index Type Access CDC DN        Agency
      [Associated SINs]
-----------------------------------------------------
    1 X.25 7 2   22222222        3 1 128 0
     SIN1 SIN2 SIN3 SIN8    AGENCY1
    2 X.25 6 2   22222222        3 1 128 0
     SIN4 SIN5 SIN6 SIN7    AGENCY2
CDC LIST DONE.
```

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

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

If the CDC is	Then go to
associated with a surveillance	step 2
not associated with a surveillance	step 3

2 Disassociate the CDC from the surveillance by typing:

```
> cdc disassoc <sin>
```

where

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

Example input:

```
> cdc disassoc sin1
```

Deleting a CDC

MAP response:

```
CDC DISASSOC DONE.
```

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

3 Delete the CDC by typing:

```
> cdc del <index>
```

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.

4 Ensure the CDC has been deleted by typing:

```
> cdc list all
```

Example of a MAP response:

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

5 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 a switched ISUP CCC or an FSK switched remote CDC that is no longer required. Once a USNBD agency has been deleted, associated CCRs, CDCs, surveillances, and users will lose the agency information.

Prerequisites

The following requirements must be met before deleting an agency:

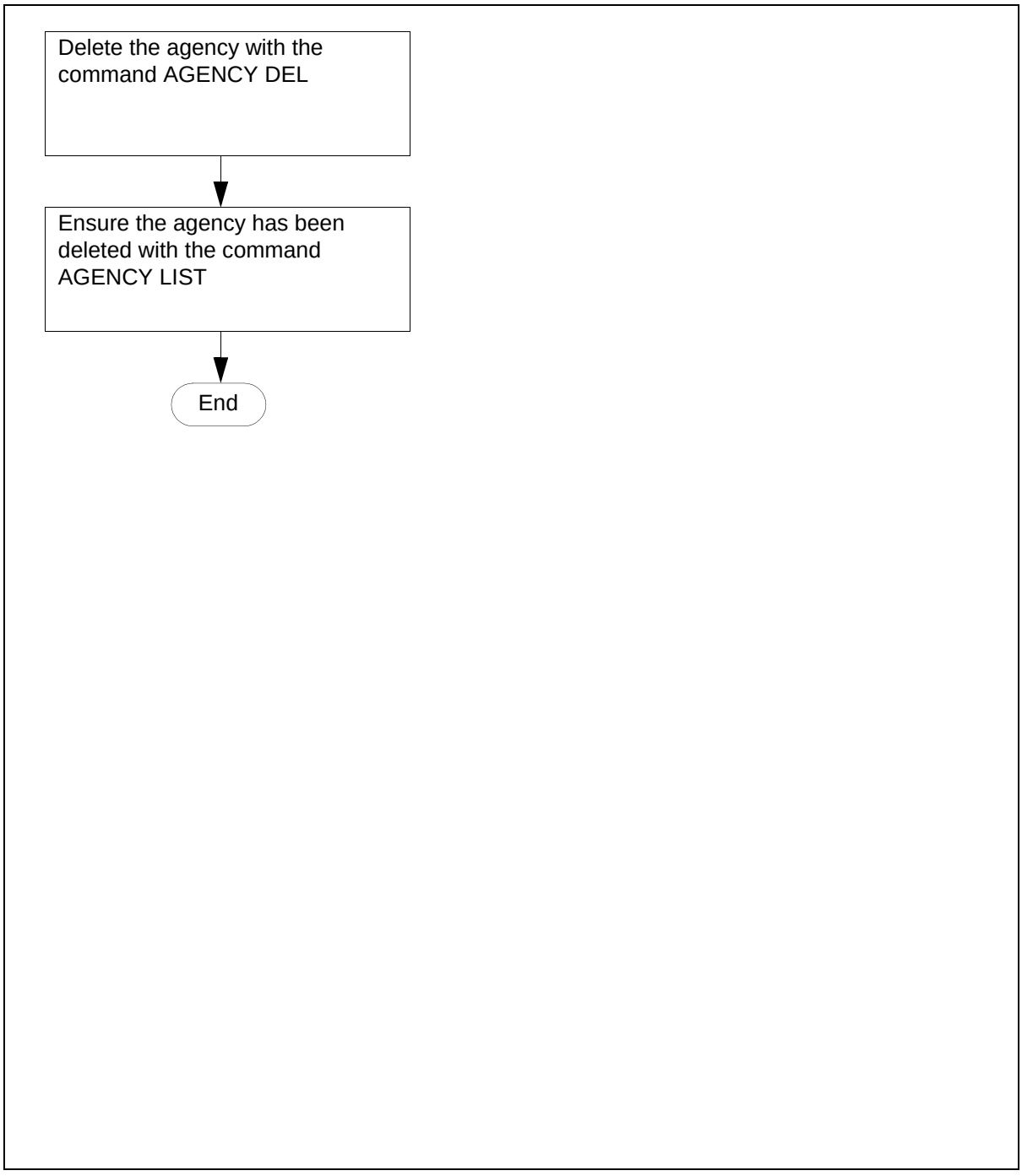
- the user must have the agency name
- switched ISUP CCRs corresponding to the agency are disassociated from all surveillances
- FSK switched remote CDC corresponding to the agency are disassociated from all surveillances

Action

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

Deleting USNBD agencies

Summary of Deleting USNBD users



Deleting USNBD agencies

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

2 Delete an agency by typing:

```
> agency del <agency_name>
```

where

agency_name is the agency to be deleted

Example input:

```
> agency del agency1
```

MAP response:

```
AGENCY DEL DONE.
```

3 Ensure the user has been deleted by typing:

```
> agency list
```

Example of a MAP response:

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

Deleting USNBD agencies

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 an attempt is made to delete the only remaining administrator, the following message is displayed:

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

It is recommended to have at least two USNBD users with administrator privileges at all times.

Prerequisites

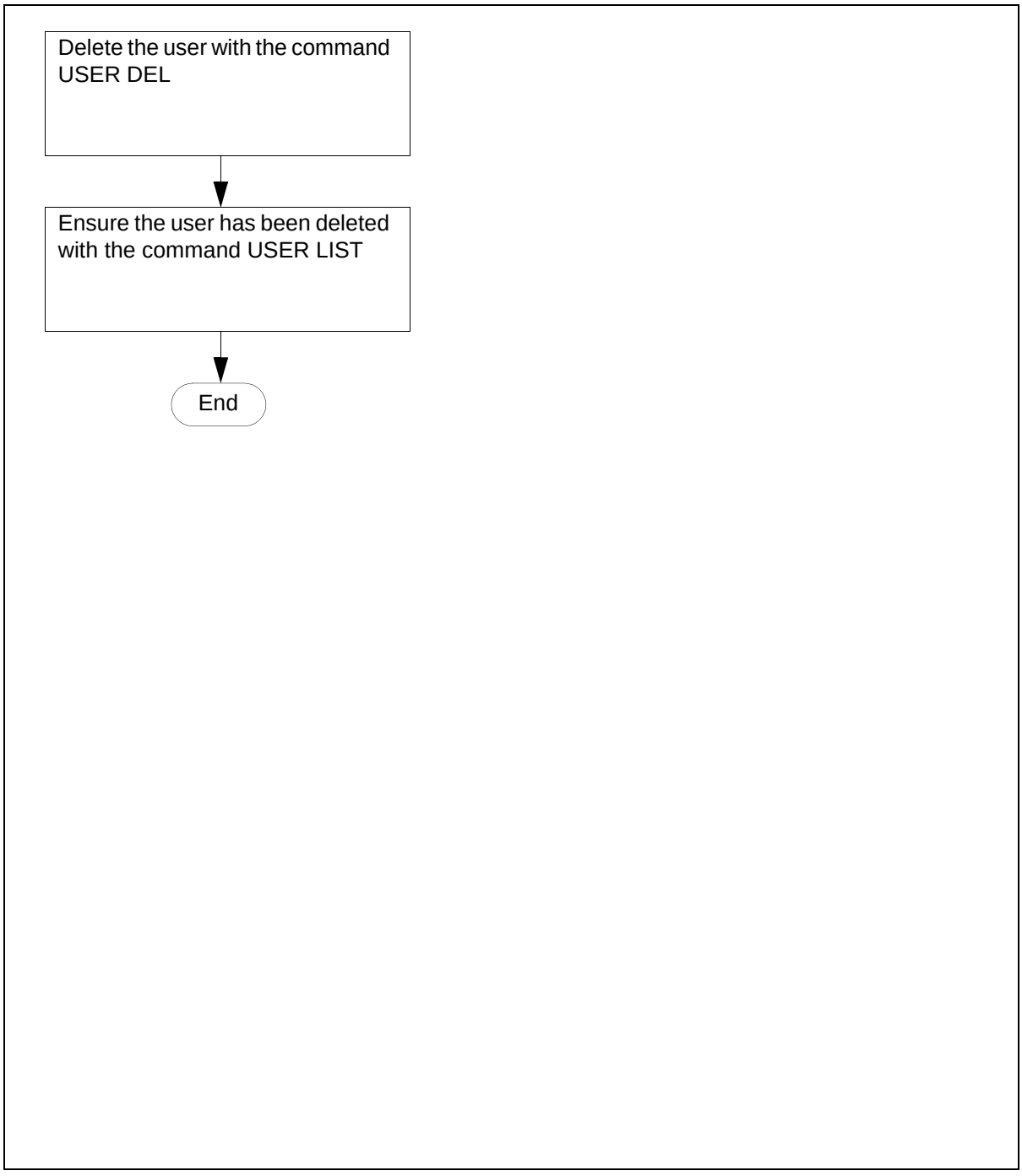
None

Action

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

Deleting USNBD users

Summary of Deleting USNBD users



Deleting USNBD users

Step	Action

At the CI level of the MAP

1 Access the USNBD level of the MAP by typing:

```
> usnbd
```

MAP response:

```
USNBD:
```

At the USNBD level of the MAP

2 Delete a user by typing:

```
> user del <user_id>
```

where

user_id is the user id of the user to be deleted

Example input:

```
> user del user1
```

MAP response:

```
USER DEL DONE.
```

3 Ensure the user has been deleted by typing:

```
> user list
```

Example of a MAP response:

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

USER LIST DONE.
```

4 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

Prior to deactivating USNBD,

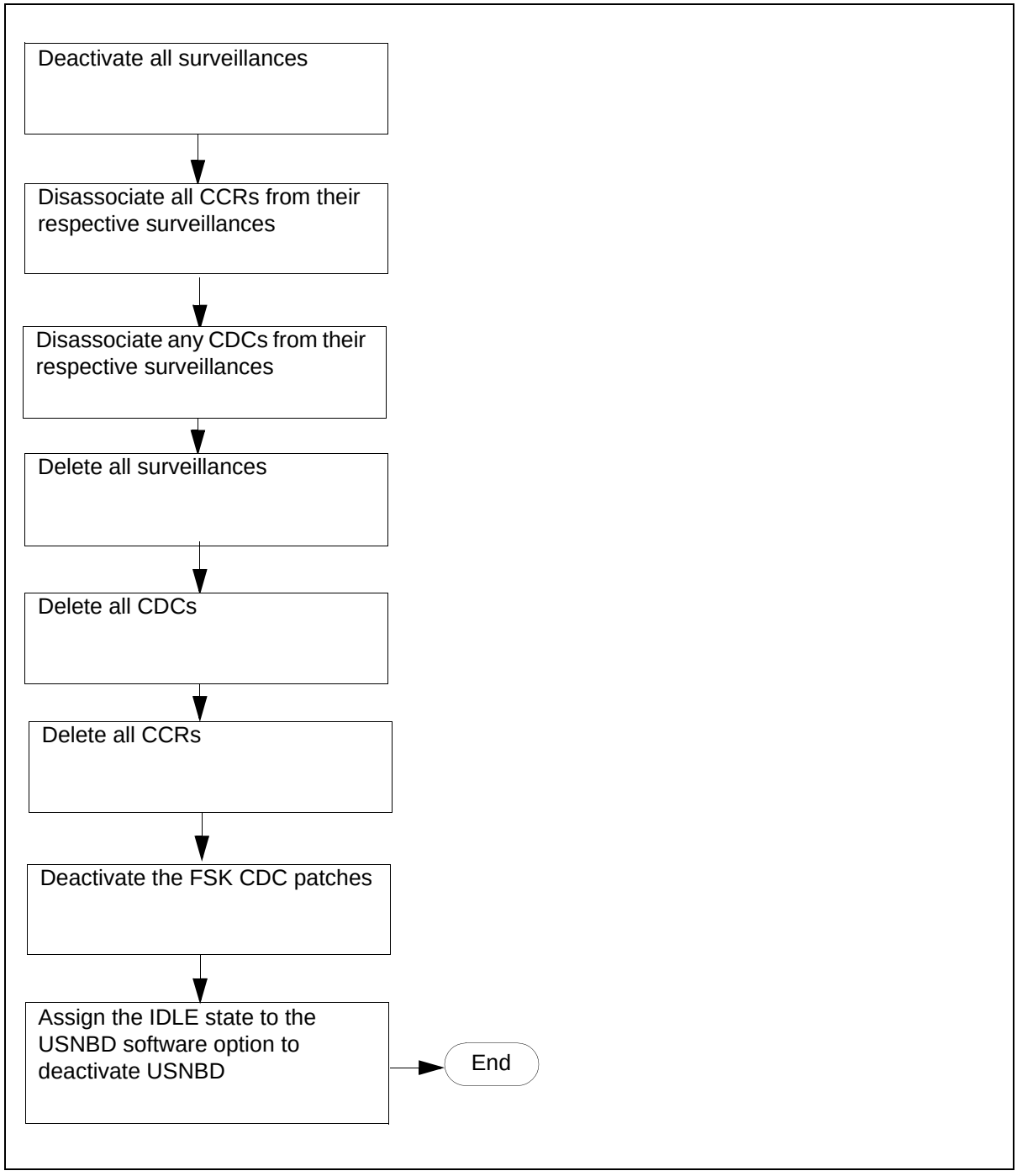
- deactivate all surveillances
- disassociate all call content resources (CCR) from their respective surveillances
- disassociate any CDCs from their respective surveillances
- delete all surveillances
- delete all CDCs
- delete all CCRs

Action

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

Deactivating SOC option NBD00003

Summary of Deactivating USNBD in an office



Deactivating SOC option NBD00003

Step	Action

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

```
> surv list act
```

Example of a MAP response:

```
Subject       CaseID SIN MRP Clg_dlvry Inband_dlvry
(Feat_status Interval) (Surv_status Interval) PNI Agency
Status {Associated_CDC} {Associated_CCRs}
-------------------------------------------------------
DN 6137213456  case1 sin1 Y Y N
               (N 0) (N 0) Y NIL
               ACTIVE { 1 } { 16 }
DN 8196696543  case2 sin2 Y Y N
               (N 0) (N 0) Y NIL
               ACTIVE { 2 } { 41 }
SURV LIST DONE.
```

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>
```

where

sin	is the surveillance identification number (SIN) of the surveillance to be deactivated

Example input:

```
> surv deact sin1
```

MAP 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
```

Deactivating SOC option NBD00003

Example of a MAP response:

```
Index Content CCRtype Acc CCRid CCC1/PVC1 [CCC2/PVC2]
[Sig] [Tag]    [Sin]     Agency
-----------------------------------------------------
1 PACKET PAIRED LINE DE 9059631003        19059631003
                          AGENCY1
2 VOICE PAIRED LINE SW 6135519970            6135519971
  Y    Y                  DEFAULT
3 PACKET PAIRED TRUNK  PT1X75OG 1 1PT1X75OG 12
                          AGENCY2
33 VOICE COMBINED LINE SW 6135510102
  N    Y                  AGENCY1
66 PACKET PAIRED TRUNK PACKETDATATRK    2 4095
PACKET DATATRK  3 3999  AGENCY3

CCR LIST DONE.
```

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>
```

where

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

MAP response:

```
CCR DISASSOC DONE.
```

Example input:

```
> ccr disassoc 10
```

8 Repeat step 7 for each CCR to be disassociated.

Deactivating SOC option NBD00003

9 Display a list of all associated CDCs by typing:

```
> cdc list assoc
```

Example of a MAP response:

```
Index Content CCRtype Acc CCRid CCC1/PVC1 [CCC2/PVC2]
[Sig] [Tag]    [Sin]     Agency
-----------------------------------------------------
1 PACKET PAIRED LINE DE 9059631003        19059631003
                          AGENCY1
2 VOICE PAIRED LINE SW 6135519970            6135519971
  Y    Y                  DEFAULT
3 PACKET PAIRED TRUNK  PT1X75OG 1 1PT1X75OG 12
                          AGENCY2
33 VOICE COMBINED LINE SW 6135510102
  N    Y                  AGENCY1
66 PACKET PAIRED TRUNK PACKETDATATRK    2 4095
PACKET DATATRK  3 3999  AGENCY3

CDC LIST DONE.
```

10 Note the surveillance identification number (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 (SIN) of the surveillance with which the CDC is associated

Example input:

```
> cdc disassoc sin1
```

MAP response:

```
CDC DISASSOC DONE.
```

12 Repeat step 11 for each CDC to be disassociated.

Deactivating SOC option NBD00003

13 Display a list of all surveillances by typing:

```
> surv list all
```

Example of a MAP response:

```
Subject       CaseID SIN MRP Clg_dlvry Inband_dlvry
(Feat_status Interval) (Surv_status Interval) PNI Agency
Status {Associated_CDC} {Associated_CCRs}
-----------------------------------------------------
LTID ISDN2 1  CASE1 SIN1 Y Y Y
              (N 15) (N 0) N AGENCY1
              ACTIVE {1} {8 6}
DN 6135520302 CASE2 SIN4 Y Y Y
              (N 15) (Y 60) N DEFAULT
              INACTIVE {1} {3}
SURV LIST DONE.
```

14 Note the surveillance identification number (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 (SIN) of the surveillance to be deleted

Example input:

```
> surv del sin1
```

MAP response:

```
SURV DEL DONE.
```

16 Repeat step 15 for each surveillance to be deleted.

17 Display a list of all CCRs by typing:

```
> ccr list all
```

Example of a MAP response:

Deactivating SOC option NBD00003

```
Index Content CCRtype Acc CCRid CCC1/PVC1 [CCC2/PVC2]
[Sig] [Tag]    [Sin]     Agency
-------------------------------------------------
1 PACKET PAIRED LINE DE 9059631003        19059631003
                          AGENCY1
2 VOICE PAIRED LINE SW 6135519970            6135519971
  Y    Y                  DEFAULT
3 PACKET PAIRED TRUNK  PT1X75OG 1 1PT1X75OG 12
                          AGENCY2
33 VOICE COMBINED LINE SW 6135510102
  N    Y                  AGENCY1
66 PACKET PAIRED TRUNK PACKETDATATRK    2 4095
PACKET DATATRK  3 3999  AGENCY3

CCR LIST DONE
```

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 input:

`> ccr del 1`

MAP response:

```
CCR DEL DONE.
```

20 Repeat step 19 for each CCR to be deleted.

21 Display a list of all CDCs by typing:

`> cdc list all`

Deactivating SOC option NBD00003

Example of a MAP response:

```
Index Type Access CDC DN     Agency
     [Associated SINs]
-----------------------------------------------------
    1  X.25 7 2   22222222        3 1 128 0
     SIN1 SIN2 SIN3 SIN8    AGENCY1
    2  X.25 6 2   22222222        3 1 128 0
     SIN4 SIN5 SIN6 SIN7    AGENCY2
CDC LIST DONE.
```

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

MAP response:

```
CDC DEL DONE.
```

Example input:

```
> cdc del 10
```

24 Repeat step 23 for each CDC to be deleted.

25 Access the SOC utility by typing:

```
> soc
```

MAP response:

```
SOC:
```

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

```
> assign state idle to nbd00003
```

Deactivating SOC option NBD00003

MAP response:

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

Confirm by typing:

```
> nanbd
```

MAP response:

```
Done.
```

If the RTU key code	Then go to
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
```

MAP response:

```
Done.
```

28 Exit the SOC utility by typing:

```
> quit
```

29 You have completed this procedure.

Appendix A: Surveillance checklists

Information required prior to surveillance setup

The following information must be agreed upon between the Law Enforcement Agency (LEA) and the service provider in order 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? (This information needs to be translated by the service provider in order to set up a proper USNBD surveillance.)
- Is call data delivery required? (For the proper X.25 link to be used, translation must be performed by the service provider to specify the proper CDC).
- Is call content delivery required?
  - — specify the delivery method (combined or paired)
  - — specify the number of CCRs associated with the surveillance
  - — specify the type of CCR (trunk or line, and if a line, whether or not signaling is required)
  - — bearer capability of the CCR (CCR's bearer capability must match the subject's bearer capability)
  - — for calls made within a Private Network?
- Is redirection monitoring to be provided?
- Is the calling party number to be delivered in CDC messages?

Switch provisioning considerations

Service providers should consider the following items:

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 purchase date of 31 March 2000. Currently, IOMs (NTFX4101) with their applicable card (NTFX30AA, NTFX31AA and NTFX34AA) must be purchased. See “Equipment for cable 1 connection” on page 10-5.

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. It has been determined through testing that under normal busy hour conditions, one 19.2 Kbps link can handle all CDC messages for the maximum 400 surveillances.

Facilities to LEAs

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

Checklist for each surveillance

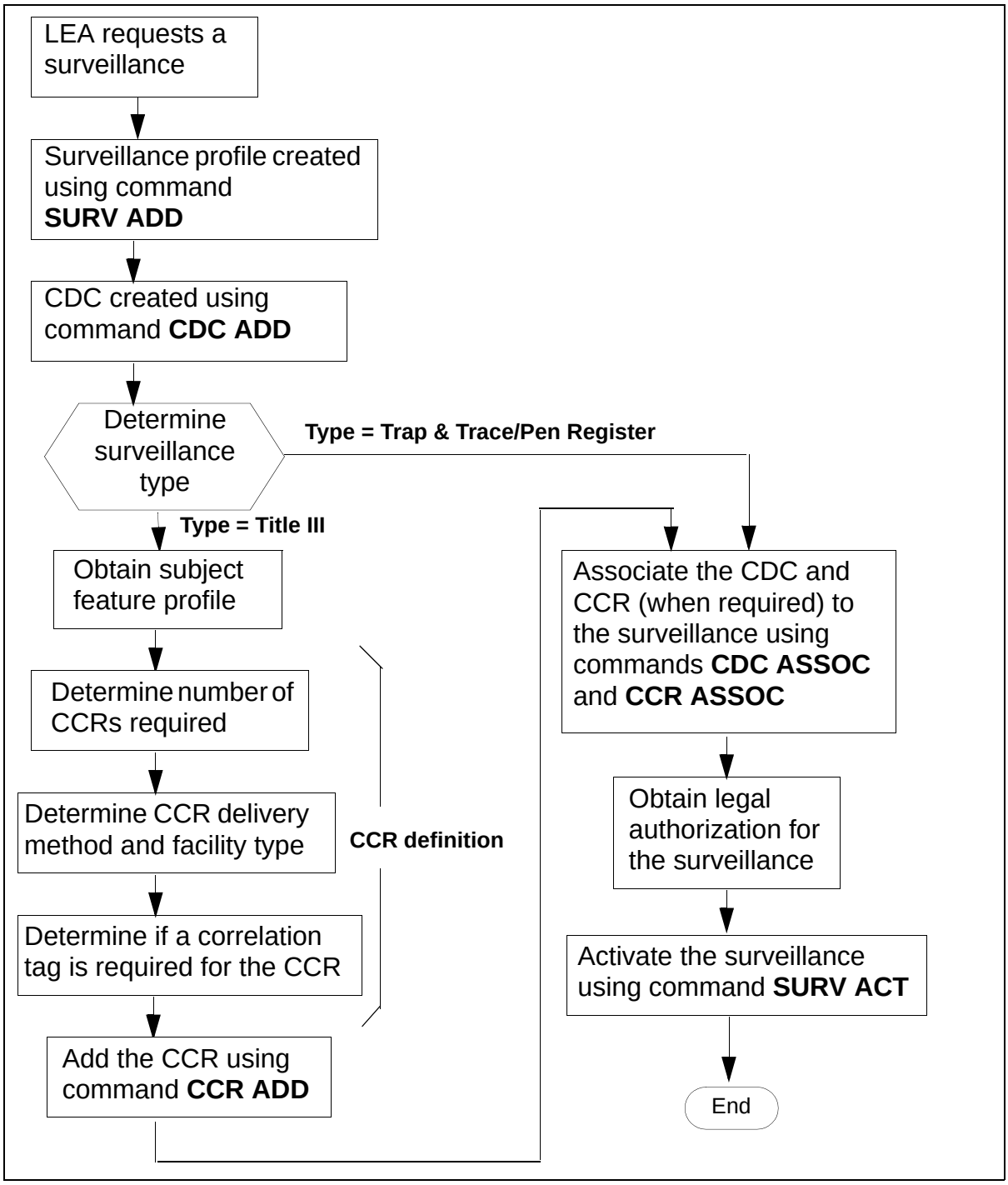
This checklist is intended as a tool to identify information required prior to setting up a surveillance, identify who will provide the information, and when applicable, specify where to find information in this document.

The following procedures must be repeated 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” on page 8-26)
- add a Call Data Channel (CDC) using the CDC ADD command (see “Creating a CDC” on page 8-21)
- add additional Call Content Resources (CCR) for a surveillance using the CCR ADD command (see “Creating CCRs” on page 8-15)
- associate a CDC with a specific surveillance using the CDC ASSOC command (see “Associating a CDC with a surveillance” on page 8-31)
- associate a CCR with a specific surveillance using the CCR ASSOC command (see “Associating a CCR with a surveillance” on page 8-36)
- activate a surveillance using the SURV ACT command (see “Activating a surveillance” on page 8-41)

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

Summary of Surveillance checklists



Step	Action

1 When a LEA requests a surveillance, the LEA must provide the Service Provider (SP) with the Directory Number (DN), surveillance type (Trap & Trace/Pen Register or Title III) and the 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 their line is a POTS subscriber and then orders a feature for their line, the line type can change from POTS to RES. If the subject then orders a residential feature for their line, this action will take down the surveillance. To re-activate the surveillance, the setup procedure must be performed again. A change in line type from RES to POTS will also take down an active surveillance.

3 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.

4 Identify the type of surveillance required.

If the surveillance type is	Then go to
Title III	step 5
Trap & Trace/Pen Register	step 10

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 call forward universal (CFU), call forward busy (CFB), call forward don't answer, (CFDA), universal 3-way calling (U3WC), or call transfer (CXR), then one additional CCR is required to increase the probability of delivering all call content.

Note: Beginning in NA012, call content is collected on CXR calls.

7 The LEA and SP determine the delivery method (combined or paired) and the facility type (line or trunk). The appropriate facility type is determined by call content collection box capabilities and the subject's use (for example, ISDN or high speed modems)

CCR definition - delivery method

Method	Equipment required for each CCR
paired	2 lines or 2 trunks
combined	1 conference circuit and 1 line

If the LEA requires the ability to decode ISDN Circuit Mode Data (CMD) which also requires non-signaling trunks, or high speed modems, paired delivery method must be used**.**

CCR definition - facility type

Facility type	Signaling option
loop start line ground start line	Y or N Y or N
trunks	N

In NA010, only loop start lines with signaling is available. Beginning with NA011, all other combinations are available**.**

8 Beginning with the NA011 load, the SP determines if the correlation tag is required. If it is, an additional DTMF sender card (NT3X68AB) may be required on the switch. See "Calculating the number of DTMF senders" on page 7-3.

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

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

11 The SP receives legal authorization for the surveillance.

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

Recommended CCR provisioning guidelines

The following CCR provisioning guidelines are suggested:

- each subject subscribing to analog line services (POTS, RES, or IBN) should be provisioned with a minimum of one CCR
- a minimum of two CCRs should be provisioned when the subject subscribes to a supported redirection feature (any call transfer or call forward variant) or conferencing features (universal 3-way calling (U3WC), Conf3, Conf6, or Call Joining)

  Note: The LEA may request more than two CCRs be provisioned in order to monitor simultaneously redirected calls.

- each subject subscribing to MDC electronic business set services should be associated with a minimum of two CCRs in order to ensure proper delivery of call content

  Note: The LEA may request more than two CCRs be provisioned in order to monitor simultaneously redirected calls.

- each subject subscribing to ISDN BRI services should be associated with a minimum of two CCRs to support the two active bearer channels the subject can access

  Note: The LEA may request more than two CCRs be provisioned in order to monitor simultaneously redirected calls.

- for subjects with a maximum bearer capacity of speech, either line or trunks CCRs can be provisioned
- for subjects subscribing to ISDN BRI services with a maximum bearer capacity of circuit mode data (CMD), non-signaling trunk CCRs should be provisioned with a paired delivery method

Typical trunk datafill for trunks used for CCRs

The following figures show typical trunk table datafill for trunks used as CCRs:

Typical datafill for table CLLI

```
 CLLI ADNUM TRKGRSIZ                                        ADMININF
-------------------------------------------------------------------
 NUTRK  315       24                                          NUTRK
```

Typical datafill for table TRKGRP

```
 GRPKEY
                                                           GRPINFO
 ----------------------------------------------------------------
 NUTRK
                            NU    0 NPDGP NCRT OG     64KDATA
```

Typical datafill for table TRKSGRP

```
          SGRPKEY CARDCODE
SGRPVAR
                                                           SGRPVAR
 ----------------------------------------------------------------
          NUTRK 0    DS1SIG          NOSIG
```

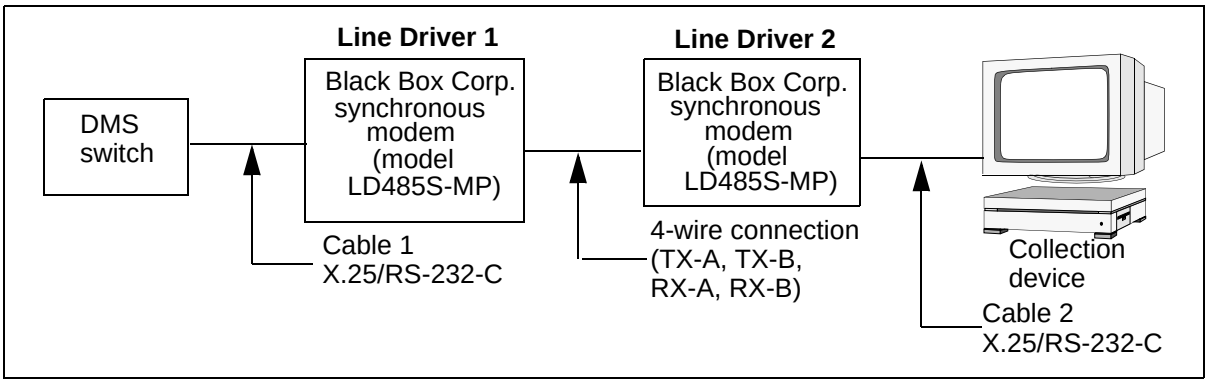
Typical datafill for table TRKMEM

```
      CLLI        EXTRKNM SGRP                            MEMVAR
-------------------------------------------------------------------
      NUTRK              1   0                 DTC  7 13   1
      .                    .                          .
      .                    .                          .
      .                    .                          .
      NUTRK1            12   0                 DTC  7 13 24
```

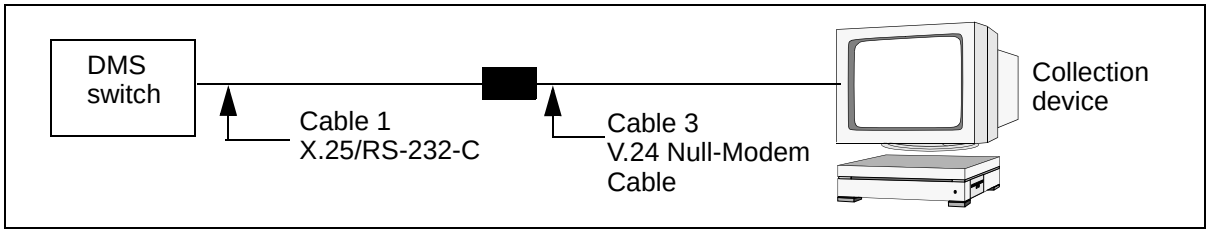
Appendix B: Sample USNBD X.25 connections

The following figures show a typical long distance USNBD X.25 connection configuration with modems, cables, and the DMS switch and collection device connections, and two typical direct connection configurations.

Typical USNBD X.25 long distance connection (Setup 1)



USNBD X.25 direct connection (Setup 2)



The following table lists the two switch and collection device node designations and the associated setup configuration.

Switch and collection device configuration

Switch end node designation	Collection device end node designation	Sample setup configuration recommended
DTE	DCE	Setup 1
DCE	DTE	Setup 2

The following table contains recommended DIP switch and jumper settings for each line driver.

Line driver (modem) jumper and DIP switch setting

Jumper or DIP switch	Description	Line Driver 1	Line Driver 2
W2	RTS/CTS Delay positions	Constant carrier	Constant carrier
S6	**Internal:** Line Driver generates transmit data clock and presents the clock to the attached DTE using pin 15. The DTE then presents synchronized data to the Line Driver using pin 2. **External:** Line Driver transmit data clock is presented to the DTE using pin 15, and is synchronized with timing of data received from the remote device. The DTE then presents synchronized data to the LIne Driver using pin 2. ***Note:*** To create a master clock, set one of the Line Drivers to internal or external clocking and the other Line Driver to recovered clock.	Recovered	Internal
W3	Half or full duplex operation	Full duplex	Full duplex
S4 and S5	Baud rate setting	19 200 bps	19 200 bps

The following table contains table MPCLINK sample datafill information for node setup 1.

Setup 1 table MPCLINK information

Field or subfield	Description	Enter value
LINKKEY	Link key contains:	
	MPCNO (Multiprotocol controller number)	28
	LINKNO (Link number)	2
LINKALM	Link alarm	Y
PROTOCOL	Link protocol data	X2584
LINKNABL	LInk enable	0
CONVNABL	Conversation enable	55
PARM	Parameter selector contains:	
	Number of 2-way switched virtual circuits (SVC)	SVCS2WAY
	NUMVCS (Number of virtual circuits)	100
	Level 2 packet window	L2WINDOW
	SIZE (Frame window size)	7
	Level 2 packet level modulo counter	L2MODULO
	MODVAL (Frame level modulo counter numbering)	MOD8
	Level 3 packet window	L3WINDOW
	SIZE (Frame window size)	2
	Level 3 packet level modulo counter	L3MODULO
	MODVAL (Frame level modulo counter numbering)	MOD8
	Node type or address of the MPC	NODETYPE
	NODE (Node type)	DTE
	Location of clock source	CLKSRCE
	SOURCE (Clock source)	EXTERNAL
	Level 3 data packet size	L3DATA
	DATASIZE ((level 3 data packet size)	P256
	End of parameter selector	$
EXINF	Example information protocol contains:	
	EXINFO (Example protocol information	SVCDNA
	DIGITS (digits for the network address)	00000911

Note: For the MAP display example associated with this setup arrangement, refer to the “USNBD Setup 1 MAP display example” on page 8-19.

The following table contains table MPCLINK sample datafill information for node setup 2.

Setup 2 table MPCLINK information

Field or subfield	Description	Enter value
LINKKEY	Link key contains:	
	MPCNO (Multiprotocol controller number)	28
	LINKNO (Link number)	3
LINKALM	Link alarm	Y
PROTOCOL	Link protocol data	X2584
LINKNABL	LInk enable	0
CONVNABL	Conversation enable	55
PARM	Parameter selector contains:	
	Number of 2-way switched virtual circuits (SVC)	SVCS2WAY
	NUMVCS (Number of virtual circuits)	100
	Level 2 packet window	L2WINDOW
	SIZE (Frame window size)	7
	Level 2 packet level modulo counter	L2MODULO
	MODVAL (Frame level modulo counter numbering)	MOD8
	Level 3 packet window	L3WINDOW
	SIZE (Frame window size)	2
	Level 3 packet level modulo counter	L3MODULO
	MODVAL (Frame level modulo counter numbering)	MOD8
	Node type or address of the MPC	NODETYPE
	NODE (Node type)	DCE
	Location of clock source	CLKSRCE
	SOURCE (Clock source)	EXTERNAL
	Level 3 data packet size	L3DATA
	DATASIZE ((level 3 data packet size)	P256
	End of parameter selector	$
EXINF	Example information protocol contains:	
	EXINFO (Example protocol information	SVCDNA
	DIGITS (digits for the network address)	10000911

Note: For the MAP display example associated with this setup arrangement, refer to the “USNBD Setup 2 MAP display example” on page 8-19.

Cable 1

The following table contains equipment product engineering codes (PEC) for cable connections associated with two typical DMS switch IOC shelves.

Equipment for cable 1 connection

DMS switch IOC shelf PEC code	IOC shelf card required	PEC code for cable between IOC connector and modem
NT1X61AD (34 pin connector)	NT1X89BA or NT1X89BB	NT0X26LY
NT1X61AG (2 x 20 pin connector)	NT1X89BA or NT1X89BB	NT0X96GS

The following table contains equipment product engineering codes (PEC) for cable connections associated with a DMS switch IOM shelf.

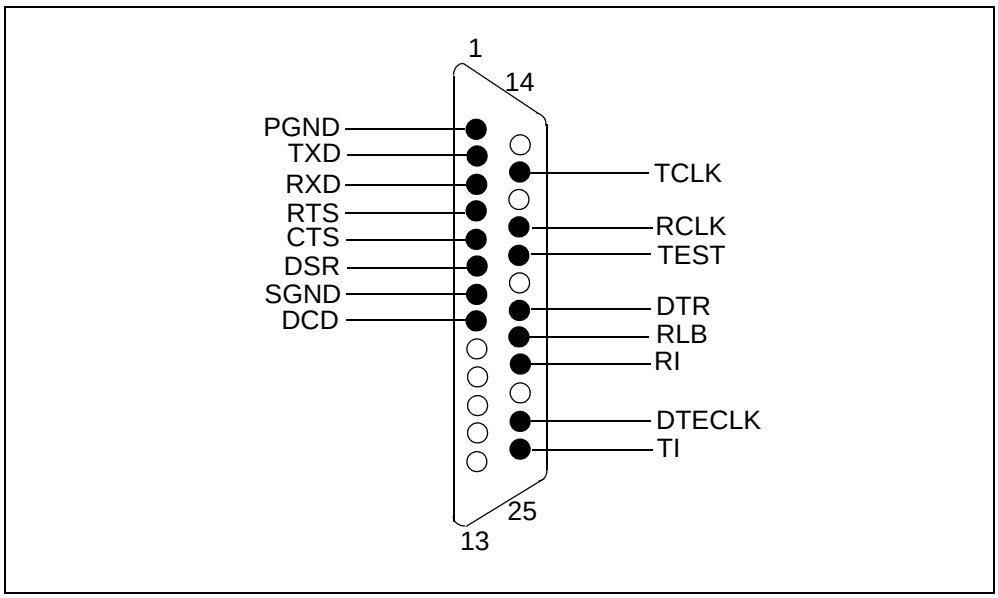
Equipment for cable 1 connection

DMS switch IOM shelf PEC code	IOM shelf cards required	PEC code for cable between IOM shelf connector and modem	PEC code for cable between IOM shelf connector and MS
NTFX4101	NTFX30AA controller card, NTFX31AA Paddle Board, P0749586 insertion guide, NTFX34AA MPC card	NT0X96LU (also require two NTFX34AA smart connectors per cable)	NT0X96KW

Cable 2

The connection between the Eicon card and the V.24 DCE is made using a standard V.24 cable (Eicon part number 300-007). Pin information and signal definitions are provided in the following figure and table.

Pin-out diagram of V.24 RS-232-C connector



Signal definitions for V.24 RS-232-C connector

Pin Number	Signal	Name	Direction	ITU number
1	PGND	Protective ground	Common	101
2	TXD	Transmit data	Output	103
3	RXD	Receive data	Input	104
4	RTS	Request to send	Output	105
5	CTS	Clear to send	Input	106
6	DSR	Data Set Ready	Input	107
7	SGND	Signal Ground	Common	102
8	DCD	Data Carrier Detect	Input	109
15	TCLK	Transmit Clock (DCE)	Input	114
17	RCLK	Receive Clock	Input	115

Signal definitions for V.24 RS-232-C connector (Continued)

18	TEST	Local Loopback Activation	Output	141
20	DTR	Data Terminal Ready	Output	108
21	RLB	Remote Loopback	Output	140
22	RI	Ring Indicator	Input	125
24	DTECLK	Transmit Clock (DTE)	Output	1113
25	TI	Transmit Indicator	Input	142

Cable 3

The connection between Cable 1 and the V.24 DCE is made using a Null-Modem connector. Pin information and signal definitions are provided in the following figure. The cable can be ordered from Eicon (part number 300-022).

Pin-out diagram of V.24 Null-Modem connector

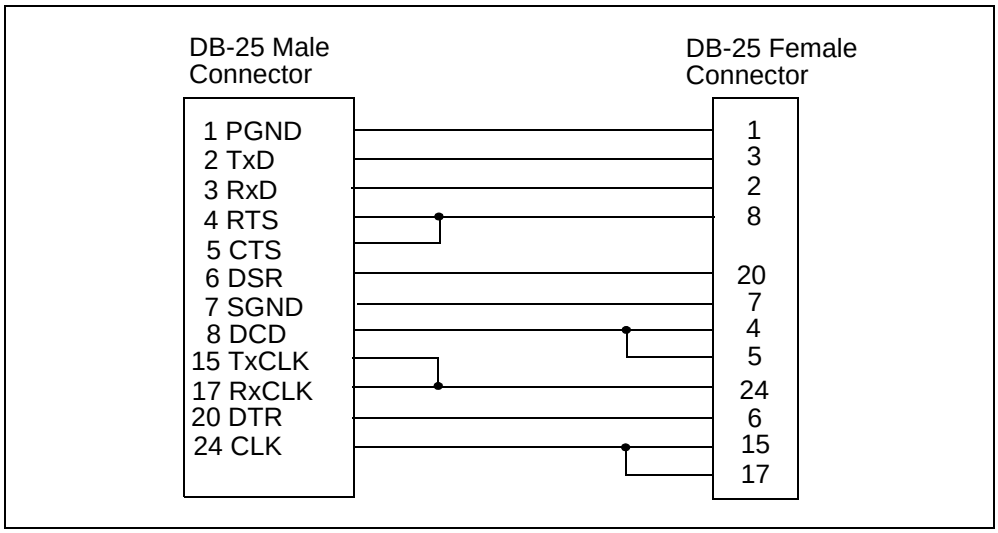


Table datafill sequence

The following table lists the data schema tables that require datafill to provide USNBD functionality. The tables are listed in the order in which they are to be datafilled.

Datafill tables required for USNBD

Table	Purpose of table
MPC	Table MPC contains the information necessary to implement a multiprotocol controller (MPC) on the DMS switch.
MPCLINK	Table MPCLINK specifies the link and protocol information for cards datafilled in table MPC.

Table MPC

Description

Table MPC contains values necessary to implement the multiprotocol controller (MPC) on the DMS switch. Table MPC identifies the MPC card hardware in the DMS computing module (CM), and requires one entry or tuple for each MPC.

Each entry contains:

- an index number for the MPC
- the number of the input/output controller (IOC) shelf where the card resides
- the card circuit number
- the product engineering code (PEC)
- the identification (ID) for the preferred download file to be used

Table MPC datafill sequence

Table IOC must be datafilled before table MPC.

Table MPC must be datafilled before table MPCLINK, which provides protocol support and link information for cards configured in table MPC.

Datafilling table MPC

The following table shows the datafill specific to USNBD for table MPC.

Datafilling table MPC

Field	Subfield	Entry	Explanation and action
MPCNO		see subfield	*Multiprotocol controller number* This field contains subfield K.
	K	0 to 255	*Multiprotocol controller number key* Enter the number of one multiprotocol controller (MPC). The MPC cards can be numbered as desired. There is no default value.
MPCIOC		0 to 19	*Multiprotocol controller input/output controller* Enter the number of the input/output (IOC) shelf on which the MPC card sits.

Datafilling table MPC (Continued)

Field	Subfield	Entry	Explanation and action
IOCCCT		0, 4, 8, 12, 16, 20, 24, 28, 32	*Input/output circuit number* Enter the slot position on the IOC shelf multiplied by 4, from 0 (zero) to 32. Entries outside this range are invalid. There is no default value.
EQ		1X89AA, 1X89BA, 1X89BB, FX30AA, FX30BA	*Equipment code* Enter the Nortel product engineering code (PEC): 1X89AA for the MPC card or 1X89BA/BB for the enhanced MPC (EMPC) card. Enter FX30AA or FX30BA if the IOC specified is an IOM. Entries outside this range are invalid. There is no default value.
DLDFILE		alphanumeric (8 characters)	*Download file* Enter a file name that begins with MPC, followed by X for X25ORIG, 0 (zero) for X2580, 4 for X.25, or A for asynchronous protocol software, followed by four alphanumeric characters designating the Telecom software release cycle and its load designation. For example, MPCX33AB. Software download files are interchangeable between MPC and EMPC. For IOM MPC, use default name IOM$LOAD. There is no default value. ***Note:*** For automatic location identification (ALI), the system enters data in field DLDFILE to specify the asynchronous protocol software download files for the current MPC load. The fourth character of the download filename is the letter A.

Datafill example for table MPC

The following example shows sample datafill for table MPC.

MAP display example for table MPC

```
MPCNO MPCIOC IOCCCT      EQ  DLDFILE
_____________________________________________

    0      0     12  1X89AA MPCX33AB
    1      1     12  1X89AA MPCX33AB
```

Table MPCLINK

Description

Table MPCLINK specifies link and protocol information for cards entered in table MPC. Table MPCLINK can be datafilled with any valid multiprotocol controller (MPC) link definition and protocol combination, followed by a group of protocol-specific fields.

Table MPCLINK supports the application of 1980 and 1984 ITU X.25 layered protocol and asynchronous communications in the MPC, as well as the previous X25ORIG (BX25) protocol. Protocol support ensures that links and conversations are established and maintained.

The fields in table MPCLINK identify the MPC data links to the computing module (CM) in the same way table MPC identifies the actual MPC hardware to the CM. These fields have no default values and must be datafilled.

Protocol parameter definitions are based on the protocol used. Most parameter fields do not require datafill. The only parameter fields that do require datafill are those that are adjusted from the default values assumed on the MPC card when it is downloaded. These fields contain timing and messaging specifications.

Users can enter a list of parameter entries and values. When you enter data in parameters at the MAP (maintenance and administration position), a prompt appears until a $ (dollar sign) is entered. Parameters that are not entered retain the default values used during download. Most of the fields in a tuple can be changed only when the affected link is in a busy state.

The MPC has a finite amount of buffer space. The data packet size determines the number of buffers normally dedicated to an activity on a single circuit. The default number of buffers is two. Requests for additional buffers are completed from a general buffer pool. This type of allocation indicates a single channel can use all remaining buffers.

Applications that output messages can receive an MPC return code when buffers are not available, invoking a 10-second CM delay before the block is sent to the MPC again. The system can take a list of parameter entries and their values out of service.

Certain parameters in table MPCLINK applying to the X.25 protocols must be datafilled to correspond to the circuit subscription for DATAPAC or the host data packet network (DPN).

The following parameters must match the circuit subscription:

- local data network address (DNA)

- number of permanent virtual circuits (PVC)
- number of switched virtual circuits (SVC)
- packet window size

Because these parameters must correspond exactly to subscription requirements, it is important to know the requirements of features that use the MPC. Users must understand the circuit subscriptions or the environment in which they operate, and configure cards and links in tables MPC and MPCLINK to conform the needs of higher-level applications.

Warning: If field PARM = L2WINDOW, field SIZE must be set to the same value at both the DTC and DCE ends of the data link. The same is also true for field PARM = L3WINDOW. If the field SIZE values are different at both ends of the data link, call processing errors, malfunctions, and lost revenue can occur.

Table MPCLINK datafill sequence

Table MPC must be datafilled before table MPCLINK.

Table size

0 to 512 tuples

Datafilling table MPCLINK

The following table shows the datafill specific to USNBD for table MPCLINK.

Datafilling table MPCLINK

Field	Subfield	Entry	Explanation and action
LINKKEY		see subfields	*Link key* This field contains subfields MPCNO and LINKNO.
	MPCNO	0 to 255	*Multiprotocol controller number* This field specifies the current multiprotocol controller (MPC) or enhanced multiprotocol controller (EMPC) card for this entry. Enter the MPC/EMPC number as entered in table MPC. There is no default value.

Datafilling table MPCLINK (Continued)

Field	Subfield	Entry	Explanation and action
	LINKNO	0 to 3	*Link number* Only logical links 2 or 3 can be specified, although a data link cable may be connected to MPC physical ports 1, 2, or 3. Physical ports 2 and 3 are low-speed RS232 ports (19.2K and below). Physical port 1 is a high-speed V.35 port (56/64K). If the data-link cable is connected to port 3, enter 3. If the data-link cable is connected to port 2, enter 2. There is no default value for this field.
LINKALM		Y or N	*Link alarm* Enter Y to enable the MPCLINK alarm for system busy (SYSB) MPC links. Otherwise, enter N. ***Note:*** If the field LINKALM is datafilled as N, no MPC908 (MPC link state transition) logs will be generated. For IOM MPC, the link is checked for any abnormal changes. If the change is abnormal, an MPC908 (MPC link state transition) log is generated. If the change is otherwise, an MPC908 log is not generated.
PRTCLDAT		see subfield	*Protocol data area* This field contains subfield PROTOCOL.
	PROTOCOL	ASYNC, X2580, X2584, or X25ORIG	*Link protocol data* The protocol choice must correspond to the download file specified in table MPC. Enter X2584 and datafill subfield LINKNABL and further refinements as specified below.

Datafilling table MPCLINK (Continued)

Field	Subfield	Entry	Explanation and action
			There is no default value for this subfield.
	LINKNABL	0 to 32767	*Link enable* Enter the time-out, in min, before a link that has failed to fully enable is system busied (SBSY) and returned to service (RTS). This value must be a multiple of 5. Enter 0 (zero) to disable the function. There is no default value for this subfield. ***Note:*** If the entry is non-zero, one link is enabled. When the other link reaches the timeout threshold, both the enabled link and the MPC card are SBSYed and RTSed. To prevent this occurrence, enter 0 to disable the function.

PROTOCOL = X2584

When the entry in subfield PROTOCOL is X2584, datafill subfields CONVNABL, PARMS, and EXINF as described below.

Field descriptions for conditional datafill

Field	Subfield	Entry	Explanation and action
	CONVNABL	0 to 32767	*Conversation enable* Enter the number of minutes a conversation is not in progress before correcting action occurs. This value must be a multiple of 5. An entry of 0 indicates a period of time is not specified. There is no default value for this subfield.
	PARMS	see subfield	*Parameter selector (ITU x 25 CC protocol* This field contains subfield PARM.

Field descriptions for conditional datafill (Continued)

Field	Subfield	Entry	Explanation and action
	PARM	SVCS2WAY, L2WINDOW, L2MODULO, L3WINDOW, L3MODULO, NODETYPE, CLKSRCE, and L3DATA	*Parameter selector* This field contains a vector of up to 37 parameter options.To change a parameter default value, enter the parameter option and an associated value. Enter parameters as a combination of the parameter name and value, one at a time, in any order. When fewer than 37 options are required, enter $ (dollar sign) to end the list. Enter SVCS2WAY (number of 2-way switched virtual circuits) (SVC) and datafill subfield NUMVCS. Enter L2WINDOW (frame window size) to specify the size of the frame window, and datafill subfield SIZE. ***Warning:*** Subfield SIZE must have the same value at both the DTC and DCE ends of the data link. Otherwise, call processing errors, malfunctions, and lost revenue can occur. Enter L2MODULO (frame level modulo counter) to specify a numbering scheme for end-to-end messaging at level 2 and datafill subfield MODVAL. Enter L3WINDOW (level 3 packet window) to specify the packet-level window size, and datafill subfield SIZE. ***Warning:*** Subfield SIZE must have the same value at both the DTC and DCE ends of the data link. Otherwise, call processing errors, malfunctions, and lost revenue can occur. Enter L3MODULO (level 3 packet level modulo counter) to specify a numbering scheme for end-to-end messaging at level 3 and datafill subfield MODVAL .

Field descriptions for conditional datafill (Continued)

Field	Subfield	Entry	Explanation and action
			Enter NODETYPE (node type or address) to specify the node type or address of the MPC and datafill subfield NODE. Enter CLKSRCE (clock source) to specify the source of the MPC system clock and datafill subfield SOURCE. Enter L3DATA (level 3 data packet size) to specify the maximum number of bytes of user data allowed in a data packet and datafill subfield DATASIZE.
	NUMVCS	0 to 255	*Number of virtual circuits* If the entry in field PARM is SVCS2WAY, enter the number of two-way SVCs configured on the link. If the total SVCs on a link is non-zero, enter SVCDNA in subfield EXINF80. You can configure a maximum of 255 SVCs, but the total number of PVCs and SVCs cannot exceed 255.
	SIZE	1 to 127	*Frame window size* If the entry in field PARM is L2WINDOW or L3WINDOW, datafill this subfield. Enter the size of the frame window. The frame window is the number of frames that level 2 and level 3 software send before the levels require confirmation that the first frame was received. A frame window of 7 is recommended, because it transmits data faster. In some cases, the end application cannot allow a frame window of 7. The digital terminal equipment (DTE) and the digital carrier equipment (DCE) must use the same value for this parameter. This field has a default value of 2.

Field descriptions for conditional datafill (Continued)

Field	Subfield	Entry	Explanation and action
	MODVAL	MOD8 or MOD128	*Frame level modulo counter* If the entry in field PARM is L2MODULO or L3MODULO, datafill this subfield. Enter a numbering scheme for end-to-end messaging at level 2 or level 3. Modulo 8 frame sequencing (MOD8) supports a maximum level 2 or level 3 window size of 7 (subfield SIZE set to 7). The default value is MOD8.
	NODE	DCE or DTE	*Node type or address* If the entry in field PARM is NODETYPE, datafill this subfield. Enter the node type or address of the MPC. Enter DCE for digital carrier equipment or DTE for data terminal equipment. This entry indicates to the MPC that frame addressing is DCE or DTE. The default value is DTE.
	SOURCE	INTERNAL or EXTERNAL	*Clock source* If the entry in field PARM is CLKSRCE, enter INTERNAL for the MPC card or EXTERNAL for a modem device. Link 2 and link 3 must have the same clock source (internal or external). If a different clock source is datafilled for link 2 and link 3, an error message is generated. The default value is EXTERNAL.
	DATASIZE	P16, P32, P64, P128, P256, P512, P1024, P2048, or P4096	*Level 3 data packet size* If the entry in field PARM is L3DATA, enter the maximum number of bytes of user data allowed in a data packet. The default value is P128.
EXINF		see subfield	*Example information protocol* This field contains subfield EXINFO.

Field descriptions for conditional datafill (Continued)

Field	Subfield	Entry	Explanation and action
	EXINFO	SVCDNA	*Example information protocol* Enter SVCDNA if SVCs are used on the link and datafill subfield DIGITS. If no SVCs are used, enter a $ (dollar sign).
	DIGITS	0 to 9 (vector of up to 15 entries)	*Digits* Enter the digits for the network address.

Datafill example for table MPCLINK

The following examples show sample datafill for table MPCLINK.

USNBD Setup 1 MAP display example

```
LINKKEY LINKALM
                                                          PRTCLDAT
_____________________________________________________________________

28 2      Y
X2584 0 55 (SVCS2WAY 100) (L2WINDOW 7) (L2MODULO MOD8) (L3WINDOW 2)
(L3MODULO MOD8) (NODETYPE DTE) (CLKSRCE EXTERNAL) (L3DATA P256) $
(SVCDNA 0000911) $
```

USNBD Setup 2 MAP display example

```
LINKKEY LINKALM
                                                          PRTCLDAT
_____________________________________________________________________

28 3     Y
X2584 0 55 (SVCS2WAY 100) (L2WINDOW 7) (L2MODULO MOD8) (L3WINDOW 2)
(L3MODULO MOD8) (NODETYPE DCE) (CLKSRCE EXTERNAL) (L3DATA P256) $
(SVCDNA 1000911) $
```

List of terms

Abandon

A call attempt that is released by the originating party after it has been routed, but before it is answered.

Agent

Switch representation of a physical facility, for example, a line or a trunk.

Associate

The party or parties with which the subject or the MRP is linked during a monitored call.

Basic rate access functional set (BRAFS)

An ISDN set that uses functional signaling. The Meridian M5317T is the Nortel Networks BRAFS.

Basic rate access multifrequency tone (BRAMFT)

An ISDN BRI line that uses extended stimulus signaling.

BRAFS

See Basic rate access functional set (BRAFS).

BRAMFT

See Basic rate access multifrequency tone (BRAMFT).

CALEA

Communications Assistance for Law Enforcement Act

Call

A call leg or a set of related call legs. *See also* Call leg.

Call content

Telephone conversation between the subject or MRP and one or more associates.

Call content channel (CCC)

Logical channel internal to USNBD software, which is represented by a directory number (DN) that corresponds to a physical facility on the subject's switch called a CCC circuit. A CCC circuit is an analog line.

Call content resource (CCR)

Set of one or two CCCs used to deliver call content to an LEA.

Call data channel (CDC)

Logical link between the subject switch and the LEA, which is used to deliver monitoring information.

Call-identifying information

Information about the call established using the subject's telephone service. *See also* Monitoring information.

Call leg

Link between two ports.

CCC

See Call content channel (CCC).

CCC circuit

Physical facility on the subject's switch, which is an analog line, used for CCCs.

CCC tag

Call ID for the terminating monitored call. Delivery of the CCC tag is optional and must be specified when a CCR is created. The CCC tag is delivered at the end of call content before C-tone is applied on the CCC circuit.

CCR

See Call content resource (CCR).

CDC

See Call data channel (CDC).

CDIAP

Call data intercept access point

CMR

CLASS modem resource card

C-Tone

Tone of the Dual Tone Multi-Frequency set, generated with the following parameters: frequency 1 at 1633Hz, and frequency 2 at 852Hz, both at -10dBm.

Digital Multiplex System (DMS)

A central office (CO) switching system in which all external signals are converted to digital data and stored in assigned time slots. Switching is performed by reassigning the original time slots.

Directory number (DN)

The full complement of digits required to designate an end user's station within one number plan area (NPA) - usually a three-digit central office code followed by a four-digit station number.

DMS

See Digital Multiplex System (DMS).

DN

See Directory number (DN).

DTMF

Dual tone multi-frequency digits

EMPC

See Enhanced multiprotocol controller (EMPC).

Enhanced multiprotocol controller (EMPC)

An enhanced data communications card that allows data communications between a DMS-100 Family switch and an external computer.

FSK

Frequency shift keying – a means of converting digital data to its analog equivalent.

IAP

Intercept access point

IDC

Inband Digit Collection

IOC

See Input/output controller.

Input/output controller (IOC)

An equipment shelf that provides an interface between I/O devices and the central message controller (CMC).

IOM

Input-Output Module; replacement shelf/unit for an IOC.

Law Enforcement Agency (LEA)

Government entity with the legal authority to conduct electronic surveillance.

LEA

See Law Enforcement Agency (LEA).

LEN

See Line equipment number (LEN).

Line equipment number (LEN)

A seven-digit functional reference that identifies line circuits (LC). The LEN provides physical location information on equipment such as site, frame number, unit number, line subgroup (shelf), and circuit pack.

Logical terminal identifier (LTID)

The unique identifier assigned to a logical terminal when it is datafilled in the ISDN access termination.

LTID

See Logical terminal identifier (LTID.)

MAP (maintenance administration position)

A group of components that provide a user interface between operating company personnel and the switch. The interface consists of a video display unit (VDU) and keyboard, a voice communications module, test facilities, and special furniture.

Monitoring information

Call-identifying information, which is information about the call established using the subject's telephone service, and non-call-identifying information, which is information that relates to the current status of the LEAs' monitored calls.

Monitored call

A call for which monitoring information, call content, or both are provided.

Monitored replacement party (MRP)

The party that replaces the subject in a monitored call. For example, when a monitored call is redirected by a call forwarding feature.

MPC

See Multiprotocol controller (MPC).

MRP

see Monitored replacement party (MRP).

Multiprotocol controller (MPC)

A general-purpose card that allows data communications between a DMS-100 Family switch and an external computer.

Non-call-identifying information

Information that relates to the current status of the LEAs' monitored calls. *See also* Monitoring information.

OM

See Operational measurements (OM).

Operational measurements (OM)

The hardware and software resources of the DMS-100 Family switches that control the collection and display of measurements taken on an operating system. The OM subsystem organizes the measurement data and manages its transfer to displays and records. The OM data is used for maintenance, traffic, accounting, and provisioning decisions.

PDC

Packet data channel that represent logical channels that are internal to USNBD.

SAI

See Surveillance administration interface (SAI).

SAS

See Surveillance administration system (SAS).

Service switching point (SSP)

A Common Channel Signaling 7 (CCS7) signaling node that interacts with the service control point (SCP) to implement special service code features.

SIN

See Surveillance identification number (SIN).

SSP

See Service Switching Point (SSP).

Surveillance administration interface (SAI)

Interface between the MAP SAS and the switch.

Surveillance administration system (SAS)

Maintenance and administration position (MAP) terminal used to interface with the switch.

Surveillance identification number (SIN)

A number that uniquely identifies a surveillance. The SIN is provided by the operating company.

Subject

Equipment, facilities, or services of an end user whose incoming, outgoing, and redirected communications is to be accessed and delivered to law enforcement agencies pursuant of a court order or lawful authorization.

Surveillance

Base provisioning unit used to monitor one subject with the information delivered to one LEA.

SVC

See Switched virtual circuit (SVC).

Switched virtual circuit (SVC)

A logical end-to-end connection for data communications made through a Data Packet Network (DPN). An SVC is established dynamically.

TSP

Telecommunication Service Provider

DMS-100 Family

North American DMS-100

US Network Broadcast Delivery (USNBD)
Feature Guide

© 1998 - 2004 Nortel Networks,
All rights reserved

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant. This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC rules, and the radio interference regulations of the Canadian Department of Communications. These limits are designed to provide protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Nortel Networks, the Nortel Networks corporate logo, the globemark design, and How the world shares ideas, DMS and MAP are trademarks of Nortel Networks Corporation.

Document number: 297-9801-300
Product Release: SN07
Document Release: Standard 07.01
Date: December 2004
Printed in the United States of America

NORTEL NETWORKS™

How the world shares ideas.