ISDN Primary Rate Interface Features Fundamentals — Book 3 of 3 Avaya Communication Server 1000

7.5
NN43001-569, 05.02
September 2011

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://www.avaya.com/support/. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: New in this release

The following sections detail what's new in this document for Avaya Communication Server 1000 Release 7.5:

Features

See the following section for information about feature changes:

SIP TAT

SIP trunk anti-tromboning (SIP TAT) feature releases the unused trunks optimizing DSP resources. For more information about SIP TAT see TAT and TRO-BA equipped on the same system on page 419

Other

Revision History

September 2011	Standard 05.02. This document is up-issued to support the removal of content for outdated features, hardware, and system types.
November 2010	Standard 05.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.5.
June 2010	Standard 04.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.0.
March 2010	Standard 03.03. This document is up-issued to support Communication Server 1000 Release 6.0. This document is up-issued to reflect changes in the section Network Message Services.

January 2010	Standard 03.02. This document is up-issued to support Communication Server 1000 Release 6.0. This document is up-issued to reflect changes in chapter Network Message Services.
May 2009	Standard 03.01. This document is up-issued to support Communication Server 1000 Release 6.0.
August 2008	Standard 02.06. This document is up-issued to reflect changes in technical content in the table "LD 86: Configure the MCDN Alternate Routing options".
December 2007	Standard 02.05. This document has been up-issued to support Communication Server Release 5.5.
July 2006	Standard 5.00. This document is up-issued to reflect changes in technical content: • Addition of Feature Packaging in the Network and Distinctive Ringing chapter. • Addition to Trunk Route Optimization chapter. • Addition of Table 137 to Engineering and Configuration Guidelines chapter.
August 2005	Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.
September 2004	Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.
October 2003	Standard 1.00. This document is a new technical document for Succession 3.0. It was created to support a restructuring of the Documentation Library, which resulted in the merging of multiple legacy technical documents. This new document consolidates information previously contained in the following legacy document, now retired: International ISDN Primary Rate Interface: Feature description and administration (553-2901-301)

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

- Getting technical documentation on page 21
- Getting product training on page 21
- Getting help from a distributor or reseller on page 21
- Getting technical support from the Avaya Web site on page 22

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Japan D70 nB+D

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

This feature provides nB+D ISDN Primary Rate connectivity between the system and the INS1500 D70 for Japan. The capability of a D-channel is expanded to support multiple PRIs (up to nine) in an nB+D configuration, where 1 ? n ? 215. This enhancement allows for non-facility associated D-channels, so that a PRI might consist of 24 B-channels. The D-channel controlling these B-channels can be shared with another PRI link. The bit rate is 1.5 Mb.

The nB+D enhancement adheres to current trunk assignment limitations on the number of trunks that can be assigned to an individual trunk group.

Operating parameters

For the ISDN layer 1 interface, the circuit pack QPC720 (Digital Trunk Interface) is used for the system to D70 connectivity.

The QPC757E version of the D-channel Handler (DCH) circuit pack provides the Layer 2 functions and incoming Layer 3 preprocessing for the system to D70 connectivity.

A Multi-purpose Serial Data Link (MSDL) can be used in place of the DCH circuit pack (NT6D80AA).

Feature interactions

PRI Channel Negotiation

When a D-channel has one or more secondary PRIs associated with it while using the D70 interface, channel negotiation requires that the PRI interface be explicitly defined for all B-channels not on the primary interface.

Japan D70 Connectivity

Interface Identifiers are required on all PRIs, including the primary PRI. This interface is used in channel negotiation.

Feature packaging

This feature requires the following packages:

- Digit Display (DDSP) package 19 for Calling Line Identification on ISDN PRI
- 1.5 Mbit Digital Trunk Interface (PBXI) package 75
- Integrated Services Digital Network (ISDN) package 145
- Primary Rate Access (PRA) package 146

- International Primary Rate Access (IPRA) package 202
- Multi-purpose Serial Data Link (MSDL) package 222 for use of the MSDL card in place of the DCH card

All of the software packages required for Japan D70 ISDN PRI connectivity are used to configure Japan D70 ISDN nB+D PRI with the addition of International nB+D (INDB) package 255.

Feature implementation

Table 1: LD 17: Configure nB+D for D70.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Configuration Record.
- ADAN	NEW DCH 0-63	Add a primary D-channel on logical port. For Large Systems.
- CTYP	aaaa	Card type.
- GRP	0-4	Network group number for Large Multi groups.
- DNUM	0-15	Device number; physical port for D-channel.
…		
- USER	PRI	D-channel mode.
…		
- IFC	D70	Interface type for Japan D70.
…		
- - DCHL	0-159 1-126	PRI loop number and interface identifier for the DCHI when IFC = D70.
…		
- PRI	0-159 1-126	Loop number and interface ID. Note that the interface ID range is larger when IFC=D70.
	<CR>	End definition of PRI loops.
- OTBF	1-(32)-127	Number of output request buffers.
- DRAT	(56K) 64KC 64KI	D-channel transmission.
…		

Prompt	Response	Description
- ADAN	NEW BDCH 0-63	Add a primary D-channel on logical port. For Large Systems.
…		
- PDCH	0-63	Primary D-channel.
…		
- CTYP	aaaa	Card type.
…		
- DNUM	0-15	Device number (physical port for the D-channel).
…		
- BCHL	0-159 1-126	PRI loop number and interface identifier for the DCHI when IFC=D70. For Large Systems.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 4: Japan TTC Common Channel Signaling

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

The Japan Telecommunication Technology Committee (JTTC) Common Channel Signaling is the Japanese version of the International Standard Organization (ISO) ISDN QSIG. It specifies the Layer 3 protocol signaling requirement for support of circuit switched call control at the "Q" reference point between a Private Integrated Services Digital Network (PISN) and a Private Telecommunication Network (PTN).

The JTTC Common Channel Signaling feature provides basic call service on the system ISDN 1.5 Mbit PRI on TTC connectivity. It also supports other supplementary services.

This feature supports the following call services on the Meridian 1 JTTC interface:

- Basic Call Service
- 64K Clear Bearer capability
- Calling Line Identification Presentation/Calling Line Identification Restriction (CLIP/CLIR)
- Channel Negotiation
- Enbloc Dialing
- User to User Information Element Transparent Transport
- TIE call types
- Traveling Class Mark (TCM) Transparent Transport

Operating parameters

Basic Rate Interface (BRI) is not supported on the JTTC interface.

Connected Line Identification Presentation/Restriction (COLP/COLR) is not defined to JTTC standard.

Backup D Channel, nB+D, Overlap Signaling (Overlap sending/Overlap receiving), Party Category, and Transit Counter are not supported on the JTTC interface.

ISDN QSIG Generic Functional Transport, Network Automatic Call Distribution (NACD), Network Call Trace (NCT), and Remote Virtual Queueing (RVQ) are not supported on the JTTC interface.

Only circuit mode connection is supported on the JTTC interface.

MCDN/JTTC gateway supports only Basic Call and CLIP/CLIR.

The Japan TTC Common Channel Signaling feature requires the following hardware for Large Systems:

- 1.5 Mbit Primary Rate Access (PRA) card (QPC720F or higher) for layer 1 interface
- 2.0 Mbit JDMI interface (Japan DTI2 QPC785 card) for ISDN Signaling Link (ISL) functionality
- Multi-purpose Serial Data Link (MSDL) card (NT6D80)
- Clock Controller (NTRB53)

- 1.5 Mbit Primary Rate Interface (PRI)/Digital Trunk Interface (DTI) card (NTAK09)
- Downloadable D-Channel Daughterboard (NTBK51)
- Clock Controller (NTAK20)

Feature interactions

Networking Features

Some networking features currently exist on more than one ISDN interface on the system. These features are listed in Table 2: Networking features that exist on more than one ISDN interface implemented on the system on page 29. The columns list the services and the rows list the interfaces.

Networking features that do not appear in Table 2: Networking features that exist on more than one ISDN interface implemented on the system on page 29 are only supported on one ISDN interface and are, therefore, rejected by all JTTC gateways when the service is requested. This is the case for all MCDN features that are not supported over the JTTC interface.

In Table 2: Networking features that exist on more than one ISDN interface implemented on the system on page 29 when a service is supported (Y), the information related to this service is accepted, decoded, and used according to the service description. When a service is not supported (N), the information related to this service is not sent to the interface. The request for the service is rejected according to the service rejection procedures. When a service is supported on two interfaces, a gateway function exists. This passes the information in order to support the service from one interface to the other.

Table 2: Networking features that exist on more than one ISDN interface implemented on the system

	JTTC	ETSI QSIG	ISO QSIG	Euro-ISDN	MCDN	ETSI BRI phones	Other BRI phones	Analog	D70
Calling Line ID/Calling Party Subaddress	Y	Y	Y	Y	Y	Y	Y	N	Y
Transit Counter	N	Y	N	N	Y	N	N	N	N
Call Charge	N	N	N	Y	N	N	N	Y	N

ISDN Signaling Link

The existing Integrated Signaling Link (ISL) operation is supported on the JTTC interface on the JDMI 2 Mbit interface only.

Only the first 23 TIE trunks of the JDMI loop are configurable for ISL operation.

Network Attendant Service

JTTC interacts with Network Attendant Service (NAS) as though the call is being sent to a route without NAS being equipped.

Network Call Redirection

The existing Network Call Redirection limitation on unsupported interfaces applies to the JTTC interface.

When a call is terminated on the system and Network Call Redirection is active, Japan TTC Common Channel Signaling can still operate. However, the original called number and the redirection number IEs that are used by the Network Call Redirection feature are not sent on the JTTC interface.

Network Calling Party Name Display

The Network Calling Party Name Display (NCPND) feature is supported within an MCDN network only. When the JTTC interface is involved in the call setup, the existing NCPND operation on unsupported interfaces applies to the JTTC interface also.

Network Message Service

Network Message Service (NMS) is supported within an MCDN network only. The NMS operation on the JTTC interface is the same as that of the existing treatment for unsupported interfaces.

Network Ring Again

Network Ring Again (NRAG) signaling is supported within a Meridian Customer Defined Network (MCDN) only. When a user requests NRAG on the JTTC interface, the request is rejected.

Trunk Route Optimization

Trunk Route Optimization (TRO) is supported within an MCDN network only. When a redirecting node sends a message to the originating node and the TRO request is accepted, the new call goes through the JTTC interface as a normal basic call. However, TRO signaling does not operate on the JTTC interface.

Virtual Network Services (VNS)

A JTTC link can be used as a B-Channel for Virtual Network Service (VNS) over a private network. All VNS services are supported normally. JTTC is used only as a speech bearer.

Feature packaging

Japan TTC Common Channel Signaling is Japan TTC (JTTC) package 335. The following packages are also required for JTTC:

- Japan Digital Multiplex Interface (JDMI) package 136 for ISL functionality
- Integrated Services Digital Network (ISDN) package 145
- Primary Rate Access (PRA) package 146
- International Primary Rate Access (IPRA) package 202
- Multi-purpose Serial Data Link (MSDL) package 222

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 3: LD 73: Define a new Digital Data Block (DDB) with a defined threshold. on page 32
2. Table 4: LD 17: Configure a digital loop number for Japan TTC. on page 32
3. Table 5: LD 17: Configure a new D-channel with Japan TTC Common Channel Signaling interface. on page 32

4. Table 6: LD 16: Configure Japan TTC interface. on page 33
5. Table 7: LD 14: Configure trunks for Japan TTC. on page 34

Table 3: LD 73: Define a new Digital Data Block (DDB) with a defined threshold.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	DDB	Digital Data Block.
- PREF	0-159	Primary Reference Source loop for Clock Controller. This prompt must be defined for the SLAV system only.
- - SREF	0-159 1-9	Secondary Reference (prompted only when PREF is not free-run). This prompt must be defined for the SLAV system only.
TRSH	0-15	Threshold set.

Table 4: LD 17: Configure a digital loop number for Japan TTC.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CEQU	Common Equipment parameters.
…		
- MODE	PRI	Primary Rate Interface mode.
- - TRSH	xx	Digital Trunk Interface threshold. The TRSH value must match the value defined in LD 73.

Table 5: LD 17: Configure a new D-channel with Japan TTC Common Channel Signaling interface.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	Action Device and Number.
ADAN	NEW DCH x	Create a new D-channel. x = 0 - 63
- CTYP	MSDL	Multi-purpose Serial Data Link card type. The MSDL card is the only card type that supports Japan TTC.
- GRP	0-4	Network Group number (Option 81C). Group numbers cannot be changed until the I/O devices associated with that group are disabled.
- DNUM	xx	Device number. All ports on the MSDL card share the same DNUM.

Prompt	Response	Description
- PORT	0-3	Port number on the MSDL card.
- USR	PRI ISLD	D Channel mode. Primary Rate Interface. Integrated Services Digital Link Dedicated.
- IFC	JTTC	Interface ID for Japan TTC.
- - ISDN_MCNT	60-(300)-350	Layer 3 call control message count per 5 second time interval.
- - ISLM	1-382	Integrated Services Signaling Link Maximum.
- -DCHL	x	PRI loop number for D-channel, as defined in LD 17.
…		
- BPS	xxxxx	Asynchronous baud rates (bits per second), where xxxxx is: 1200, 2400, 4800, 9600, 19200, 48000, 56000, 64000.
- SIDE	(USR) NET	system node type. Slave to the controller. Network, the controlling switch.
- RLS	23	Release ID of the switch at the far-end of the D-channel.

Table 6: LD 16: Configure Japan TTC interface.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
TKTP	TIE	TIE trunk type. Used for PBX-to-PBX interface.
DTRK	YES	Digital trunk route.
- DGTP	PRI	Digital trunk type.
ISDN	YES	Integrated Services Digital Network.
- MODE	PRA ISLD	Mode of operation. D-channel mode is Primary Rate Interface. D-channel mode is Integrated Services Digital Link Dedicated.

Prompt	Response	Description
- DCH	0-159	D channel number, as defined in LD 17.
…		
- IFC	JTTC	Interface for Japan TTC.
- - PNI	(0)-32700	Private Network Identifier. Must match far end PBX.

Table 7: LD 14: Configure trunks for Japan TTC.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	TIE	TIE trunk data block.
TN		Terminal Number
	l ch	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, ch = channel.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
SICA	(1)-16	Signaling category table number. The default is 16 if the loop type = JDMI.
RTMB		Route number and Member Number
	0-511 1-4000	Range for Large System, Media Gateway 1000B, and CS 1000E system.
TGAR	0 - (1) - 31	Trunk Group Access Restriction. The default value (1) automatically blocks direct access.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 5: Malicious Call Trace Enhancements

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Malicious Call Trace (MCT) allows users of selected phones to activate a call trace that results in a printed report of the calling and called parties. The report is generated on all system TTYs designated as maintenance (MTC) terminals.

The Malicious Call Trace feature has been enhanced to offer advanced capabilities across an ISDN PRI network, as explained in the following sections. For a description of the basic Malicious Call Trace feature, refer to *Avaya Features and Services Fundamentals, NN43001-106*.

Functional enhancements

The following enhancements add to the functionality of the basic Malicious Call Trace feature:

- For a call (from or to a Central Office on an analog CO or DID trunk), a special signal (hook flash and optional DTMF digit string) is sent to the Central Office if the option is configured.
- Alarm operation is maintained; however, the duration of the alarm is now flexible (0-15 minutes), instead of being fixed at 15 minutes.
- The malicious call can be recorded using a recording trunk, if provisioned.
- The call trace record can now be printed on any Serial Data Interface (SDI) port with MCT defined as a user.
- The flexible firmware flash can be transmitted on the EXUT and XFCOT cards. This functionality is used by the Enhanced Malicious Call Trace, Meridian 911, and Autodial Tandem Transfer features.
- The MCT feature can be activated from a proprietary phone during the established state of the call or during call clearing when interfaced with AXE10 Australia on 2 Mbit PRI trunks.

MCT record

Prior to this enhancement, during an established call, the user of a phone having Malicious Call Trace (MCT) Allowed Class of Service could invoke a call trace against the call. Activation of the feature resulted in the printing of a call trace record on the maintenance teletype terminal (TTY) of the system. The Malicious Call Trace record did not contain any identifier of whether the call was external or internal; the format of these records is changed to provide information about the type of call (internal or external).

Malicious Call Trace for Saudi Arabia

In Saudi Arabia, from a user's perspective, the Malicious Call Trace feature activation remains the same as it was prior to this enhancement. However, with this enhancement, the feature is now available for different types of analog and digital (CO, DID, and DOD) trunks. In order to send the MCT request, a special digit string is transmitted to the CO for an analog or digital trunk interface.

Malicious Call Trace for AXE-10 Australia

In Australia, MCT can be activated during the established state of the call when interfaced with AXE-10 Australia on 2.0 Mbit Primary Rate Interface (PRI) trunks. MCT can also be activated during the call clearing state of the call (within a maximum of 30 seconds from the caller going on hook). When MCT is activated, a special FACILITY message, with a keypad information element, is transmitted to the CO.

Trace Number (TRC) Key Lamp Status

The TRC key lamp status indicates the progress and success of the Malicious Call Trace request signaling to the CO and the availability of the recorder. The following are the lamp states:

Lamp Winking

Activation of the TRC key changes its lamp from dark to winking if the trunk involved in the call requires the signaling to be done. The lamp remains winking, indicating a transient state, until the call trace request signaling to the CO has been completed.

In a Meridian Customer Defined Network (MCDN) tandem scenario, the phone which originated the call trace remains winking until a Facility message is received from the node nearest to the Central Office. The user cannot invoke MCT again while the lamp is in the winking state.

Lamp Lit

If the call trace request to the CO is successful and the recorder is conferenced in the call, the lamp state is changed to lit.

In an MCDN tandem scenario, the lamp goes from winking to lit if a Facility message received from the node nearest to the CO indicates that the MCT request was successful. Activation of the TRC key during this state is ignored.

Lamp Flashing

This lamp state indicates that the call trace request to the CO was transmitted successfully, but a recorder could not be conferenced in. Activation of the TRC key during this state regenerates the MCT record, activates the alarm, and again attempts to conference in the recorder. The call trace request signaling to the Central Office is not transmitted again.

Lamp Dark

This lamp state indicates an idle TRC key or failure of the call trace request to the CO.

In an MCDN tandem scenario, the lamp goes from winking to dark if a Facility message received from the node nearest the CO indicates that the MCT request was unsuccessful.

Activation of the TRC during this state initiates all call trace elements again, including: transmission of trunk hook flash, conferencing a recorder (if one is not already hooked in), generating an MCT record, and activating an alarm.

Operating parameters

Any country using flexible firmware flash timing (60-1536 msec.) requires the Generic XFCOT cards NTCK16AE or NTCK16BE; or the EXUT card NT8D14BA. For any country not using either the Generic XFCOT card or the EXUT card, the same functionality is provided by software control.

The following hardware is required to activate this feature on Large Systems:

- Analog CO/FX/WATS QPC 525A
- DID trunk QPC449B LP TRK, QPC825
- 2.0 Mbit DTI interface QPC 536 B
- PRI2 interface NT8D72BA
- Digitone Receiver QPC574A, NT8D16AB
- TDS QPC609D, NTAK03AA
- Recorded phone trunk QPC71
- Conference card QPC444A
- MSDL card NT6D80AA

Feature interactions

For feature interactions pertaining to the basic Malicious Call Trace feature, refer to *Avaya Features and Services Fundamentals, NN43001-106*.

Malicious Call Trace Enhancements

ACD Emergency Key (EMR)

The Malicious Call Trace feature operates in a similar manner to the ACD Emergency key feature when conferencing a recording. In this enhancement, the ACD phone can activate both the Malicious Call Trace and ACD EMR features.

Autodial Tandem Transfer

The Trunk Hook Flash functionality is used by Autodial Tandem Transfer and Enhanced Malicious Call Trace.

Centrex Switchhook Flash

Interaction with the Centrex Switchhook Flash results because the flash range is changed for this feature. Communication to the CO (trunk hook flash) is performed by using the Centrex Switchhook Flash feature base code. The enhanced range is available for the Centrex Switchhook Flash.

Called Party Control (CDPC) Option

Prior to this feature, the CDPC option was not supported for conference calls. This has changed; the CDPC option is now supported if the conference contains exactly one recording trunk, one MCT activating party, and one other trunk. This is done to make the recorder transparent to the user. The CDPC option remains unsupported for all other conference calls.

Malicious Call Trace Idle Signal

The existing operation of the Malicious Call Trace Idle Signal feature is unchanged.

MCT DN/TN Print

If the option MCDC (in LD 15) is set, a second line is added in the MCT reports to show the DN of both parties of the call. If CLID is available it is printed in the second line.

M911

The Trunk Hook Flash functionality is used by M911 and Enhanced Malicious Call Trace.

Feature packaging

Enhanced Malicious Call Trace is packaged under the existing Malicious Call Trace (MCT) package 107.

For ISDN environments, ISDN packages are required based on the node and network interface applicable to the specific country. In addition, International Supplementary ISDN Features (ISDN INTL SUPP) package 161 is required.

In order to send an MCT message request to a tandem node, Network Attendant Service (NAS) package 159 must be equipped.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 8: LD 10: Enable MCTA for an analog (500/2500-type) phone. on page 41
2. Table 9: LD 11: Enable MCTA for a digital proprietary phone. on page 41

   To activate Malicious call Trace from a Meridian 1 Proprietary Phone, Class of Service MCTA, and TRC KEY should be defined. However, the same function can be achieved using a transfer or conference key and the SPRE + 83 or the MCT FFC.
3. Table 10: LD 17: Define the TTY as an MCT port. on page 41

   In order to print the MCT record on a dedicated MCT TTY port, USER type MCT must be defined.
4. Table 11: LD 16: Program the recorder route. on page 42
5. Table 12: LD 14: Program the recorder trunk. on page 42
6. Table 13: LD 15: Program the recorder and alarm options. on page 42
7. Table 14: LD 16: Enable the alarm for external calls. on page 43
8. Table 15: LD 57: Program Malicious Call Trace Feature codes. on page 43

   In order to activate malicious call trace from the analog (500/2500-type) phone without using the SPRE and 83, the MCT FFC must be defined.
9. Table 16: LD 16: Configure the flash timer range for the CO. on page 44

   For analog and 2.0 Mbit digital trunks, the flash range to be sent to the Central Office is configured using the FLH timer. In order to send the string to the Central Office, MCCD must be defined.
10. Table 17: LD 14: Set the WTM prompt to YES. on page 44

    The WTM prompt is provided for EXUT and XCOT cards. This prompt should be set to YES if firmware timing is to be done for the flash and the card supports this functionality. If the prompt is set to YES for one unit, it is also set to YES for all other units.

11. Table 18: LD 73: Define the DTI2 flash time range. on page 45
12. Table 19: LD 16: Setup MCTM timer and tandem delay (2 Mbit PRI for AXE-10 Australia only). on page 45

Table 8: LD 10: Enable MCTA for an analog (500/2500-type) phone.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	500	Phone type.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
CLS	(MCTD) MCTA	Malicious Call Trace is allowed if class is MCTA.

Table 9: LD 11: Enable MCTA for a digital proprietary phone.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	a...a	Telephone type. Type ? for a list of possible responses.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
CLS	(MCTD) MCTA	Malicious Call Trace is allowed if class is MCTA.

Table 10: LD 17: Define the TTY as an MCT port.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Type of data block.
ADAN	xxx TTY yy	xxx = new or change. yy = port number 0-63 (for Large Systems)
USR	MCT	Dedicated TTY port for MCT record.

Table 11: LD 16: Program the recorder route.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
TKTP	RCD	Recorder trunk data block.
ACOD	xxxx	Recorder route access code.

Table 12: LD 14: Program the recorder trunk.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RCD	Recorder trunk.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
RTMB		Route number and Member Number
	0-511 1-4000	Range for Large System, Media Gateway 1000B, and CS 1000E system.

Table 13: LD 15: Program the recorder and alarm options.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	FTR	Features and options data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		

Prompt	Response	Description
- ALDN	xxxxxxx	DN for the alarm.
- ALRM	(NO) YES	The ALRM prompt appears only if ALDN is defined. ALRM has to be set to YES if the alarm is to be rung for any call (external or internal) when MCT is activated.
- TIME	0-(15)	Time is prompted only if ALRM is set to YES. Time for the alarm is set in one-minute increments from 1 to 15.
- INT	(NO) YES	INT is prompted only if ALRM is set to YES. In addition, INT must be YES if the alarm is to be rung when MCT is activated against internal calls.
- RECD	(NO) YES	If the user wants the recorder, set RECD to YES. This prompt does not appear when a new customer is being defined.
- - MCRT	xx	The user has to use the recorder route number defined in LD 16. It will only be prompted if the RECD is set to YES.

Table 14: LD 16: Enable the alarm for external calls.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
TKTP	DID COT	Direct Inward Dialing Trunk. Central Office Trunk.
ALRM	(NO) YES	Malicious Call Trace is allowed for external calls when the response is YES.

Table 15: LD 57: Program Malicious Call Trace Feature codes.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	FFC	Flexible Feature Code.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
CODE	MTRC	Malicious Call Trace.
- MTRC	xxxx	Flexible Feature Code for Malicious Call Trace.

Table 16: LD 16: Configure the flash timer range for the CO.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
RCLS	(EXT) INT	Class marked route as (external) or internal.
...		
CNTL	YES	Changes control or timers.
- TIMR	FLH <space> 60-(510)-1536	Flash timer in msec. The range of the Centrex switch hook flash timer is 60-(510)-1536. The FLH value is rounded down to the nearest 10 msec. tick. If the value entered is 128 or 129, then it is set to 130 msec. *Software controlled flash* 60-127 msec. Digit 1 will be sent. (Not applicable to XFCOT card. It is applicable to XUT card.) 128-1536 msec. software controlled switch hook flash. (Applicable to both XUT and XFCOT cards.) *Firmware controlled flash* The user can enter any value from 60 to 1536 msec. 90 msec. is the hardcoded firmware flash for an XFCOT pack; the craftsperson should enter 90 msec. **Note:** the FWTM prompt must be set to YES for the trunk associated with this route in LD 14, if firmware timing is to be used.
...		
MCTS	(NO) YES	Enter YES to get the new prompts
- MCCD	0-8 digits	The call trace request string can be 0-8 digits in length. Valid digits are 0-9, *, and #.
- MCDT	(0)-4	Digit string delay is in seconds, in increments of one second.

Table 17: LD 14: Set the WTM prompt to YES.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	DID COT	Direct Inward Dialing Trunk. Central Office Trunk.
TN		Terminal number

Prompt	Response	Description
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
XTRK	EXUT XCOT	Enhanced Extended Universal Trunk. Extended Central Office trunk card.
FWTM	(NO) YES	Firmware timing for the trunk hook flash is available. This prompt is set to YES if firmware timing for trunk hook flash is supported by the pack.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
RTMB		Route number and Member Number
	0-511 1-4000	Range for Large System, Media Gateway 1000B, and CS 1000E system.

Table 18: LD 73: Define the DTI2 flash time range.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	DTI2	2.0 Mbit Digital Trunk Interface
FEAT	ABCD	Digital signaling category.
SICA	2-16	SICA table number.
...		
FALT (R)	ABCD N	Fault (DTI out-of-service). If Fault is not required.
P RRC (S)	ABCD	Register recall signal activated by MCT.
TIME	10-(100)-630	Time of RRC(S) signal in milliseconds. This is the flash duration used for 2.0 Mbit DTI trunks. It is programmable in one-millisecond increments from 10 to 630.

Table 19: LD 16: Setup MCTM timer and tandem delay (2 Mbit PRI for AXE-10 Australia only).

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.

Prompt	Response	Description
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
MCTS	(NO) YES	Malicious Call Trace Signal.
- MCTM	(0) - 30	Malicious call trace timer (in seconds).
- MTND	(NO) YES	Malicious Call Trace disconnect delay for tandem calls for AXE10 Australia.

Feature operation

To activate Malicious Call Trace from an analog (500/2500-type) phone dial SPRE + two-digit access code (83) or the MCT FFC.

Chapter 6: MCDN Alternate Routing

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Meridian Customer Defined Network (MCDN) Alternate Routing feature provides a solution to calls encountering congestion due to high traffic situations within an MCDN network. The MCDN Alternate Routing feature is supported over an MCDN-based ISDN protocol.

The MCDN Alternate Routing feature uses the routing capability of Network Alternate Route Selection (NARS) to re-route a congested call. For each MCDN call translated at a system node, NARS selects one route from up to 512 routes to complete the call. These routes are programmed in a route list. Each route in the list is called an entry. There can be up to 64 entries in each route list. Any combination of trunks can be specified in a route list.

The MCDN Alternate Routing feature can be configured for each of the 512 different routes.

Congestion occurs when channels within the network are not available. With the introduction of the MCDN Alternate Routing feature, each entry of a route list on one node can be configured to take an alternate entry (route) from the route list of that node (Private Exchange or Central Office), if congestion is encountered.

Alternate routing configuration takes place in LD 86, the Electronic Switched Network (ESN) administration overlay. The option defined for the Step Back On Congestion (SBOC) prompt determines the type of alternate routing available to calls over a particular route.

Alternate routing options are:

- NRR: no alternate routing is performed. The call receives congestion treatment.
- RRO: re-route at the originating node if a call encounters congestion. If congestion is encountered at a transit node, the call drops back to the preceding node, so that the preceding node decides if re-routing is required.
- RRA: re-route the call at any node, whether originating or transit node, when congestion is encountered.

The MCDN Alternate Routing feature is triggered at the controlling node when a Call Clearing message (DISCONNECT or RELEASE COMPLETE) is received, and the cause value in the Call Clearing message is supported for the MCDN Alternate Routing feature.

The cause values which activate the MCDN Alternate Routing feature are:

- Cause 3 = No route to destination
- Cause 27 = Destination is out of service
- Cause 34 = No channel/circuit available
- Cause 38 = Network out of order
- Cause 41 = Temporary failure
- Cause 42 = Congestion

Note:

To ensure that MCDN Alternate Routing occurs for all nodes in a system, define all nodes as SBOC = RRA. Conversely, to prevent MCDN Alternate Routing from occurring on any nodes, define all nodes as SBOC = NRR.

Refer to Originating node operation on page 49, Transit node operation on page 50, and MCDN Alternate Routing examples on page 51 for more information on MCDN Alternate Routing operation for each SBOC prompt.

Note:

If any of the cause values listed below are received in a Call Clearing message, the non-MCDN Alternate Routing retry operation occurs. That is, an attempt is made to retry the call. The retry first attempts to find another idle channel in the same route. If all the channels in that route are busy, it attempts to find another channel in the next alternate route in the Route List Block.

Cause values received in a Call Clearing message in order for the non-MCDN Alternate Routing retry operation to occur:

- Cause 6 = Channel unacceptable
- Cause 44 = Requested circuit/channel not available
- Cause 82 = Identified channel does not exist

  Refer to Originating node operation on page 49, Originating node operation. If Node C sends one of the non-MCDN Alternate Routing cause values, the Call Clearing message is sent back to Node A which attempts non-MCDN Alternate Routing.

Refer to Figure 2: Transit node RRA operation on page 51, Transit node operation. If Node C receives one of the non-MCDN Alternate Routing cause values:

- Node C attempts to find an alternate route but none is available.
- Node B is a transit note and does not attempt to find an alternate route.
- Node A attempts to find an alternate route but none is available.

Originating node operation

Consider the following calling scenario for an originating node operation. An attempt is being made to establish a call over an MCDN link, from originating node A to terminating node D, through transit nodes B and C. Congestion occurs between nodes C and D.

Whether node C is defined as SBOC = RRA or RRO or NRR, the congestion message, along with a MCDN Alternate Routing feature cause value, is always sent back to node B.

At node B, the SBOC option is checked to determine the routing treatment if:

- Node B is defined as SBOC = NRR, the Call Clearing message is sent back to the preceding node A.
- Node B is defined as SBOC = RRO, the Call Clearing message is sent back to node A because A is the originating node.
- Node B is defined as SBOC = RRA, an attempt is made to find an available alternate route until all of the alternate routes, as defined in the Route List (the RLB prompt in LD 86) are tried. If no alternate route is available, the congestion message information is sent from node B to the preceding node A.

In the originating node operation, node A must be defined as SBOC = RRA or RRO to perform MCDN alternate routing from node A to E to D.

Figure 1: Originating node operation on page 50 illustrates an originating node operation. With congestion between nodes C and D, the Call Clearing message is sent from node C to B. Because node B is defined as SBOC = RRO or NRR, the Call Clearing message is sent back to node A. With node A defined as RRA or RRO, an attempt is made to find an available alternate route.

The first available alternate route is found between nodes A and E. Node E can either be a Private Exchange or Central Office. The Network Class of Service access checks are passed, the direct leg between the congested node, C, is released, and an alternate route is created from node A through node E. The call is then rerouted from nodes A and E to the terminating node, D.

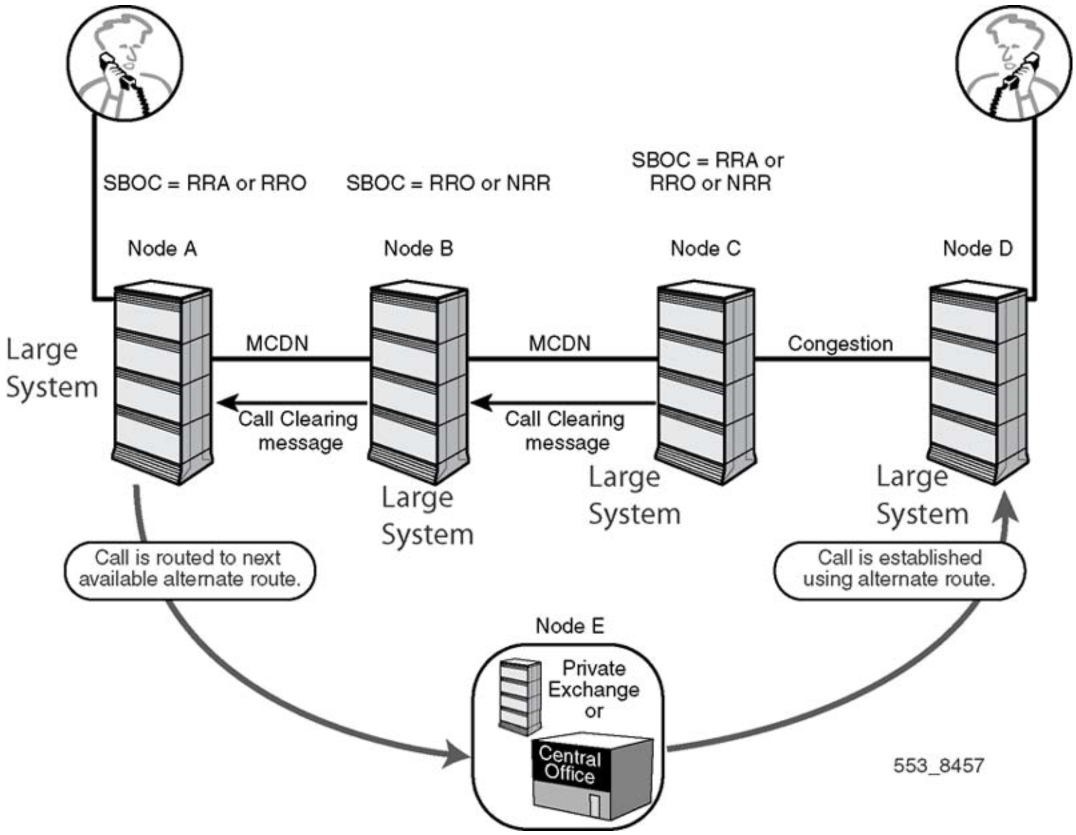

Figure 1: Originating node operation

Transit node operation

Consider the following calling scenario for a transit node operation. An attempt is being made to establish a call over an MCDN link, from originating node A to terminating node D, through transit nodes B and C. Congestion occurs between nodes C and D.

Whether node C is defined as SBOC = RRA or RRO or NRR, the congestion message, along with a MCDN Alternate Routing feature cause value, is always sent back to node B.

At node B, the SBOC option is checked to determine the routing treatment if:

- Node B is defined as SBOC = NRR, no rerouting occurs; the Call Clearing message is sent back to the preceding node, A.
- Node B is defined as SBOC = RRO, the Call Clearing message is sent back to the preceding node, A, because node B is not the originating node.
- Node B is defined as SBOC = RRA, an attempt is made to find an available alternate route until all of the alternate routes, as defined by Route List (the RLB prompt in LD 86) are tried.

Figure 2: Transit node RRA operation on page 51 illustrates a transit node operation with node B defined as SBOC = RRA. The first available alternate route is found between nodes B

and E. Node E can either be a Private Exchange or Central Office. The Network Class of Service access checks are passed, the direct leg between the congested node (node D) is released, and an alternate route is created from node B through node E to the terminating node D.

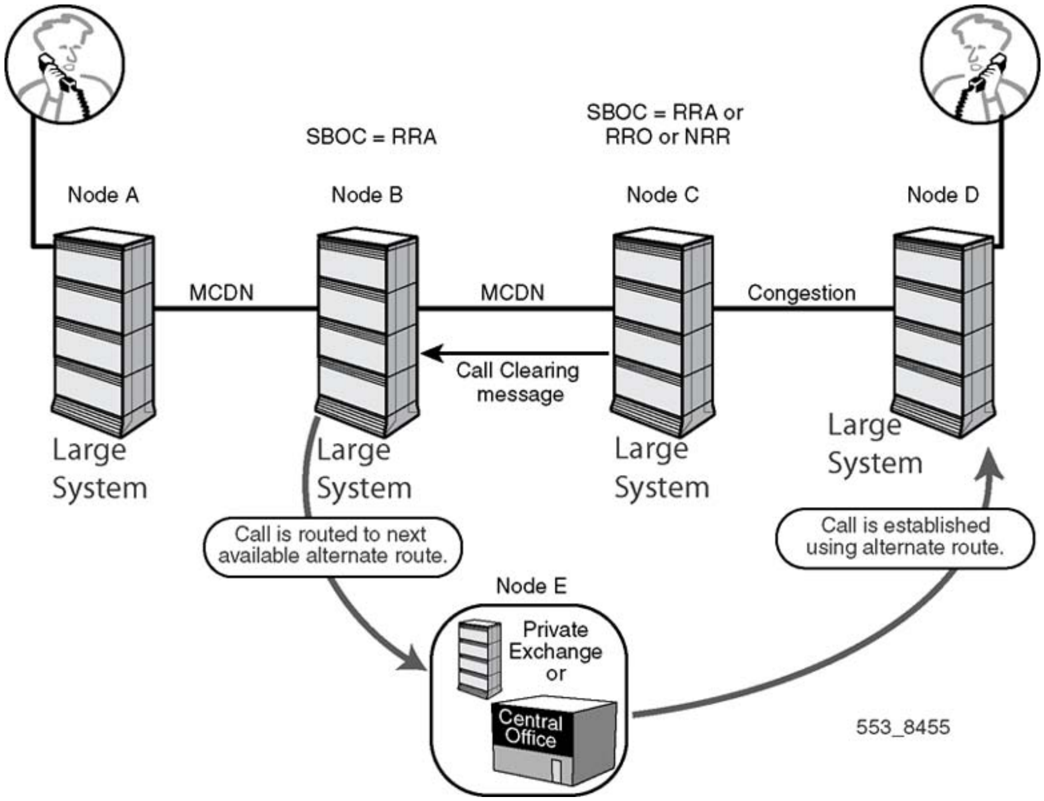

Figure 2: Transit node RRA operation

MCDN Alternate Routing examples

Example 1: System networked with Passport

In this scenario (refer to Figure 3: Example of System with Passport network on page 52), node A attempts to call node B using a primary route through Passport. The primary route is congested. Passport sends the cause value in the Call Clearing message to node A. With node A defined as SBOC = RRA or RRO, the cause value triggers a retry to make the call through the next alternate route. Alternate route 1 is from node A to node B through nodes C and D. If alternate route 1 is unavailable, then an attempt is made to route the call through alternate route 2: node A to node B through the Public Network.

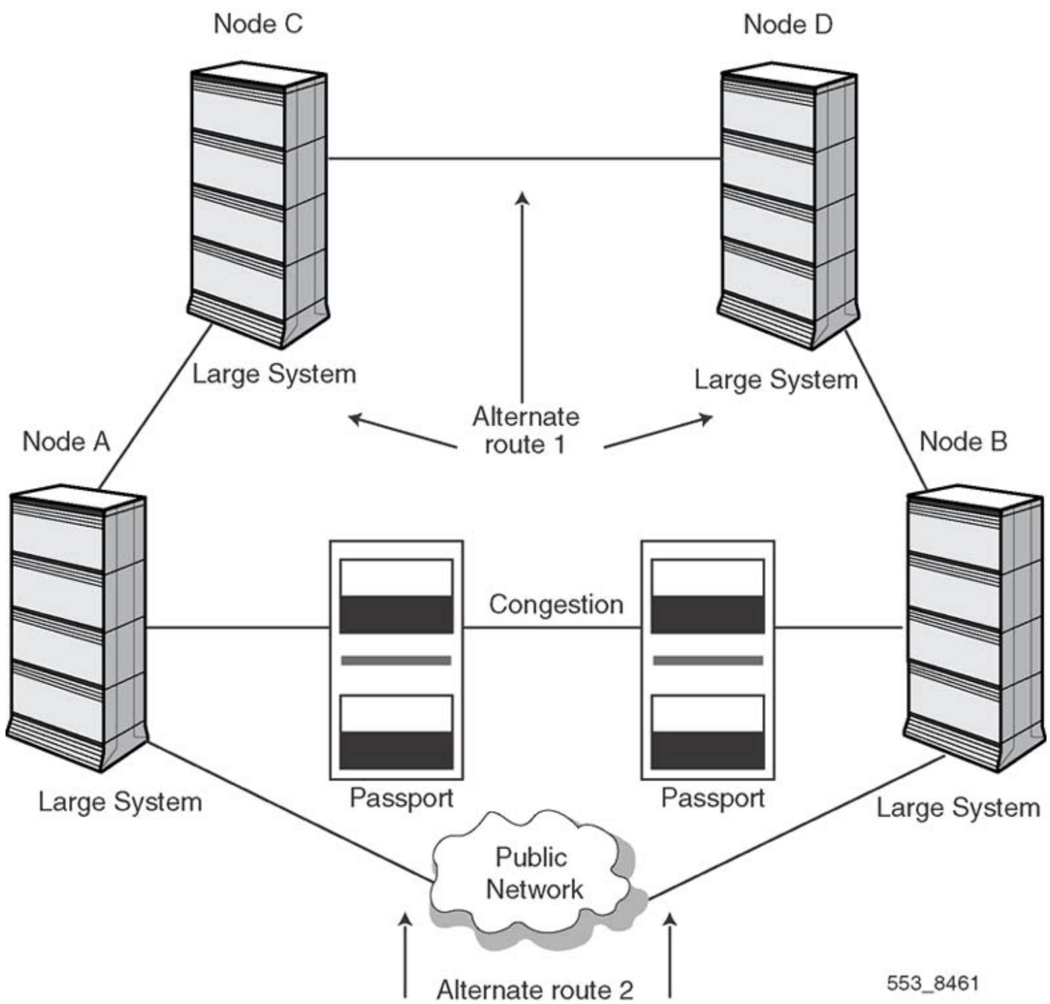

Figure 3: Example of System with Passport network

Example 2: Multi node network

Consider a scenario (refer to Figure 4: Example of multi node network on page 53) where a call is made from node A to node E through nodes B, C, and D. If there is congestion between nodes D and E, the Call Clearing message is sent from node D to node C:

- If node C is defined as SBOC = RRA, an attempt is made to find an alternate route. An alternate route is found from node C through node X to node E.
- If node C is defined as SBOC = RRO or NRR, the Call Clearing message is sent back to node B. Whether node B is defined as SBOC = NRR or RRO or RRA, the Call Clearing message is sent back to node A. Whether node A is defined as SBOC = RRA or SBOC = RRO, an attempt is made to find an alternate route. Alternate routes in this case are either from node A through node X to node E or from node A to node E through the Public Network.

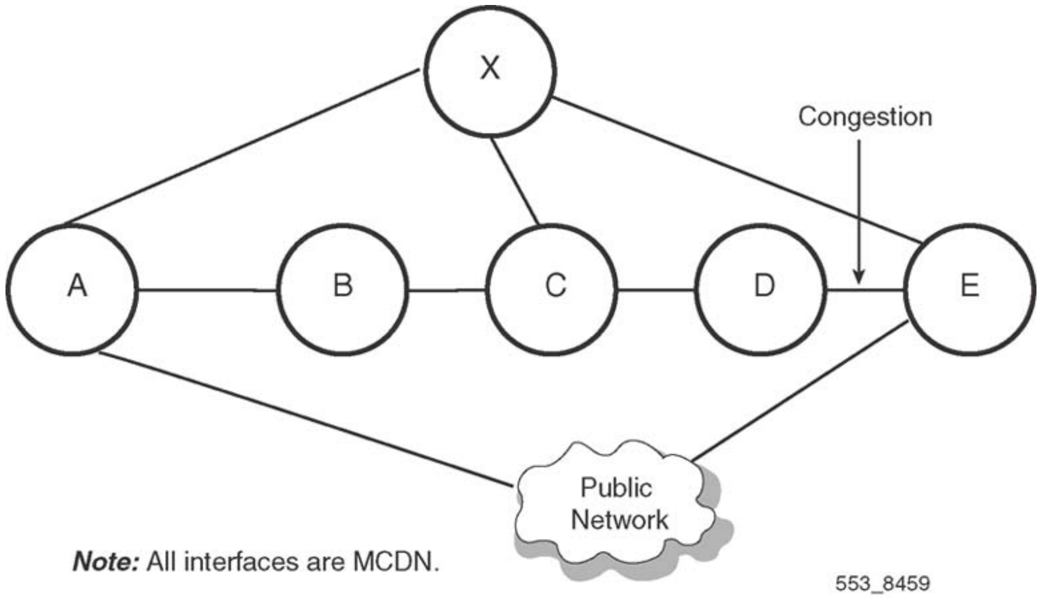

Figure 4: Example of multi node network

Example 3: Tandem call with non-ISDN originating node

This scenario (refer to Figure 5: Example of a tandem call with non-ISDN originating node on page 54) shows a tandem call with a non-ISDN originating node. When a call is made from node A to node D, the call is routed through nodes B and C. Congestion is encountered between nodes C and D.

Whether node C is defined as SBOC = RRA or RRO or NRR, the Call Clearing message is always sent back to node B.

- If node B is defined as SBOC = RRA, an attempt is made to find an alternate route. The alternate route through node X or through the Public Network to terminating node D is used to route the call.
- If node B is defined as SBOC = RRO or NRR, no alternate routing is attempted because the link between nodes B and A is non-ISDN. The call is cleared according to non-MCDN Alternate Routing operations.

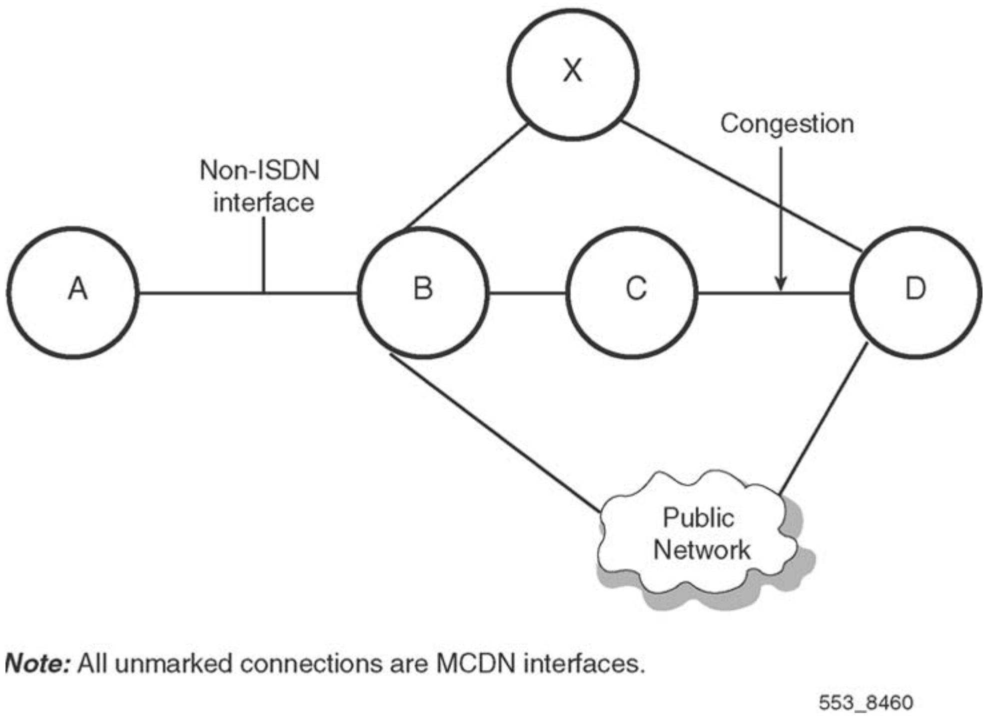

Figure 5: Example of a tandem call with non-ISDN originating node

Operating parameters

Route Access codes are not supported for MCDN Alternate Routing. The Coordinated Dialing Plan (CDP) or the Uniform Dialing Plan (UDP) is required for MCDN Alternate Routing, but not both. If UDP is used, Network Alternate Route Selection (NARS) or Basic Alternate Route Selection (BARS) must be provisioned.

The MCDN Alternate Routing feature does not support MCDN ISDN BRI trunks.

Feature interactions

Automatic Least Cost Routing

When a Call Clearing message is received, the MCDN Alternate Routing feature attempts a retry through the next alternative route, whether the alternative route is an Initial Set (ISET) or an Extend Set (ESET) route.

Drop Back Busy

If both the MCDN Alternate Routing feature and Drop Back Busy feature are configured in the same MCDN network, the MCDN Alternate Routing feature takes precedence.

Expensive Route Warning Tone

The Expensive Route Warning Tone is provided at the originating node when the MCDN Alternate Routing attempts to re-route the call through an expensive route. The Expensive Route Warning Tone is not provided when re-route to an expensive route occurs at a transit node.

Intercept treatment

The intercept treatment for network blocking is not applied at the transit node if the MCDN Alternate Routing feature is active at the transit node. The call is dropped back with the appropriate congestion IE information.

If the MCDN Alternate Routing feature fails to find an alternate route for a call encountering congestion at a transit node, intercept treatment is not applied at the transit node. The call is dropped back to the originating node with the appropriate congestion IE information.

Integrated Services Access

The MCDN Alternate Routing feature is supported for MCDN Integrated Services Access (ISA) routes.

ISDN Signaling Link

The MCDN Alternate Routing feature is supported for MCDN D-Channel ISDN Signaling Link (ISL) routes.

Network Attendant Service

The Network Attendant Service (NAS) feature operation is transparent to the MCDN Alternate Routing. The NAS drop back function takes priority over the MCDN Alternate Routing drop back function.

Off-Hook Queuing

Off-Hook Queuing (OHQ) takes precedence over the MCDN Alternate Routing feature. At the node where congestion is first encountered, if all outgoing routes are busy, the call is cleared back immediately to the preceding node only if there are no queuing features at this node.

The MCDN Alternate Routing feature comes into operation only at the preceding node when a Call Clearing message is received. OHQ waits until the busy route becomes available. If this route does not become available before OHQ times out, a Call Clearing message is sent.

Overlap Signaling

The MCDN Alternate Routing feature is supported over both the enbloc and overlap signaling methods.

Remote Virtual Queuing

The MCDN Alternate Routing feature takes precedence over Remote Virtual Queuing (RVQ) when congestion is encountered at the tandem node: an attempt is made to find an alternative route instead of informing the call originator to activate Ring Again Allowed.

Trunk Barring

If trunk barring prevents any trunk to trunk connection at the tandem node, the MCDN Alternate Routing feature retries on the next available route in the Route List Index (RLI).

Vacant Number Routing

Vacant Number Routing (VNR) is a default route used for routing untranslatable, invalid or unassigned dialed numbers (DN). IP networks usually contain only a subset of the numbers that can be used to reach them. An enterprise network rarely has sufficient data to route calls based on prefixes. Therefore, calls to the IP network need to be able to reroute to alternate routes, while maintaining the ability to receive vacant number treatment when the called destination is an unassigned number. The main purpose of the VNR enhancement feature is to provide appropriate call clearing treatment for 'vacant number' calls over IP domain.

This feature combines the functionality of VNR and Meridian Customer Defined Network Alternate Routing (MALT) for calls routed over IP, to route the call to the correct destination and provide appropriate vacant number treatment.

This feature also allows the user to configure predefined cause values to perform MALT, using Element Manager. The feature interacts with the Element Manager to determine whether to provide MALT for a particular cause. EM provides ten causes to perform MALT for VNR calls. For more information about configuring MALT VNR, see *Avaya Element Manager System Reference - Administration, NN43001-632* and *Avaya IP Peer Networking Installation and Commissioning, NN43001-313*.

The MALT and VNR on IP feature uses Call to Vacant Number (CTVN) to provide treatment for the VNR call, but does not change any of the CTVN functionality.

There are no specific requirements for upgrade. However, when a system is downgraded from 7.0, ensure that the lower release systems have the correct patches to build reason header when interacting with higher releases.

MALT on calls routed by VNR to the IP domain

When a call is routed by Vacant Number Routing (VNR) to the IP network, the user can perform MCDN Alternate Routing (MALT) for an additional ten causes, along with the existing six causes. These extra MALT causes can be configured in Element Manager. If the call is determined to be a VNR call, which is tried at least once to route over an IP route, then vacant number treatment is provided to the call.

When a call fails to route to the destination over H.323/SIP (for example, with reason "No entry present in the NRS/SPS" or due to rejection from the destination side), the call disconnects with a cause, which matches one of the original MALT cause codes, or disconnects with an indication to “use MALT”. Based on this information, MALT is performed at the Call Server to retry the call using an alternate route.

If MALT exhausts all routes in the VNR route list block (RLB) identified by the then the Route List Index (RLI), or an intermediate entry to a TDM route fails with a cause code other than the original MALT cause codes, then the treatment corresponding to the disconnect cause is provided. If the call clearing message has the cause ‘Unassigned Number’ or ‘Invalid Number format’ in all the accessed entries of the VNR RLI, then vacant number treatment is provided.

If any of the accessed entries clear the call with a cause other than Unassigned Number or Invalid number format, and the last entry cleared the call as an Unassigned Number, then the treatment corresponding to the previous cause is provided. Vacant number treatment is not provided to that call.

If MALT fails at an intermediate entry in the RLB (which is indexed by the RLI) then the alternate routing may end abruptly. For a non IP route, only the six MALT cause codes are used. For non QSIG or non MCDN routes, alternate routing is not triggered.

Note:

MALT is performed in the CS when there is an IP FEATURE IE with MALT indication in the call clearing message, irrespective of the call type (VNR/non VNR). This feature is limited to VNR calls over IP, originating from a CS 1000.

Configurable MALT causes for different vendors IP gateways

Element Manager allows different vendors (subdivided into “All Avaya Component” and “Third Party”) to configure ten causes (in addition to the existing six MALT causes) to perform MALT at CS 1000.

If a call is disconnected prior to establishing, and the call clearing message uses one of the ten causes on the Signaling Server to perform MALT, then a new IP Information Element (IE) is built with an indication “use MALT” with the cause in the received clearing message. This IE is sent to the Call Server with the 'Disconnect' message, and it triggers MALT for the particular cause.

In Element Manager, the 'Unassigned Number' cause is selected by default to perform MALT for Avaya and third party vendors.

The feature does not introduce any new configuration changes in CS. Table 20: Parameters added for MALT causes configuration on page 58 details the ten parameters added to support VNR and MALT configuration for Avaya and third party vendors.

Table 20: Parameters added for MALT causes configuration

Parameter	EM Description	Default value	Range
01 - UnassignedNumber	Unassigned number	1	0 and 1
20 - SubscriberAbsent	Subscriber absent	0	0 and 1
47 - ResourcesUnavailable	Resources unavailable	0	0 and 1
51 - CallRejected	Call rejected	0	0 and 1
52 - OutgoingCallBarred	Outgoing call barred	0	0 and 1
53 - OutgoingCallBarredCUG	Outgoing call barred CUG	0	0 and 1
54 - IncomingCallBarred	Incoming call barred	0	0 and 1
55 - IncomingCallBarredCUG	Incoming call barred CUG	0	0 and 1
63 - ServiceOrOptionNotAvailable	Service or option not available	0	0 and 1
127 - InternetworkingUnspecified	Internetworking unspecified	0	0 and 1

For more information about configuring MALT VNR, see *Avaya Element Manager System Reference - Administration, NN43001-632*

Limitations

The feature is supported only for IP routes (H323/SIP).

The feature supports only PRI/PRI2/ISL over TDM SL1 interface as a fall back route/first route. Other interfaces such as QSIG, EURO, DPNSS, and ANALOG are not considered a part of this feature.

The CS 1000 uses MCDN between the CS and SS and therefore as the TDM to IP protocol; it does not use QSIG.

The feature is supported only with Element Manager on Linux.

At present, Overlap Signaling is not supported in CS 1000 for SIP, so the cause code 484 is not generated by the NRS for the SIP redirect server or SPS.

Feature implementation

Task summary list: The following is a summary of the tasks in this section:

- Table 21: LD 15: Configure Vacant Number Routing on IP on page 59
- Table 22: LD 15: Configure Call to Vacant Number on page 59
- Table 23: LD 86: Configure MALT on page 59

Table 21: LD 15: Configure Vacant Number Routing on IP

Prompt	Response	Description
FNP	YES	Enable FNP
VNR	YES	Enable VNR
NET_DATA		
RLI	RRA/RRB/ NRR	SBOC configurations

Table 22: LD 15: Configure Call to Vacant Number

Prompt	Response	Description
INT_DATA	RAN	RAN route number

There is no code change in CTVN to give RAN treatment for the 'Unassigned number/Invalid number format' causes, as this functionality already exists.

Table 23: LD 86: Configure MALT

Prompt	Response	Description
SBOC	RRA RRO NRR	RRA: Reroute for all MALT cause values in the current node RRO: Reroute at the originating node NRR: No reroute

For more information on VNR configuration, see *Avaya IP Peer Networking Installation and Commissioning, NN43001-313*.

Virtual Network Services

The MCDN Alternate Routing feature can function over all MCDN-based bearer interfaces supporting Virtual Network Services (VNS).

Feature packaging

This feature requires the following packages:

- Basic Routing (BRTE) package 14
- Network Class of Service (NCOS) package 32
- Coordinated Dialing Plan (CDP) package 59, or Uniform Dialing Plan (UDP)
- UDP requires either Network Alternate Route Selection (NARS) package 58, or Basic Alternate Route Selection (BARS) package 57
- Digital Trunk Interface (DTI) package 75
- ISDN Signaling (ISDN) package 145
- 1.5 Mbit Primary Rate Access (PRA) package 146, or 2.0 Mbit Primary Rate Interface (PRI2) package 154, or International Primary Rate Interface (IPRA) package 202, or ISDN Signaling Link Interface (ISL) package 147

Feature implementation

Note:
To ensure that MCDN Alternate Routing occurs for all nodes in a system, define all nodes as SBOC = RRA. Conversely, to prevent MCDN Alternate Routing from occurring on any nodes, define all nodes as SBOC = NRR.

Table 24: LD 86: Configure the MCDN Alternate Routing options.

Prompt	Response	Description
REQ	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	RLB	Configure the Route List as a feature.

Prompt	Response	Description
RLI	xxx	Route List Index to be accessed. xxx = 1-127 if a Coordinated Dialing Plan or Basic Alternate Route Selection is used. xxx = 1-255 if Network Alternate Route Selection is configured. xxx = 0-999 if the Flexible Numbering Plan is configured.
ENTR	0-63	Entry number for the NARS or BARS route list.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
SBOC		Step Back On Congestion option. (NRR) = No re-routing
	RRO	Re-route at the originating node if congestion is encountered. If congestion is encountered at a transit node, drop back to the preceding node so that the preceding node determines if re-routing is needed.
	RRA	Re-route at any node, originating or transit (tandem), when congestion is encountered.
..		
ISET	(0)-64	Initial Set. Number of entries in Initial Set for route list block.
NALT	1-(5)-10	Number of MCDN Alternate Routing attempts (MALT retries only). Prompt appears once per RLI.
MFRL	(MIN) 0-7	Set Maximum Facility Restriction Level used to determine autocode prompting. Use default of MiN to set to the minimum FRL value.

Note:

The NALT prompt is introduced to limit the number of MALT retries. The retries include only those that are retried as a result of MALT Feature invoked. MALT retry count will be incremented only for such retries. The retries performed as a result of disabled routes or busy routes do not form a part of MALT Retry. For Example, if the retry to ENTRY 2 is performed because the route in ENTRY 1 is either busy or disabled, then this retry is not considered as MALT retry and MALT retry count will not be incremented for such attempts.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 7: MCDN End to End Transparency

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Meridian Customer Defined Network (MCDN) services are based on propriety specific Integrated Services Digital Network (ISDN) signaling. The MCDN End to End Transparency (MEET) feature conveys MCDN proprietary services on a standardized interface, ISDN QSIG. The QSIG gateway supports MCDN features both in a QSIG network and a mixed MCDN/QSIG network. It is the MCDN QSIG conversion tool which provides the basis for support of the selected MCDN applications such as Network Attendant Service (NAS), Network Automatic Call Distribution (NACD), and Network Message Service (NMS). MEET supports the following features:

- MCDN to QSIG encapsulation conversion tool
- NAS using the QSIG transport
- NACD using the QSIG transport
- Network Message Service - Message Center (NMS-MC) and Network Message Service - Meridian Mail (NMS-MM) using the QSIG transport

All three MCDN applications, NAS, NACD, and NMS, are supported over the ISDN Primary Rate Interface (PRI) or the ISDN Basic Rate Interface (BRI) using the QSIG generic functional protocol (transport).Figure 6: MCDN End-to-End Transparency on page 64 illustrates the MEET feature.

Note:
ISDN BRI trunk access is not supported in North America.

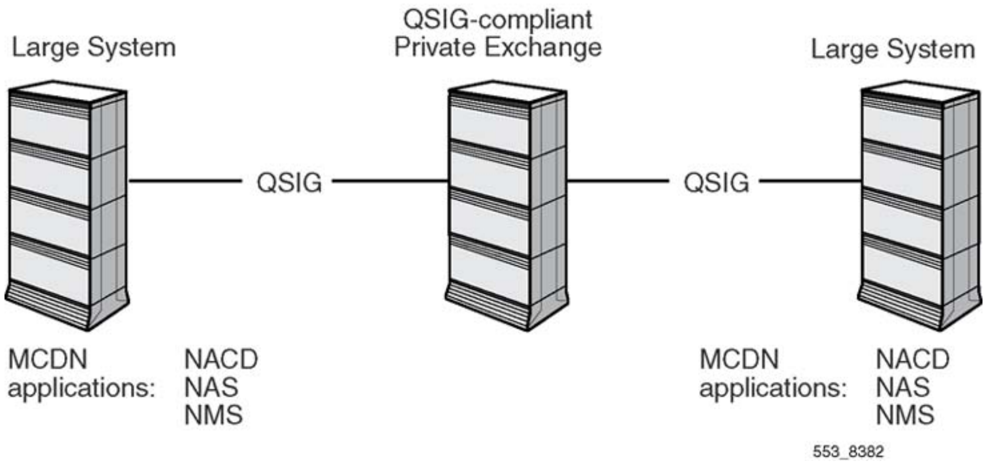

Figure 6: MCDN End-to-End Transparency

NAS using the QSIG transport

The MEET feature supports NAS on the ISDN Primary Rate Interface (PRI) or the ISDN Basic Rate Interface (BRI) using the QSIG transport. The following NAS functions are available on QSIG:

- NAS Routing
- ISDN Call Connection Limitations
- Incoming Call Indication
- Attendant Break-In
- NAS Anti-Tromboning
- Call Extension
- Timed Reminder Recall
- Camp-On
- Call Waiting

For further information about these NAS features, refer to the NAS feature description in this document.

NACD using the QSIG transport

The MEET feature supports NACD on the ISDN Primary Rate Interface (PRI) or the ISDN Basic Rate Interface (BRI) using the QSIG transport. The ESN Coordinated Dialing Plan (CDP) or Uniform Dialing Plan (UDP) is required but cannot be mixed together. The following NACD functions are available on QSIG:

- Make Set Busy (MSB) key
- Not Ready (NRD) key
- Individual DN key (IDN)
- Dialed Number Identification Service (DNIS) and DNIS Name Display
- Calling Line Identification (CLID)
- ACD-C and ACD-D reports

For information about these NACD features, see *Avaya Automatic Call Distribution Fundamentals, NN43001-351*.

NMS-MC and NMS-MM using the QSIG transport

The MEET feature supports both NMS-MC and NMS-MM on the ISDN Primary Rate Interface (PRI) or the ISDN Basic Rate Interface (BRI) using the QSIG transport.

NMS-MC using the QSIG transport provides:

- Message Center access (direct or indirect)
- Message Waiting Indication notification

A direct call results from a station dialing the DN of the Message Center or pressing the Message Waiting key. An indirect call is a call network redirected to the Message Center.

NMS-MM using the QSIG transport provides:

- Meridian Mail access (direct or indirect)
- Message Waiting Indication notification
- NMS-MM features except Call Sender and Thru-Dialing

For further information about these NMS-MC and MNS-MM features, see the NAS feature description in this document.

Operating parameters

The Manufacturer Specific Information (MSI) carries the MCDN proprietary information transparently over a QSIG network. The third-party node must support the QSIG generic functional protocol (transport) and MSI.

Directory Number (DN) address translation requires the association with a customer number, as configured using the CUST prompt in LD 15.

Either CDP or UDP is required, but they can not be mixed together.

Digit manipulation is not supported for DN transported on QSIG.

Operating parameters for NAS using the QSIG transport

Attendant and users must be located on system nodes to obtain full NAS capabilities.

For NAS Anti-Tromboning capability, both legs must be on the same D-Channel. If the tromboning occurs with one MCDN trunk and one QSIG trunk, the redundant legs are not removed because they are not associated with the same D-Channel.

For a call established through International Standards Organization (ISO) QSIG trunks, the transit counter information is not updated at a QSIG tandem node because the message information is transparent; therefore, the transit counter does not reflect exactly the number of transit nodes the call has gone through.

NAS using the QSIG transport does not support Supervisory Console, Call Park, Charge Account, Do Not Disturb and Group Do Not Disturb, Barge-in, or Emergency Transfer.

There is no gateway developed between NAS functionalities using the QSIG transport and the corresponding DPNSS services. At a QSIG/DPNSS gateway, if NAS information is present, the NAS information is discarded.

Operating parameters for NACD using the QSIG transport

With the MEET feature, NACD continues to work fully with Symposium in an MCDN network. The MEET feature does not support NACD with Symposium using the QSIG transport or a mixed MCDN/QSIG network.

Messages which are resent at the first timer expiration on MCDN are sent once only on QSIG. At the first timer expiration on QSIG, the transaction is cancelled. This applies to the following messages: database update, the logical call request, the cancellation (from source or from target and for any reason) and the status exchange.

Operating parameters for NMS-MC and NMS-MM using the QSIG transport

NMS-MC and NMS-MM using the QSIG transport indirect access are based on the QSIG Call Diversion feature. The QSIG Call Diversion feature must be available and configured in the network.

NMS-MC using the QSIG transport is provided for NMS-MC users and operations located on system nodes.

NMS-MM using the QSIG transport supports all NMS-MM features except Call Sender and Thru-Dialing.

Feature interactions

Feature interactions with NAS using the QSIG transport

Interactions specific to NAS using the QSIG transport are discussed in the following section. Refer to the NAS feature description in this document for generic NAS feature interactions.

QSIG Transit Counter

The QSIG Transit Counter Information Element (IE) is defined only with the ETSI interface; it carries the number of transit nodes the call has gone through. It is updated when a SETUP is sent on an ETSI QSIG trunk. Similarly, the NAS ISDN Call Connection Limitations (ICCL) information is updated when a SETUP is sent on a NAS MCDN or QSIG trunk.

For a call established using the International Standards Organization (ISO) interface for QSIG trunks, the counter information is not updated at a QSIG tandem node because the message information is transparent; therefore, the transit counter does not reflect exactly the number of transit nodes the call has gone through.

QSIG Attendant Recall

QSIG Attendant Recall allows a call extended on an ETSI QSIG trunk to recall the attendant if it is not answered within a customer-defined time. When ETSI QSIG is used and MQC_FEAT is set to NAS, NAS Timed Reminder Recall is enabled and takes precedence over QSIG Attendant Recall.

QSIG ANF Path Replacement/QSIG Call Transfer

QSIG ANF Path Replacement allows an established connection through a QSIG private network to be replaced by a new connection after a call modification to obtain a more efficient connection. It handles triangulation as well as tromboning mechanisms.

QSIG ANF Path Replacement take precedence on NAS anti-tromboning if the "Call transfer complete" FACILITY message is received before the ÔCall extension complete" FACILITY message. Otherwise, NAS anti-tromboning applies and the QSIG ANF Path Replacement is not initiated when a ÔCall transfer complete' FACILITY message is received.

Feature interactions with NACD using the QSIG transport

Interactions specific to NACD using the QSIG transport are discussed in the following section. Refer to *Avaya Automatic Call Distribution Fundamentals, NN43001-351* for information on generic NACD feature interactions.

QSIG Name Display

When QSIG Name Display is configured using the QSIG transport D-Channels and the name is allowed to be displayed and if the call is diverted to the target node through NACD routing, the originator's name is displayed on the target agent's phone and the name of the target agent's ACD DN is displayed on the originator's phone when the target agent answers the call.

Feature interactions with NMS-MC using the QSIG transport

Interactions specific to NMS-MC using the QSIG transport are discussed in the following section. Refer to *Avaya Automatic Call Distribution Fundamentals, NN43001-351* for information on generic NACD feature interactions.

NACD and NAS encapsulation within QSIG

For ACD and attendant Message Centers that are NACD or NAS, the ACD agents and attendants can reside at different nodes. With packaging requirements satisfied at the node where the MC call is presented, either the NACD agents or the NAS attendants are treated as a Message Center.

If the Message Center is an attendant, the NMS-MC feature operation remains the same as for a simple NMS-MC phone. If the attendant NMS-MC has a specific ICI key defined, when a message Waiting call terminates to the attendant NMC-MC, the ICI lamp changes to lit to indicate a NMS-MC call.

As for MCDN, it is not recommended to use NACD or NAS as a NMS-MC unless the message data base can be made available to all agents or attendants at different nodes.

Feature packaging

This feature requires the following packages:

- Multi-purpose Serial Data Link (MSDL) package 222
- QM reference signaling point Interface (QSIG) package 263
- QSIG Generic Functional protocol (QSIGGF) package 305
- MCDN End to End Transparency (MEET) package 348

Depending on the application, other packages are also required.

For the QSIG ISDN PRI interface, the following packages are also required:

- ISDN Signaling (ISDN) package 145
- Advanced ISDN Network Services (NTWK) package 148
- 1.5 Mbit Primary Rate Access (PRA) package 146, or
- 2.0 Mbit Primary Rate Interface (PRI2) package 154, or
- International Primary Rate Interface (IPRA) package 202

The following software packages are required for this feature to operate over QSIG ISDN BRI Trunks:

Note:
ISDN BRI trunk access is not supported in North America.

- Basic Rate Interface (BRI) 216
- ISDN BRI Trunk Access (BRIT) 233

For NAS using the QSIG transport, you must have the ISDN PRI packages or ISDN BRI package and the following packages (the same packages as required for on the MCDN transport):

- Basic Routing (BRTE) package 14
- Basic Queuing (BQUE) package 28
- Network Class of Service (NCOS) package 32
- Network Alternate Route Selection (NARS) package 58
- Coordinated Dialing Plan (CDP) package 59
- Flexible Call Back Queuing (FCBQ) package 61

- Multi-Tenant Service (TENS) package 86
- Attendant Break-In/Trunk Offer (BKI) package 127
- Network Attendant Service (NAS) package 159
- ISDN Supplementary Features (ISDN INTL SUP) package 161
- Remote Virtual Queuing (ORC/RVQ) package 192

Note:
NAS packages and Attendant Overflow Position (AOP) are mutually exclusive and cannot be equipped on the same system.

Note:
NAS packages and Centralized Attendant Service (CAS) are mutually exclusive and cannot be packaged together.

For NACD using the QSIG transport, you must have the ISDN PRI packages or the ISDN BRI package and the following packages (the same packages as required for NACD on the MCDN transport):

- Basic Routing (BRTE) package 14
- Digit Display (DDSP) package 19
- Basic Queuing (BQUE) package 28
- Network Class of Service (NCOS) package 32
- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution, Package B (ACDB), package 41
- Basic Alternate Route Selection (BARS) package 57 or Coordinated Dialing Plan (CDP) package 59 or Network Alternate Route Selection (NARS) package 58
- ACD Enhanced Flow (EOVF) package 178
- Network Automatic Call Distribution (NACD) package 207

For NMS-MC using the QSIG transport, you must have the ISDN PRI packages or ISDN BRI package and the following packages (the same packages as required for NMS-MC on the MCDN transport):

- Message Waiting Center (MWC) package 46
- Network Message Services (NMS) package 175

In addition, Automatic Call Distribution (ACD) Messages Services require the following ACD packages.

- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution, Package B (ACDB), package 41

- Automatic Call Distribution, Package C, (ACDC) package 42
- Automatic Call Distribution, Package A (ACDA) package 45

For NMS-MM using the QSIG transport, you must have the ISDN PRI packages or ISDN BRI package and the following packages (the same packages as required for NMS-MM on the MCDN transport):

- End-to-End Signaling (EES) package 10
- Integrated Message System (IMS) package 35 (for home node only)
- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution, Package A (ACDA) package 45
- Message Waiting Center (MWC) package 46
- Command/Status Link (Class of Service) package 77
- Network Message Services (NMS) package 175

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

10. Table 34: LD 10: Define an analog (500/2500-type) phone at source and/or target node. on page 79
11. Table 35: LD 15: Allow Message Waiting Center access. on page 80.
12. Table 36: LD 11: Define a Meridian 1 proprietary ACD agent phone at source and/or target node. on page 81
13. Table 37: LD 11: Define a Meridian 1 proprietary NMS-MC user phone. on page 81
14. Table 38: LD 23: Create primary voice messaging ACD queue. on page 82
15. Table 39: LD 11: Add agents to the primary agent queue. on page 82
16. Table 40: LD 23: Configure ACD parameters for all voice service queue. on page 83

The following is a summary of the steps required to implement MEET:

1. In LD 17, configure a D-Channel for a PRI interface using the QSIG transport and select the NAS, NACD and/or NMS MCDN features or in LD 16, configure a route for an ISDN BRI interface using the QSIG transport and add the NAS, NACD and/or NMS MCDN features.
2. After selecting NAS in LD 17 or LD 16, configure NAS for a QSIG link by following these steps:
    a. LD 12 – Configure attendant consoles with NAS key (optional).
    b. LD 15 – Enable or disable network attendant control, NAS control and define trunk ICI keys and NAS routing thresholds in LD 15.
    c. LD 86 – Define the NAS routing table.
3. After selecting NACD in LD 17 or LD 16, configure NACD for a QSIG link by following these steps:
    a. Define a CDP or UDP between the two nodes in LD 87 and LD 90.
    b. LD 15 – Configure a CLID table.
    c. LD 23 – Configure the ACD DN queue at source and target nodes.
    d. LD 23 – Configure the NACD routing table in LD 23.
    e. LD 11 – Define a Meridian 1 proprietary ACD phone at source and/or target node.
4. After selecting NMS in LD 17 or LD 16, configure NMS-MC for a QSIG link by following these steps:
    a. Define a CDP (DSC or LSC) or UDP between the two nodes in LD 87 and LD 90.
    b. LD 15 – Allow Message Waiting Center access.

c. LD 11 – Define a Meridian 1 proprietary ACD agent phone at source and/ or target node.

d. LD 11 – Define a Meridian 1 proprietary NMS-MC user phone.

5. After selecting NMS in LD 17 or LD 16, configure NMS-MM for a QSIG link by following these steps:

    a. LD 23 – Configure the primary voice messaging ACD queue at the prime location (where Meridian Mail is installed).

    b. LD 11 – Add agents to the primary agent queue.

    c. LD 23 – Configure ACD parameters for all voice service queues.

    d. Configure the Voice Services DN (VSDN) table in NMS-MM administration terminal. Refer to Meridian Mail documentation for this configuration information.

ISDN PRI implementation using the QSIG transport

Table 25: LD 17: Configure a D-Channel for an ISDN PRI interface using the QSIG transport and add MCDN features.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Configuration database.
...		
ADAN	CHG DCH aaa	Change D-Channel information.
...		
- IFC	ESGF ISGF	ETSI QSIG interface with GF platform. ISO QSIG interface with GF platform.
...		
- RCAP	MQC	Add MCDN QSIG Conversion as a new remote capability. XMQC removes MCDN QSIG Conversion as a remote capability.
-- MQC_FEAT		MCDN QSIG feature type. Prompted if RCAP = MQC. Precede MQC feature type with X to remove.
	NAS	Enable NAS on QSIG. XNAS disables NAS on QSIG.
	NACD	Enable NACD on QSIG. XACD disables NACD on QSIG
	NMS	Enable NMS on QSIG. XNMS disables NMS on QSIG.

ISDN BRI implementation using QSIG transport

Table 26: LD 16: Configure route for an ISDN BRI interface using the QSIG transport and add MCDN features.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
TKTP	a...a	Trunk Type.
...		
DTRK	(NO) YES	Digital Trunk Route.
- BRIP	(NO) YES	ISDN BRI Packet handler route
- DGTP	a...a BRI	Digital Trunk Type for route. Basic Rate Interface (Allowed if TKTP = TIE, COT or DID and BRIP = NO
...		
- IFC	ESGF ISGF	ETSI QSIG interface with GF platform. ISO QSIG interface with GF platform.
...		
- RCAP	MQC	Add MCDN QSIG Conversion as a new remote capability. XMQC removes MCDN QSIG Conversion as a remote capability.
-- MQC_FEAT		MCDN QSIG feature type. Prompted if RCAP = MQC. Precede MQC feature type with X to remove.
	NAS	Enable NAS on QSIG.
	NACD	Enable NACD on QSIG.
	NMS	Enable NMS-MC and NMS-MM on QSIG.

NAS implementation using the QSIG transport

To configure NAS using the QSIG transport, follow these steps:

- Configure an ISDN PRI interface using the QSIG transport and select NAS as an MCDN feature in LD 17, or configure an ISDN BRI interface using the QSIG transport or and select NAS as an MCDN feature in LD 16.
- Configure NAS for a QSIG link:
    - Configure attendant consoles with NAS key (optional) in LD 12.
    - Enable or disable network attendant control, NAS control and define trunk ICI keys and NAS routing thresholds in LD 15.
    - Define the NAS routing table in LD 86.

Table 27: LD 12: Configure Attendant Consoles with NAS keys. (optional)

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	2250	Attendant Console type.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
KEY	xx NAS	xx = the key number assigned the NAS function. Each attendant console can have only one NAS key defined. This key is optional.

Table 28: LD 15: Enable or disable network attendant control, NAS routing, and define a trunk ICI key.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ATT	Attendant data.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...	...	...

Prompt	Response	Description
- ISDN	YES	Integrated Services Digital Network.
...	...	...
- ICI	0-19	Key number. Followed with a space and the trunk type.
	NCO NDID NTIE NFEX NWAT	Network CO trunk. Network DID trunk. Network TIE trunk. Network FEX trunk. Network WAT trunk.
...	...	...
- CWCL	(0)-255 (0)-255	Call Waiting Call Limit. Lower and upper thresholds.
- CWTM	(0)-511 (0)-511	Call Waiting Time. Lower and upper thresholds (in seconds).
...	...	...
- NAS ATCL	YES (NO)	Allow/deny attendant control for call extension.
- NAS ACTV	YES (NO)	Allow/deny NAS routing.

Table 29: LD 86: Define NAS routing tables.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	NAS	Type of data.
TBL	0-63	Routing table number. Without Multi-Tenant Service, 0 is the customer routing table. With Multi-Tenant Service enabled, NAS tables 1-63 can be associated with Console Presentation Groups (CPGs) 1-63.
ALT	1-7	An alternative attendant or routing table. (To clear an old number, type an X before typing the new number. The old number cannot be cleared if it is associated with a schedule period. Reach TODS by pressing the return key.)
ID	xx...x <CR>	The dialed digits (including the network access code) needed to reach an attendant associated with the alternative number. Respond with a string of up to 16 digits to change the attendant ID. Press the return key to leave the ID unchanged, exit the prompt, and return to ALT.
TODS	0-31	Time of Day schedule where;

Prompt	Response	Description
		0 = default to handle all time periods not defined in 1 through 31. Press the return key to continue the NAS feature setup process.
- PER	hr: mm hr: mm	Specify start and stop times for the period using 24-hour format. Start time must be before stop time. mm = 00 or 30 only.
	<CR>	<CR> = leave times unchanged; move to the DAYS prompt.
- DAYS	a,a...a	Specify applicable days of the week for the time period. Input a number representing each day for which the schedule is active (where 1 = Monday, 2 = Tuesday... 7 = Sunday).
ALST	1-7	Alternatives list to be used for the schedule period.
DBK	(NO) YES	Disable/enable Drop Back busy option.
QUE	(NO) YES	Disable/enable queuing to a route.

NACD implementation using the QSIG transport

To configure NACD using the QSIG transport, follow these steps:

- Configure an ISDN PRI interface using the QSIG transport or and select NACD as an MCDN feature in LD 17, or configure an ISDN BRI interface using the QSIG transport or and select NACD as an MCDN feature in LD 16.
- Configure NACD for a QSIG link:
    - Define a CDP or UDP between the two nodes.
    - Configure a CLID table in LD 15.
    - Configure the ACD DN queue at source and target nodes in LD 23.
    - Configure the NACD routing table in LD 23.
    - Define a Meridian 1 proprietary ACD phone at source and/or target node in LD 11.

Table 30: LD 15: Configure a CLID table.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	NET	Networking data (if REQ = CHG only).
CUST		Customer number

Prompt	Response	Description
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
- CLID		CLID option.
	YES (NO)	Configure a CLID table for the customer. (the default) do not configure a CLID table. Remaining prompts are not generated and no CLID is sent for the customer.
...		
- - ENTRY	y	CLID entry number.

Table 31: LD 23: Configure ACD Directory Number queues at source and target nodes.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ACD	Automatic Call Distribution data block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
ACDN	xxxx	ACD Directory Number.

Table 32: LD 23: Configure an NACD Routing Table.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	aaaa	Type of data block. Enter NACD for Network ACD.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ACDN	xxxx	ACD Directory Number.
TABL	a	Day or Night Table. a = D or N.
- OUTS	xxxx xxxx	Routing Table entries to be removed.
- TRGT	xxxx tttt	Target ACD DN and the timer in seconds.

Note:
When assigning a CLID entry to an ACD phone, you cannot use the position ID already on the phone. You must out the set first or null the ACD key and then rebuild with the table entry number.

Table 33: LD 11: Define a Meridian 1 proprietary ACD phone at source and/or target node.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	a...a	Telephone type. Type **?** for a list of possible responses.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
CLS	(AGN) SPV	Class of Service group. AGN = (default) ACD Agent. SPV = ACD Supervisor.
...		
KEY	xx ACD yyyy 0-N/D zzzz	ACD key, where: xx = key number (*must be key 0*). yyyy = ACD DN or Message Center DN. 0-N = CLID entry, with N = CLID SIZE-1 (SIZE defined in LD 15). D = CLID entry, Search for a CLID entry from key 0 upwards, to find a DN key. the found CLID is used as the CLID entry for the active DN key. zzzz = ACD agent's position ID. Refer to the note at the top of LD 11 on assigning a CLID entry to an ACD phone.
KEY		Phone function key assignments.
	xx MSB yyyy (0)-N/D) xx NRD yyy (0)-N/D	xx = key number. MSB = Make Set Busy key. NRD = Not Ready key.

Table 34: LD 10: Define an analog (500/2500-type) phone at source and/or target node.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	500	Analog (500/2500-type) phone.
TN		Terminal number

Prompt	Response	Description
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
CLS	AGTA	ACD services for analog (500/2500-type) phones allowed.
...		
FTR	ACD xxxx 0-N/D zzzz	ACD feature where: aaa = ACD. xxxx = ACD DN. 0-N/D = CLID entry. zzzz = ACD agent's position ID.

NMS implementation using the QSIG transport

To configure NMS-MC using the QSIG transport, follow these steps:

- Configure an ISDN PRI interface using the QSIG transport or and select NMS as an MCDN feature in LD 17, or configure an ISDN BRI interface using the QSIG transport or and select NMS as an MCDN feature in LD 16.
- Configure NMS-MC for a QSIG link:
    - Define a CDP (DSC or LSC) or UDP between the two nodes.
    - Allow Message Waiting Center access in LD 15.
    - Define an ACD agent phone at source and/or target node in LD 11.
    - Define an NMS-MC user phone in LD 11.

Table 35: LD 15: Allow Message Waiting Center access.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	FTR	Feature data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
OPT	(MCX) MCI	Message Center excluded. Message Center included.
	(MWUD) MWUA	Message Waiting Unconditional Denied. Message Waiting Unconditional Allowed.

Table 36: LD 11: Define a Meridian 1 proprietary ACD agent phone at source and/or target node.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	a...a	Telephone type. Type **?** for a list of possible responses.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
CLS	(MWD) MWA	Class of Service options. Message Waiting Denied Message Waiting Allowed.
...		
KEY	xx MIK	MIK = Message Indication Key. xx = key number.
	xx MCK	MCK = Message Cancellation Key. xx = key number.

Table 37: LD 11: Define a Meridian 1 proprietary NMS-MC user phone.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	a...a	Telephone type. Type **?** for a list of possible responses.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
CLS	AGTA	ACD services for analog (500/2500-type) phones allowed.
KEY	xx MWK x...x	Phone function key assignments where:
		xx = key number. MWK = Message Waiting Key x...x = NMS-MC DN.

To configure NMS-MM on QSIG, follow these steps:

- Configure an ISDN PRI interface using the QSIG transport or and select NMS as an MCDN feature in LD 17, or configure an ISDN BRI interface using the QSIG transport or and select NMS as an MCDN feature in LD 16.
- Configure NMS-MM for a QSIG link:

- Configure the primary voice messaging ACD queue at the prime location (where Meridian Mail is installed) in LD 23.
- Add agents to the primary agent queue in LD 11.
- Configure ACD parameters for all voice service queues in LD 23.
- Configure the Voice Services DN (VSDN) table in NMS-MM administration terminal.

Table 38: LD 23: Create primary voice messaging ACD queue.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	ACD	Type of data block. ACD = Automatic Call Distribution data block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ACDN	xxxx	ACD DN = Express Messaging DN (the DN which users dial to access their mailboxes).
MWC	YES	ACD DN is a message center DN.
.		
NCFW	xx...x	Night Call Forward DN (up to 23 digits).

Note:

When assigning a CLID entry to an ACD phone, you cannot use the position ID already on the phone. You must out the phone first or null the ACD key and then rebuild with the table entry number.

Table 39: LD 11: Add agents to the primary agent queue.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	xx	ACD data block.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
CLS	VMA	Allow voice messaging.
...		
KEY		xx = key number

Prompt	Response	Description
	xx ACD yyyy 0-N/ D zzzz	ACD key, where: xx = key number (must be key 0). yyyy = ACD DN or Message Center DN. 0-N = CLID entry, with N = CLID SIZE-1 (SIZE defined in LD 15). D = CLID entry, Search for a CLID entry from key 0 upwards, to find a DN key. the found CLID is used as the CLID entry for the active DN key. zzzz = ACD agent's position ID. Please refer to the note at the top of LD 11 on assigning a CLID entry to an ACD phone.
	xx SCN yyyy (ccc or D).	Single Call Non-Ringing DN where: yyyy = DN ccc = CLID entry of (0)-N, where N = the value entered at the SIZE prompt in LD 15 minus 1. D = the character D can be entered to search a CLID entry from key 0 and up to find a DN key. The CLID associated with the found DN key will then be used. The DN can be up to 4 digits, up to 7 digits with Directory Number Expansion (DNXP) package 150. Once the SCN key has been defined, MARO is prompted.
	xx MSB	Make Set Busy key.
	xx NRD	Not Ready key.
	xx TRN	Call Transfer key.
	xx A03	A03 = Three-Party Conference key.
	xx A06	A06 = Six-Party Conference key.
	xx RLS	Release key.
		Requires CLS = LUXA. Key/lamp pair is not required.

Table 40: LD 23: Configure ACD parameters for all voice service queue.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	ACD	Automatic Call Distribution data block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ACDN	x...x	ACD Directory Number.
MWC	(NO) YES	Message Waiting Center.
...		
MAXP	xxxx	Maximum number of positions. Enter 1.
...		

Prompt	Response	Description
NCFW	xx...x	Night Call Forward DN = DN of the primary voice messaging queue in network format. xx...x = up to 23 digits.

Feature operation

Feature operation for direct Message Center calls and Indirect Message Center calls are presented in the following sections.

For NAS and NMS-MC and NMS-MM feature operation, see the NAS feature description in this document.

For NACD feature operation, see *Avaya Automatic Call Distribution Fundamentals, NN43001-351*.

Direct Message Center call

1. User A dials their MC DN or presses their MWK key.
2. The MC rings. For ACD phones, the MCK lamp state shows the MC user's message indication state: lit if there is no message; slow flash if a message is waiting; fast flash if there is bad data; dark if message waiting indication class of service is denied.
3. The MC operator answers the call. For DN phones, the MCK lamp state reflects MC user's message indication state.
4. User B is connected to MC and is given their message by the MC operator.
5. The MC operator presses MCK key (if MCK lamp is flashing) to turn off message waiting indication at station B. The MCK lamp changes to dark.
6. User A disconnects from the MC.

Indirect Message Center call

1. User A calls User B.
2. User B has calls redirected to the MC (Call Forward all Calls or No Answer).
3. The call is presented to the MC; MC rings; MC operator answers the call.
4. If QSIG Diversion is configured, the MIK lamp has the lamp state that reflects the MC user's message indication state: lit if there is no message; flash if a message

is waiting; fast flash if there is bad data; dark if message waiting indication class of service is denied.User A is connected to MC and leaves a message.

5. If QSIG diversion is not configured, the MC operator activates the Message Waiting indication in the following sequence:

    - MC operator puts the call On Hold, presses the MIK key and MIK lamp lights.
    - MC operator dials User B's DN. The MIK lamp changes to the lamp state that reflects the MC user's message indication state.
    - If the MIK lamp is lit, the MC operator presses the MIK key to turn on the message waiting indication at station B, The MIK lamp changes to dark.
    - The MC operator returns to the Held call.

6. User A disconnects from the call.

Chapter 8: Meridian Hospitality Voice Services

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

This feature provides an enhanced form of Meridian Mail tailored to Hospitality Services. It simplifies the use of mailboxes and allows more dynamic management of mailboxes as guests check in and out.

Two components of this feature rely on ISDN. These are:

- Property Management System Interface Enhancement (Message Waiting Indication Enhancement)
- ISDN/AP Recovery Enhancement

Message Waiting Indication Enhancement

Under the Property Management System Interface enhancement, Text Messaging on a Property Management System (PMS) and Voice Mail on Meridian Mail are integrated. The handling of Message Waiting Indications from the ISDN/AP is enhanced to ensure that Meridian Mail controls the Message Waiting status for both voice and text messages. Message

Waiting Indications will be handled only by way of the ISDN/AP link (when that link is enabled).

Note:
If the ISDN/AP link is disabled for any reason, the PMS link will be used to update Message Waiting Indication status.

ISDN/AP recovery enhancement

The ISDN/AP link is used to pass all of the command and status information between the system and any Value Added Server (VAS). When the ISDN/AP link fails, due either to faults in the link itself or failure of the VAS, all signaling between the system and the VAS stops. Calls could be left in various ringing states indefinitely (until the ISDN/AP link is restored).

The ISDN/AP Recovery Enhancement ensures that callers to any VAS, using a particular ISDN/AP link, are redirected to some alternate DN, should that ISDN/AP link fail. This redirection only applies to calls in the ringing state which are being presented to virtual Voice Messaging Service agents.

Calls in the following call states can be recovered under this enhancement:

- calls ringing to a virtual Voice Messaging Service agent, but not yet answered by the VAS
- calls in an ACD queue at the time the failure is detected
- new calls arriving at the queue after the failure is detected, but before the link is restored

Calls are recovered from ACD queues under the following conditions:

- The ACD queue is defined as a Message Waiting Center.
- The ACD queue uses the ISDN/AP.
- All ISDN/AP links associated with the ACD queue are not active.
- If an ACD agent is involved in the call, the agents must be defined as Virtual Voice Messages access agents for the enhancement to take effect.

When calls are redirected, they are routed to the Night Call Forward DN (NCFW) for the particular ACD queue involved. The treatment of calls will be identical to that of existing Night Call Forward operation for ACD queues, except that the Night Call Forward DN must be located on the same switch as the attendant and room phones.

When the ISDN/AP link fails, any calls without disconnect supervision which are connected to the VAS are disconnected immediately. Calls with disconnect supervision remain connected, until the originating end disconnects. In either case, a CDR record is produced when the call is released from the agent.

When the ISDN/AP link becomes operational once again (through either automatic or manual recovery), the handling of new calls will return to normal.

Operating parameters

No operating parameters are specified for this feature.

Feature interactions

Attendant End-to-End Signaling (AEES)

AEES, which uses Dual-tone Multifrequency signaling, requires an additional Attendant EES key.

Attendant Overflow Position (AOP)

Attendant Overflow allows unanswered calls to the attendant to be forwarded to a customer-defined DN after a defined time. With AOP equipped, overflowed calls can be directed to Meridian Mail. The AOP DN must be defined as an ACD DN, and the ACD DN must be an ACD agent configured as a Virtual Voice Messaging Service (VMS) agent. A call can also be overflowed if all the attendants are in Position Busy.

Centralized Attendant Service (CAS)

The attendant must be located on the same switch as Meridian Mail for the attendant to use Meridian Mail features.

Digit Key Signaling (DKS)

With the DKS package (180) equipped, attendants assist callers in operating Meridian Mail Voice Messaging Service. The attendant enters the digits for Meridian Mail and extends the call to Meridian Mail. The caller can then access voice messaging. DKS is only supported from the attendant consoles local to Meridian Mail. The attendant can also place direct calls to Meridian Mail.

Digit Key Signaling at Console (DKS)

With DKS equipped, attendants assist callers in Meridian Mail activities. The attendant extends source calls to Meridian Mail or direct calls to Meridian Mail.

Do Not Disturb (DND)

Individual DND allows the attendant to place a DN in the Do Not Disturb mode. A DN in this mode is free to originate calls, but appears busy to incoming calls. With DND equipped, callers can be redirected to Meridian Mail for Voice Mail Services. A called phone must have Hunting Allowed (HTA) Class of Service and the Customer Route Data Block must be set to "YES" in LD 15.

M2317 and Meridian Modular soft key menus

M2317 or Meridian Modular soft key menus are not supported by MHVS. These three phones with CCSA Class of Service are not presented with the Meridian Mail softkey menus when connected to Meridian Mail.

Network Automatic CallDistribution

The Night Number specified for the Automatic Call Distribution (ACD) involved in the ISDN/AP recovery operation must be local to the node.

PMSI, DKS, DND, and Message Waiting Indication

These operations are only supported when PMSI, Meridian Mail, and attendant room phones are located on the same switch.

Pretranslation

Prior to MHVS, the setup of calls using the ISDN/AP was not supported from phones using the Pretranslation feature. With MHVS equipped, call setup using the ISDN/AP is supported.

Stripping of Calling Party Name Display (CPND) Blanks

The maximum length of a CPND name sent from the PMSI/Background (BGD) terminal is 27 characters. When the full 27-character length is used, part of the CPND name can scroll off the screen. To avoid this problem, the PMSI/BGD software has been updated to strip all trailing blanks from the CPND name from the screen.

Feature packaging

Meridian Hospitality Voice Services (MHVS) requires software package 179.

The standard Meridian Mail packages must be equipped for the Pretranslation and Do Not Disturb functions to operate properly. These include:

- Recorded Announcement (RAN) package 7
- End-to-End Signaling (EES) package 10
- Make Set Busy (MSB) package 17
- Integrated Message Services (IMS) package 35
- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution Package A (ACDA) package 45
- Message Waiting Center (MWC) package 46
- Command Status Link (CSL) package 77
- CSL with Alpha Signaling (CSLA) package 85
- Auxiliary Processor Link (APL) package 109

The Property Management System Interface (PMSI) package requires the following packages:

- Controlled Class of Service (CCOS) package 81
- Background Terminal (BGD) package 99
- Room Status (RMS) package 100
- Property Management System Interface (PMSI) package 103

The Attendant Overflow (AOP) package 56 is required for AOP DN enhancement.

The Digit Key Signaling (DKS) package 180 requires that the standard Meridian Mail packages, such as those listed under Meridian Hospitality Voice Services (MHVS) package 179, are equipped.

The site can also require other packages such as PPM/Message Registration (MR) package 101 and Automatic Wake-up (AWU) package 102; however, these packages do not impact MHVS operations.

Integrated Services Digital Network (ISDN) package 145 is also required.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 41: LD 15: Allow call redirection to Meridian Mail for voice messaging. on page 92
2. Table 42: LD 23: Define the Attendant Overflow Position (AOP) Directory Number. on page 92

Table 41: LD 15: Allow call redirection to Meridian Mail for voice messaging.

Prompt	Response	Description
REQ	CHG	Change
TYPE	RDR	Call Redirection data
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
DNDH	YES	Do Not Disturb Hunting. MHVS package (179) must be equipped for this prompt to appear. LD 21 will reflect the DNDH option if MHVS is equipped.

Table 42: LD 23: Define the Attendant Overflow Position (AOP) Directory Number.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ACD	Automatic Call Distribution Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ACDN	xxxx	ACD Directory Number.
MWC	YES	ACD DN Message Center DN.

Prompt	Response	Description
CMS	YES	Command and status link.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 9: Meridian Mail Trunk Access Restriction

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Meridian Mail Trunk Access Restriction (MTAR) feature prevents direct or indirect call transfer or conference of external calls to Meridian Mail. In this feature, external calls are defined as incoming/outgoing trunk calls that originate or terminate outside a private network.

This definition is applicable to all types of trunks, with the exception of TIE trunk calls. External calls are separated from a transferring/conferencing phone on a network using TIE trunks. MTAR operation is dependant on the information sent to the remote node from the node that is attempting to transfer/conference.

MTAR is triggered if the network information (such as Network Attendant Service or Calling Line Identification) indicates that an external call and a transfer/conference attempt to Meridian Mail is occurring. MTAR is also triggered if local information, such as Route Class, indicates an external call and a transfer/conference attempt to Meridian Mail is occurring.

Meridian Mail Trunk Access Restriction averts potential Meridian Mail system abuse by distinguishing between internal and external calls that are directed to Meridian Mail. When activated, Meridian Mail Trunk Access Restriction impacts the operation of the following features:

- Call Transfer
- Conference
- No Hold Conference
- Call Join capabilities of the Multi-Party Operation feature

Meridian Mail Trunk Access Restriction prevents the completion of any Call Transfer, Conference, No Hold Conference or Call Join attempts on incoming/outgoing external calls to Meridian Mail.

As illustrated in Figure 7: Meridian Mail Trunk Access Restriction Call Transfer on page 96, MTAR capabilities prevent an established call between Phone A, an internal call, and Phone B, an external call, from being forwarded to Meridian Mail. When Phone A attempts to either Transfer, Conference, No Hold Conference or Call Join Phone B to Phone C, which is either a direct Meridian Mail DN or has activated Call Forward All Calls (CFAC) to Meridian Mail, the transfer and conference keys are ignored when pressed to complete operation.

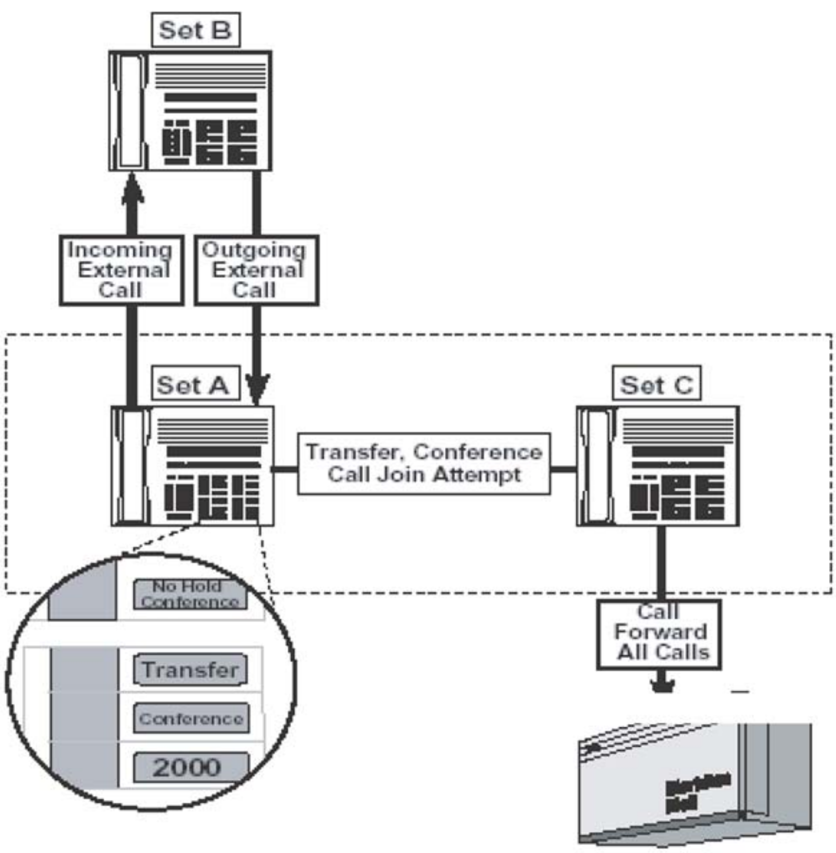

Figure 7: Meridian Mail Trunk Access Restriction Call Transfer

Operating parameters

MTAR does not treat Centralized Attendant Position and Night Attendant phones as Attendant Consoles. These phones receive treatment based on their actual phone type. For example, if the night attendant is a Meridian 1 Proprietary Phone, then it is treated as Meridian 1 Proprietary Phone.

The operation of an Attendant Console is not affected when this feature is enabled. An attendant can transfer or conference an external line to Meridian Mail directly or indirectly.

MTAR does not affect Automatic Attendant, Customer Controller Routing, Integrated Voice Response or Meridian Link features. However, if a user disallows any of these features from accessing Meridian Mail, the application must be written to take this into account.

Call transfer from ISDN Basic Rate Interface (BRI) phone is not supported.

In a networking environment, Meridian Mail must reside on the same node as the transferring/ conferencing phone.

Feature interactions

Traffic Reporting

Traffic Reporting and Meridian Administration Tool's (MAT) traffic report, TFC005, are modified to report the number of times this feature is requested. A new line is added for the Meridian Mail Trunk Access Restriction which is identified by the feature number "27" and its peg count.

Network Call Transfer

Network Call Conference

Meridian Mail Trunk Access Restriction (MTAR) requires the transferring or conferencing phone and Meridian Mail to be located on the same node. If the transferring or conferencing phone are located not on the same node as Meridian Mail, the MTAR feature is not provoked because the call transfer/conference attempt is terminated by a network on Meridian Mail.

However, an external call can be transferred or conferenced over the network, using TIE trunks. This operation is dependant on the type of network information the remote node forwards to the node where the transfer/conference attempt is made. Meridian Mail must be on the transferring/conferencing node. If network information is provided, indicating that an external call is attempting to transfer/conference to Meridian Mail, the MTAR feature is invoked. When no network information is provided, MTAR is provoked if the local information (Route Class) indicates that an external call to Meridian Mail is being attempted.

Feature packaging

Meridian Mail Trunk Access Restriction requires Message Waiting Center (MWC) package 46.

Feature implementation

Note:

Meridian Mail Trunk Access Restriction feature requires prior installation of Meridian Mail. The implementation of this feature, therefore, assumes that Meridian Mail has been properly configured.

Table 43: LD 15: Enable Meridian Mail Trunk Access Restriction.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	FTR	Customer Features and Options.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
- OPT	MCI	Message Centre Included.
...		
- MTAR	YES	Meridian Mail Trunk Access restricted. NO = Meridian Mail Trunk Access allowed.

Feature operation

Call Transfer/Conference

digital phone

Phone A is a digital proprietary phone with Transfer Key and Conference Key.

1. An incoming/outgoing external call is established between Phone A and Phone B, an external party. The call between Phone A and Phone B is active on Key X.
2. Phone A presses the Transfer/Conference Key that automatically puts Phone B on Hold.
3. Phone A dials Phone C. Phone C has either Call Forward All Calls to Meridian Mail or is a Meridian Mail DN.
4. When Phone A attempts to transfer/conference Phone B by pressing more than once the Transfer/Conference Key it is ignored.
5. Phone A recovers Phone B by pressing Key X.

No Hold Conference

Digital phone/ISDN BRI phone

When Meridian Mail Trunk Access Restriction is enabled, direct or indirect no hold conference to an external call is permitted. During direct or indirect no hold conference, the calling party is never put on hold.

Phone A is a digital proprietary phone or an ISDN BRI phone with a No Hold Conference Key configured as either No Hold Conference, Conference Autodial, Conference Speed or Conference Hotline.

1. An incoming/outgoing external call is established between Phone A and Phone B, an external party. The call between Phone A and Phone B is active on Key X.
2. Phone A presses the No Hold Conference Key.
3. Phone A dials Phone C. Phone C is has either Call Forward All Calls to Meridian Mail enabled or is a Meridian Mail DN.
4. The conference is set up as normal. However a two party connection between Phone B, an external party, and Meridian Mail is not allowed if the call controller releases. If this occurs, the connection between the trunk and Meridian Mail party is dropped.

Transfer analog (500/2500-type) phone

Phone A is an analog (500/2500-type) phone with a XFA Class of Service (transfer and three/six party conference allowed).

1. An incoming or outgoing external call is established between Phone A and Phone B, an external party.
2. Phone A performs a switchhook flash that puts Phone B on hold.
3. Phone A dials Phone C. Phone C has either Call Forward All Calls to Meridian Mail enabled or is a Meridian Mail DN.
4. Before or after the Meridian Mail has answered, Phone A attempts to transfer Phone B to Meridian Mail by going on-hook.
5. This attempt is treated as an illegal transfer. Phone A is re-rung and reconnected with Phone B when going off-hook.

Conference analog (500/2500-type) phone

Phone A is an analog (500/2500-type) phone with a XFA Class of Service (transfer and three/six party conference allowed).

- An incoming or outgoing external call is established between Phone A and Phone B, an external party.
- Phone A performs a switch hook flash that puts Phone B on hold.
- Phone A dials Phone C. Phone C has either Call Forward All Calls to Meridian Mail enabled or is a Meridian Mail DN.
- Before or after the Meridian Mail has answered, Phone A attempts to conference Phone B to Meridian Mail by performing another switchhook flash.
- The conference is not permitted. Phone A is reconnected to Phone B. The call to Meridian Mail is disconnected.

Phone A is an analog (500/2500-type) phone with a TSA Class of Service (three party service allowed).

- An incoming or outgoing external call is established between Phone A and Phone B, an external party.
- Phone A perform a switch hook flash that puts Phone B on hold.
- Phone A dials Phone C. Phone C has either Call Forward All Calls to Meridian Mail enabled or is a Meridian Mail DN.
- Before or after Meridian Mail has answered, Phone A attempts to conference Phone B to Meridian Mail by dialing the conference control digits.
- The conference is not permitted and Phone A is reconnected to Phone B. The call to Meridian Mail is disconnected.

Table 44: Summary of Meridian Mail Trunk Access Restrictions on page 101 summarizes how different external calls are handled when Meridian Mail Trunk Access Restriction is enabled.

Table 44: Summary of Meridian Mail Trunk Access Restrictions

Phone	External Call Type	Operation	Failure Treatment	Result
500/2500	Incoming	Transfer to Meridian Mail (MMail)	Re-ring to transferring phone	Not allowed
500/2500	Incoming	Transfer to phone with Call Forward All Calls (CFAC) to MMail	Re-ring to transferring phone	Not allowed
500/2500	Outgoing	Transfer to MMail	Disconnect external call and Meridian Mail	Not allowed
500/2500	Outgoing	Conference to phone with CFAC to MMail	Disconnect external call and Meridian Mail	Not allowed
500/2500	Outgoing/ Incoming	Conference to MMail	Reconnect to external call. Disconnect call to MMail	Not allowed
500/2500	Outgoing/ Incoming	Conference to phone with CFAC to MMail	Reconnect to external call. Disconnect call to MMail	Not allowed
Meridian 1 Proprietary	Outgoing/ Incoming	Transfer/ Conference to MMail	Operation ignored	Not allowed
Meridian 1 Proprietary	Outgoing/ Incoming	Transfer/ Conference to phone with CFAC to MMail	Operation ignored	Not allowed
Meridian 1 Proprietary	Outgoing/ Incoming	No Hold Conference to Meridian Mail or to set CFAC to MMail	Not applicable	Allow
Meridian 1 Proprietary	Outgoing/ Incoming	No Hold Conference release to make MMail to trunk two-party connection	Disconnect MMail and external trunk	Not allowed
Meridian 1 Proprietary	Outgoing/ Incoming	Call Join of external call to MMail	Operation ignored	Not allowed
Basic Rate Interface	Outgoing/ Incoming	Conference to MMail	Operation ignored	Not allowed

Phone	External Call Type	Operation	Failure Treatment	Result
Basic Rate Interface	Outgoing/ Incoming	Conference to set with CFAC to MMail	Operation ignored	Not allowed
Attendant	Outgoing/ Incoming	Transfer/ Conference to Meridian Mail	Not Applicable	Allowed
Attendant	Outgoing/ Incoming	Transfer/ Conference to phone with Call Forward All Calls to Meridian Mail	Not Applicable	Allowed

Chapter 10: Message Waiting Indication Interworking with DMS

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

This interworking feature allows a Message Center on either a system or DMS-100 (Centrex) to exchange Message Waiting Indicator information with phones serviced by either type of system on the network. Calls redirected to the Message Center can be from private or public network callers on either system. A caller served by the system can use the Message Center on DMS. A caller served by DMS can use the Message Center (Meridian Mail) on the system. The system must use Meridian Mail as its Message Center.

MWI uses the non-call associated Facility messages on ISDN PRI for transporting the TCAP information.

The system and DMS systems can be connected directly or in tandem to whichever system hosts the Message Center. When a caller from either system leaves a message on either system, the Message Waiting Indicator is activated. When the receiver retrieves the message, the Message Waiting Indicator is deactivated. The indicator is either a visual LED (light emitting diode), an icon, or an audible tone in the phone handset.

Figure 8: Private corporate network with the system hosting the Message Center on page 104 shows a network in which the system hosts the Message Center that serves both system users and users of a DMS-100 in the same customer group.

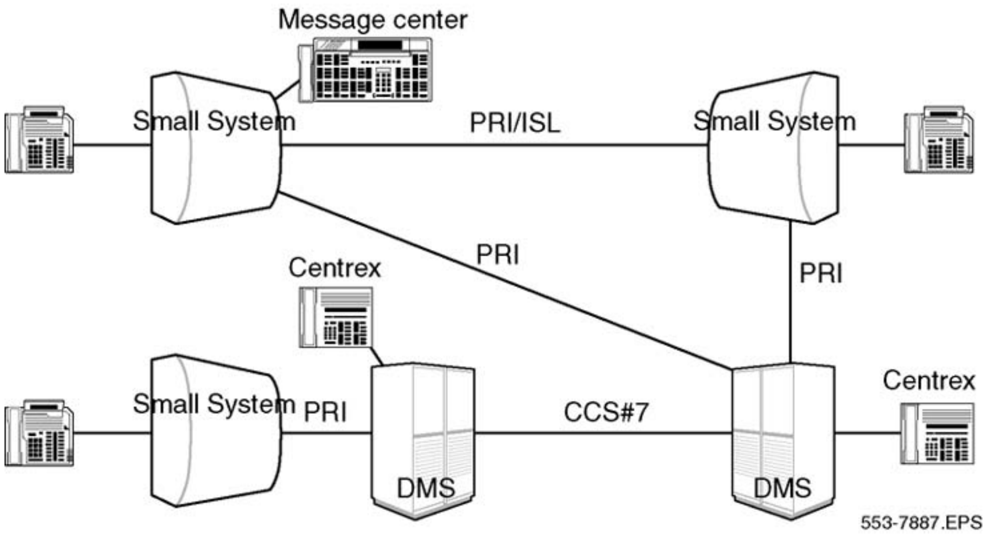

Figure 8: Private corporate network with the system hosting the Message Center

Note:

CCS#7 is not supported by Meridian 1, CS 1000M. CCS#7 must be a DMS-to-DMS configuration.

Figure 9: Private corporate network with DMS hosting the Message Center on page 105 shows a network in which DMS hosts the Message Center that serves both system users and DMS users in the same or different enterprise groups.

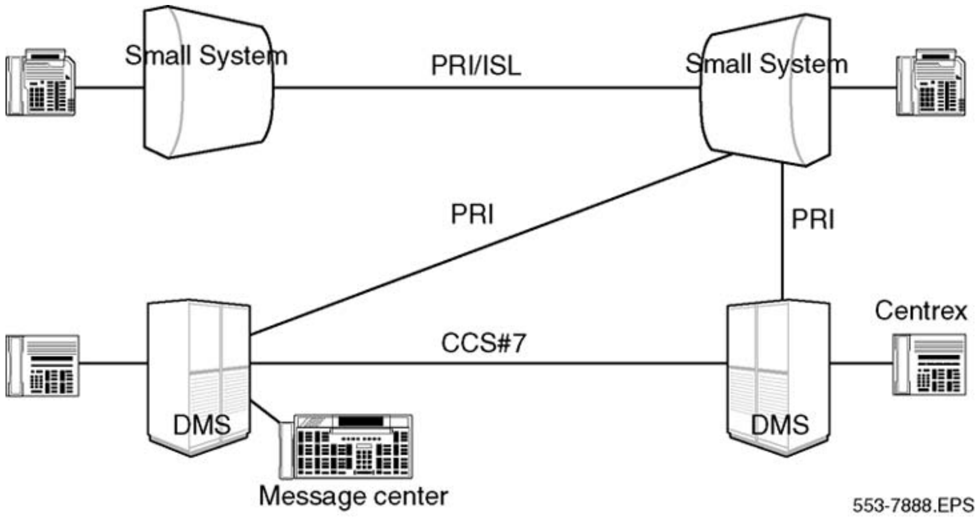

Figure 9: Private corporate network with DMS hosting the Message Center

Note:
CCS#7 is not supported by the system; CCS#7 must be a DMS-to-DMS configuration.

Operating parameters

MWI supports DMS-100 and SL-100 as tandem switches, but does not support non-Avaya switches as tandems.

Only Meridian Mail is supported as the Message Center.

Both DMS-100 and the system can transport Facility messages for MWI and can be tandem switches. DMS-100 can tandem Facility messages from system to system for features, such as Call Sender, activated by system users of Meridian Mail. Other Facility messages that DMS-100 can tandem are for updating the voice mail softkeys of an M2317 phone.

MWI allows public and private numbers for the Original Called Number (OCN) in the Setup message during call forwarding. It also allows public and private numbers for the Directory Numbers (DN) in the ORIG and DEST Information Elements (IE) of the Facility message in order to toggle the MWI Indicator. The OCN refers to the user's mailbox DN. The OCN must be unique in the Meridian Mail database. If the call forwarding DN to the Message Center is a private number, the OCN constructed in the setup message will contain a private number. If the call forwarding DN to the Message Center is a public number, then the OCN constructed in the setup message will contain a public number.

If Meridian Mail is on the system:

- For Meridian 1and CS 1000M users, Meridian Mail provides the same functions as for the NMS-MM users, if a private number is used.
- For DMS users, some Meridian Mail features are not available. Contact your local DMS administrator for available Meridian Mail features.

If the Message Center is on DMS:

If a phone on the system does not have a DID number, the call forwarding DN to the Message Center should be private. Thus, a phone that cannot receive DID calls will still be able to use the Message Center services provided that the DMS Message Center supports private numbers for the mailbox DNs.

End-to-End in-band signaling is required for accessing Message Center features for a local or remote switch.

The call forwarding connection from the caller to the Message Center on another switch must be with ISDN conductivity between the system and DMS. This is for passing the OCN from the caller's switch to the switch that hosts the Message Center for leaving voice messages and for transporting TCAP messages to toggle the MWI Indicator.

Feature interactions

Multiple Customer

Serving multiple customers requires multiple Meridian Mail servers. MWI itself does not support multiple customers.

Multi-Tenant Service

Meridian Mail Phase 8 supports Multi-Tenant Service. Tenants from the same customer can use one or more Message Center servers. Tenants from different customers cannot use the same Meridian Mail. The customer controls tenant access to MWI using the phones that belong to the tenant.

Network Message Services, Meridian Mail

Although the Facility message for MWI uses a different TCAP format from that used for NMS, the functions continue to operate.

DCH Error Monitoring

The DCH Error Monitoring monitors ISDN messages for each feature. If the MWI RCAP for the D-channel is added or deleted in LD 17, DCH Error Monitoring will work properly for the NMS feature when the D-channel message monitoring is disabled and then enabled.

Trunk Optimization Before Answer

There is no Trunk Optimization when the call is redirected to DMS or answered by Meridian Mail. This applies to applications such as Auto Attendant.

AML Link Recovery

AML Link Recovery redirects the calls to the ACD queue of the ACD Night Forward DN when the AML link goes down. This recovery is also available for calls in the Meridian Mail ACD queue on the system when the AML link goes down.

Feature packaging

The package requirements for Message Waiting Indication (MWI) are different for each node. The following packages are required for an MWI originating node:

- End-to-End Signaling (EES) package 10
- Basic ACD (BACD) package 40
- ACD package A (ACDA) package 45
- Message Center (MWC) package 46
- ISDN Signaling (ISDN) package 145
- ISDN Primary Rate Access (PRI) package 146 or ISDN Signaling Link (ISL) package 147 (for system to system
- ISDN Network Service (NTWK) package 148
- Network Message Service (NMS) package 175
- Message Waiting Indication (MWI) package 219 (if connected to DMS for interworking)

Note:
Packages 40 and 45 are required only if ACD is used as the Message Center DN.

The following packages are also necessary:

- End-to-End Signaling (EES) package 10
- Integrated Message Service (IMS) package 35
- Basic ACD (BACD) package 40
- ACD package A (ACDA) package 45
- Message Center (MWC) package 46
- Command Status Link (CSL) package 77
- ISDN Signaling (ISDN) package 145
- ISDN Primary Rate Interface (PRI) package 146 or ISDN Signaling Link (ISL) package 147 (for system to system)
- ISDN Network Service (NTWK) package 148
- Network Message Service (NMS) package 175
- Message Waiting Indication (MWI) package 219 (if connected to DMS for interworking)

The following packages are required for an MWI tandem node:

- ISDN Signaling (ISDN) package 145
- ISDN Primary Rate Access (PRI) package 146 or
- 2.0 Mbit Primary Rate Interface (PRI2) package PRI2 or
- ISDN Signaling Link (ISL) package 147 (for system to system)
- ISDN Network Service (NTWK) package 148
- Message Waiting Indication (MWI) package 219 (if connected to DMS for interworking)

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 45: LD 17: Configure remote D-channel capability. on page 109
2. Table 46: LD 15: Enable Message Service. on page 109
3. Table 47: LD 23: Configure an ACD Group for the Message Center users in the remote switch. on page 110

4. Table 48: LD 11: Define the ACD Group as the Message Center DN for each phone. on page 110
5. Table 49: LD 15: Configure AC2 to insert ESN Access Code and PNI. on page 110
6. Table 50: LD 16: Configure PNI and INAC or INST. on page 111
7. Table 51: LD 90: Configure Home Location Code. on page 112
8. Table 52: LD 90: Configure Home NPA. on page 112
9. Table 53: LD 90: Configure Central Office Translation. on page 113

Table 45: LD 17: Configure remote D-channel capability.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Configuration record.
- ADAN	CHG DCH x	Change Primary D-Channel. x = 0-63
...		
- RLS	xx yy	Release ID of the switch at the far end of the D-channel interface (xx = systems, yy = DMS).
- RCAP	MWI XMWI	Add remote D-channel capabilities for MWI Remove remote D-channel capabilities for MWI

If the Message Center is on a system, it must be a Meridian Mail. No other messaging devices are supported for the system. The DMS can use Meridian Mail or other messaging devices (Octel) for its Message Center.

Table 46: LD 15: Enable Message Service.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	IMS	Integrated Message Service data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
- IMS	YES	Change Integrated Message System.
- IMA	YES	Enable Integrated Message System.

Table 47: LD 23: Configure an ACD Group for the Message Center users in the remote switch.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ACD	Automatic Call Distribution.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ACDN	xxxx	ACD Directory Number.
MWC	YES	ACD DN Message Center DN.
NCFW	xx ... xx	Message Center DN: • a public DN (10 digits) prefixed by an ESN Access Code. • an ESN number prefixed by an ESN Access Code Do not define an agent for this ACD group to allow for the automatic call redirection to the ACD Night Call Forward DN where the Message Center DN is defined.

Table 48: LD 11: Define the ACD Group as the Message Center DN for each phone.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	xxxx	Type of phone.
...		
FDN	x..x	Flexible Call Forward No Answer to Message Center DN
...		
EFD	x..x	Call Forward by Call Type—External No Answer to Message Center DN
EHT	x..x	Call Forward by Call Type—External Hunt to Message Center DN
HUNT	x	Hunt to Message Center DN
KEY	xx MWK x..x	Message Waiting key, where x..x is the Message Center DN.

Table 49: LD 15: Configure AC2 to insert ESN Access Code and PNI.

Prompt	Response	Description
REQ	NEW	Add new data.

Prompt	Response	Description
	CHG	Change existing data.
TYPE	NET	Networking Data.
...		
- AC2		Access Code 2. Enter call types (type of number) that use Access Code 2. Multiple call types can be entered. Default is to Access Code 1.
	NPA	E.164 National
	NXX	E.164 Subscriber
	INTL	International
	SPN	Special Number
	LOC	Location code
- ISDN	YES	Change ISDN options
- PNI	1–32700	Customer private identifier—unique to a customer. Within one network, use the same value for PNI in both the Customer Data Block (LD 15) and the Route Data Block (LD 16) in all PBXs.
...		
- HNPA	200- 999 1200- 1999	Home Number Plan Area Code defined in LD 90
- HNXX	100–9999	Prefix for the Central Office
- HLOC	100–999	Home Location Code (NARS)
- LSC	1–9999	1- to 4-digit Local Steering Code established in the Coordinated Dialing Plan (CDP). The LSC prompt only appears if user has a 5- or 6-digit dialing plan.

For ISDN Networking Features, such as NRAG, NMS and MWI, the originating switch must not use the digit manipulation (DMI) to insert the ESN Access Code. The ESN Access Code must be inserted at the terminating/tandem node through the INST prompt if it connects to the DMS in the Public Network.

Table 50: LD 16: Configure PNI and INAC or INST.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
...		

Prompt	Response	Description
- PNI	1–32700	Customer private identifier—unique to a customer. Within one network, use the same value for PNI in both the Customer Data Block (LD 15) and the Route Data Block (LD 16) in all PBXs.
- INAC	(NO) YES	Insert Access Code. Permit an ESN Access Code to be automatically added to an incoming ESN call from a private network. If INAC is YES, the digit insertion option (INST) is bypassed. This prompt only appears if the route type is a TIE trunk.
- INST	(0)–99999999	Digits to be inserted in front of leading digits. Use this prompt if route is used for connection to DMS.

Use "INST" in LD 16 at the system location A for incoming tandem/terminating calls. Use "INAC" at the system locations B and C. For the Message Center users on the system, configure Home Location Code and Home NPA to terminate a Facility message from the Message Center, either on the system or on DMS to the Message Center user's switch. The Facility message is for turning on/off the Message Waiting Indicator for the user.

For the private ESN Uniform Dialing Plan, use LD 90 to configure Home Location Code (HLOC).

Table 51: LD 90: Configure Home Location Code.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	NET	Network translation tables.
TRAN	AC1 AC2	Access Code 1. Access Code 2.
TYPE	HLOC	Home Location Code.
HLOC	xxx	Home Location Code (3–7 digits).

For the public numbering plan, a 10 digit number (NPA+NXX+XXXX) is used in the ORIG and DEST IE of the Facility message. Use LD 90 to configure Home NPA and Central Office Translation (NXX) to terminate the Facility message onto the Message Center user's DN.

Table 52: LD 90: Configure Home NPA.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.

Prompt	Response	Description
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	NET	Network Translation Tables.
TRAN	AC1 AC2	Access Code 1. Access Code 2.
TYPE	HPNA	Home NPA Translation.
HNPA	xxx	Home NPA.

Table 53: LD 90: Configure Central Office Translation.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	NET	Network Translation Tables.
TRAN	AC1 AC2	Access Code 1. Access Code 2.
TYPE	NXX	Central Office Translation.
NXX	xxx	Office code translation.
- RLI	0–255	Route list index.
- SDRR	LDID	Recognized local DID codes.
- - DMI	1–255	Digit manipulation table index. DMI should delete 3 digits.
- LDID	xxx	Local DID number recognized within the NPA and NXX.

Feature operation

MWI performs two basic operations:

- Activates the MWI at the caller's phone
- Deactivates the MWI at the subscriber's phone. Table 54: When MWI is activated on page 114 shows the sequence that activates the MWI. Table 55: When MWI is deactivated on page 114 shows the sequence that deactivates the MWI.

Table 54: When MWI is activated

Sequence	Caller	Receiver	Message Center
1	Calls receiver	Receiver not available	
2	Leaves a message		Records caller's message
3	Hangs up		Activates MWI on receiver's phone

Table 55: When MWI is deactivated

Sequence	Receiver	Message Center
1	Notices MWI	
2	Calls the Message Center	Plays messages
3	Clears the mailbox	
4	Hangs up	Deactivates MWI on receiver's phone

Some of the failures that can occur and how MWI handles those failures are as follows:

- AML/CSL link failure

  If the AML/CSL link fails between Meridian Mail and its host system, calls are redirected to the ACD Night Call Forward DN for the ACD queue involved.

- D-channel failure

  If the D-channel is out of service, the Facility message is lost. For Meridian Mail, an MWI CSL message is sent to the Meridian Mail server.

- Inconsistent data base

  If the Facility message that toggles MWI cannot be delivered to the caller's phone because the DN is invalid or MWI is not supported in the remote switch, an MWI CSL message is sent to Meridian Mail.

Chapter 11: MSDL Idle Code Selection

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

When a T1 carrier is disabled at the remote end, the remote T1 or ISDN PRI hardware raises a "Red Alarm" status and sends a "Yellow Alarm," to the local (near end) system, which takes all trunks and channels out of service, and responds to the remote end by sending an "Unassigned PCM" (FF) code. However, some switches do not recognize the "Unassigned PCM" code, and instead expect an "Idle PCM" (7F) code.

The Idle Code Selection feature allows a system, upon receiving a "Yellow Alarm" condition from the remote end with a disabled T1 carrier, to be configured to respond by sending an "Idle

PCM" code instead of an "Unassigned PCM" code. Therefore, a remote switch, such as a Lucent 5ESS, which expects to receive an "Idle PCM" code can be cleared of a Red Alarm, the system can be cleared of a Yellow Alarm, and trunks and channels can be brought back into service.

The craftsperson should confirm that the remote end supports the "Idle PCM" code, before configuring this feature on a loop.

The Idle Code Selection is an enhancement to the existing DTI (package 75) and PRA (package 146) packages.

Figure 10: System response to Yellow Alarm condition prior to Idle Code Selection feature on page 117 shows the existing operation, where the system responds to the remote end only with an "Unassigned PCM" code.Figure 11: System with Idle Code Selection feature responding to Yellow Alarm condition on page 118 shows the enhancement made by the Idle Code Selection feature, where the system responds with either the "Unassigned PCM" code or the "Idle PCM" code, depending on how the loop has been configured, as described in Feature implementation on page 119.

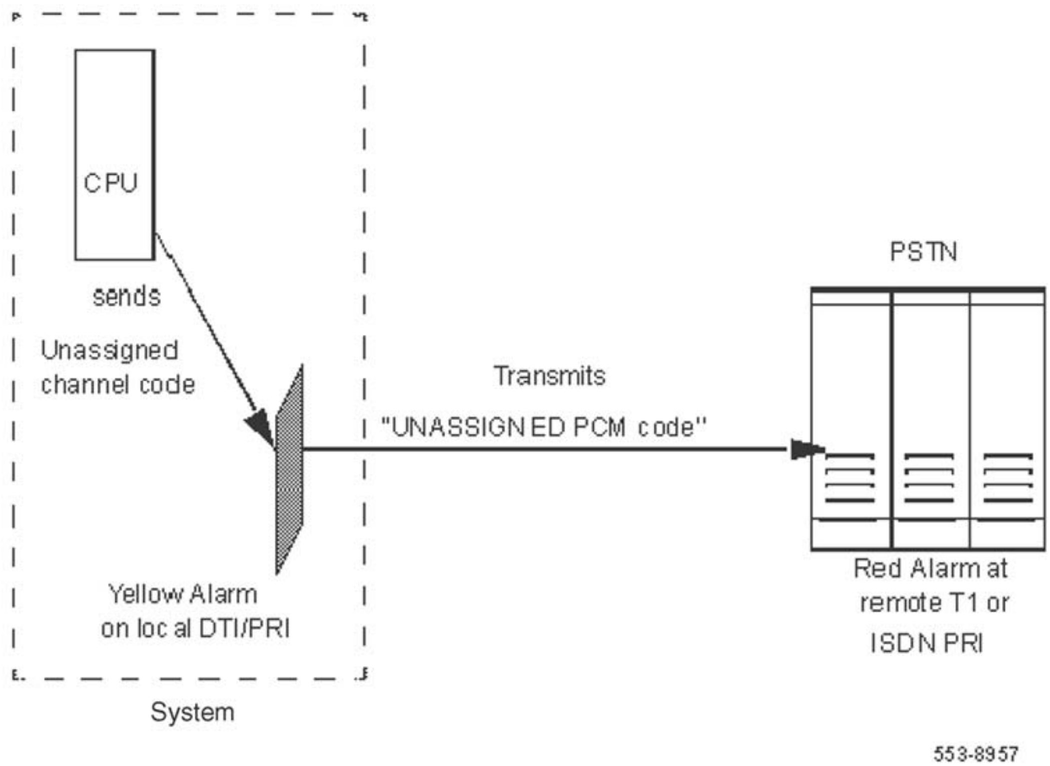

Figure 10: System response to Yellow Alarm condition prior to Idle Code Selection feature

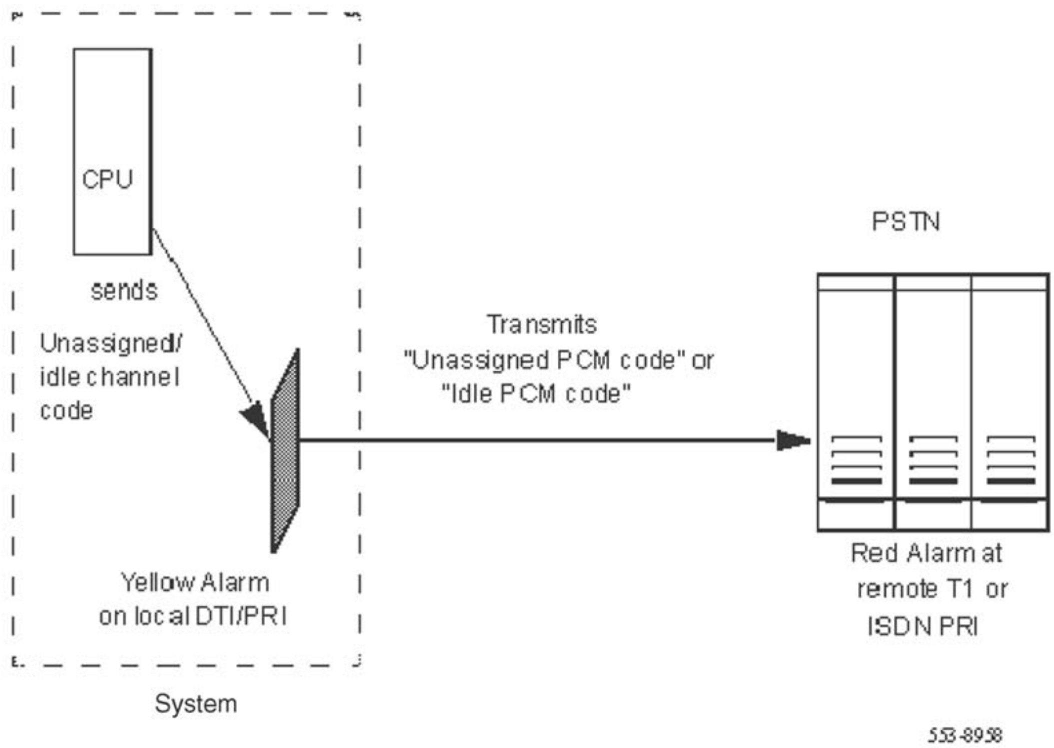

Figure 11: System with Idle Code Selection feature responding to Yellow Alarm condition

Operating parameters

This feature applies to DTI and PRI (1.5 Mb) only and not to DTI2 nor PRI2.

Feature interactions

Idle Code Selection, as an addition to the existing DTI (package 75) or PRA (package 146) packages, does not add any additional feature interactions.

In the following cases, when modifying or deleting loops, a new SCH warning message will be output, indicating that "ICS data associated with the loop is removed."

- when changing the IFC type of a PRI loop that has ICS data associated with it and,
- when removing a DTI/PRI loop that has ICS data associated with it.

Feature packaging

Idle Code Selection is not a separate package, but is an enhancement to the existing DTI (package 75) and PRA (package 146) packages. Idle Code Selection requires either the DTI or PRA package. ISDN package 145 is required for ISDN.

Feature implementation

Task summary list

The following is the task in this section:

Table 56: LD 73: Activate (or deactivate) a loop to send Idle PCM code. on page 119

Table 56: LD 73: Activate (or deactivate) a loop to send Idle PCM code.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	DDB	Digital Data Block
...	...	
SRMM	1-(2)-127	Slip Rate Maintenance Maximum.
ICS	0-159 0-63 (Xnnn)	Idle Code Selection loop number For Large Systems to deactivate the feature on loop xxx.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 12: MSDL Port Overload Counter

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The MSDL Port Overload Counter feature provides the capability of locking out individual MSDL ports when incoming messages through a port exceed or equal the port overload threshold of 200 messages in a two-second time period.

When any of the four ports on the MSDL card reaches the port overload threshold it is locked-out, but the operation of other ports on the MSDL card will not be affected.

The MSDL card is still subject to a card overload threshold, which will cause a lock-out if it receives 300 or more messages for every two seconds. However, when an individual MSDL port becomes overloaded, the messages to that port are subtracted from the total card messages used in performing the card overload check. Furthermore, port overload checks have priority over card overload checks.

The overloaded port on the MSDL card is locked-out so that the card stops responding to the incoming messages from the overloaded port. This prevents the CPU from servicing a very high incoming message rate from the port, which could cause system degradation.

Figure 12: MSDL card lock-out on page 123 shows the existing MSDL card lockout, whileFigure 13: MSDL port overload check preceding card overload check on page 123 shows the port lockout functionality introduced by the Port Overload Counter feature. Figure 13: MSDL port overload check preceding card overload check on page 123 demonstrates a port overload check being performed before a card overload check.

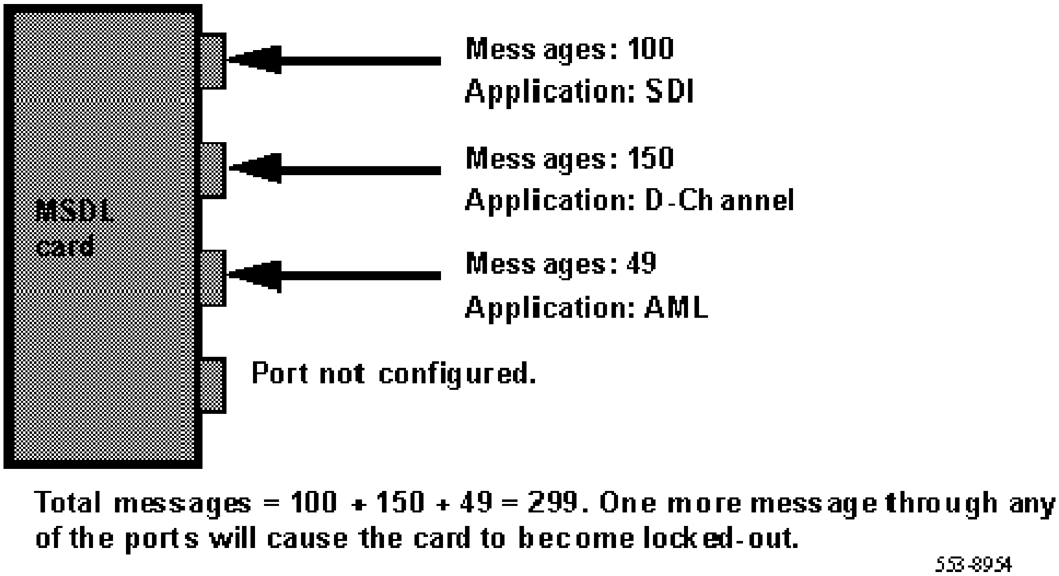

Figure 12: MSDL card lock-out

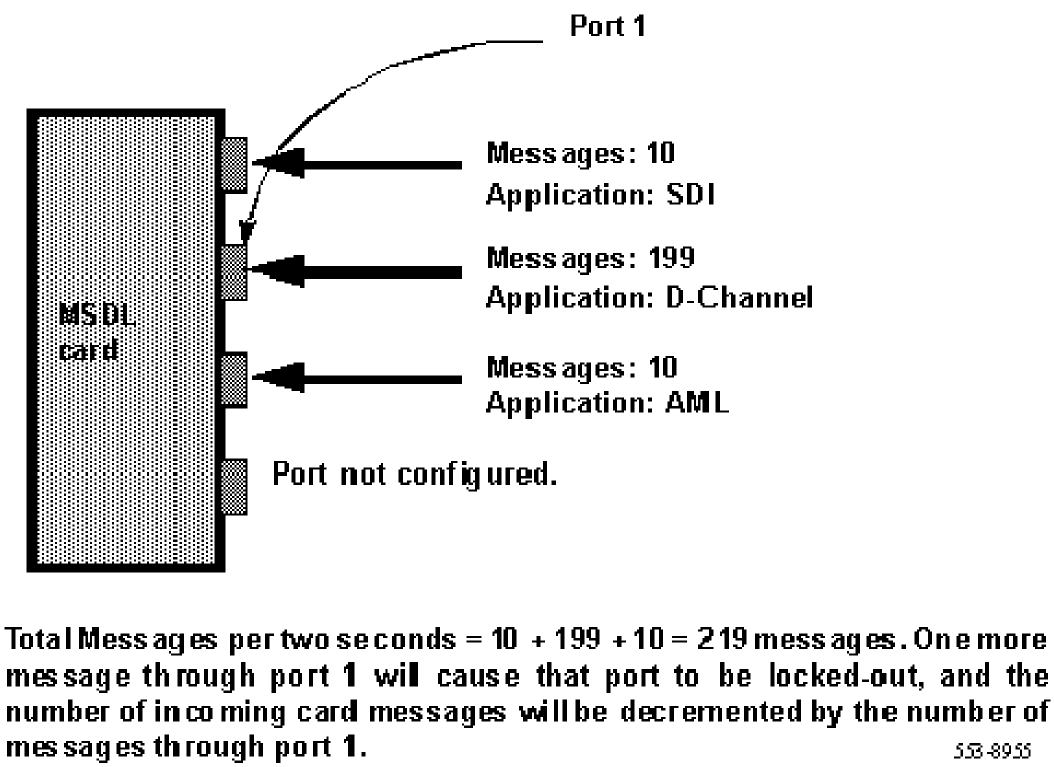

Figure 13: MSDL port overload check preceding card overload check

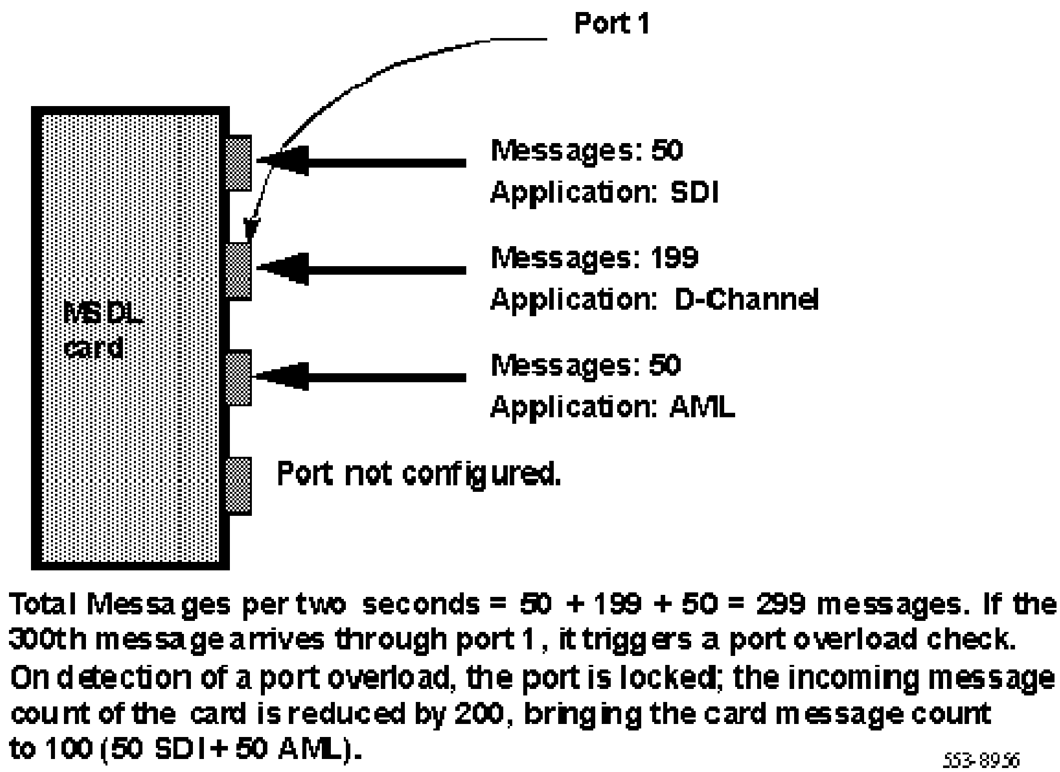

Figure 14: MSDL port overload check preceding card overload check

Operating parameters

There are no operating parameter specified for this feature.

Feature interactions

MSDL/MISP Interface Handler (MMIH)

The MMIH provides a software interface between the MSDL/MISP card and the system software, and allows applications on the MSDL/MISP card to access each other through the interface.

Previously, the interface software maintained a counter of incoming messages on an MSDL application basis. When the sum of all messages received indicated an excessive incoming message rate, the MSDL card was locked-out.

The Port Overload Counter feature modifies the MMIH so that incoming message counters are maintained for individual MSDL ports

This feature changes the functionality of the MMIH for an MSDL card, but the MISP remains unchanged.

DCH/SDI/AML Application

The Port Overload Counter feature changes the DCH/SDI/AML Application to cause the MSDL port to lockout when the incoming messages exceed the Port Overload threshold value.

B-Channel Overload Control (BCOC)

This feature has no interaction with the B-Channel Overload Control Feature.

MISP

This feature does not change the functionality of the MISP card interface.

Feature packaging

This feature requires package MSDL Card Package, package 222.

Feature implementation

There are no specific implementation procedures for this feature. However, as described in Maintenance and Diagnostics on page 126, modifications have been made to overlay maintenance and diagnostic commands.

The feature is activated whenever a configured application on an MSDL card is active and is receiving messages through the active port.

Feature operation

No specific operating procedures are required to use this feature.

Maintenance and Diagnostics

The Port Overload Counter feature has made the following modifications to overlay maintenance and diagnostic commands:

Table 57: LD 37: I/O Diagnostic.

Commands	System Responses	Description
STAT MSDL xx (Where xx = physical MSDL number)	MSDL xx: ENBL SDI 7 OVLD PORT 0 DCH 11 OVLD PORT 1 AML 12 OVLD PORT 2	Display the status of ports on a card. The status includes overloaded ports.
STAT TTY xx (Where xx = logical SDI number)	TTY xx: OVLD	Display the status of an overloaded MSDL port running an SDI application.
ENL TTY xx Where xx = logical SDI number)	IOD_xxx	Failed to enable the SDI on MSDL port xx. Refer to Overloaded MSDL port running an SDI Application on page 128.

Table 58: LD 48: Link Diagnostic.

Commands	System Responses	Description
STAT MSDL xx (Where xx = physical MSDL number)	MSDL xx: ENBL SDI 7 OVLD PORT 0 DCH 11 OVLD PORT 1 AML 12 OVLD PORT 2 (Where xx = physical MSDL number)	Display the status of ports on a card. The status includes overloaded ports.
STAT AML a (Where xx = logical AML number)	AML: xx MSDL: yy PORT: zz DES: LYR2: OVLD (Where xx = logical AML number, yy = physical MSDL number, and zz = MSDL port)	Display the status of an overloaded MSDL port.
ENL AML xx (Where xx = logical AML number)	CSA_xxx	Failed to enable AML link. Refer to Overloaded MSDL

Commands	System Responses	Description
		port running an AML Application on page 127.

Table 59: LD 96: PRI D Channel Diagnostic

Commands	System Responses	Description
STAT MSDL xx (Where xx = physical MSDL number)	SDI 7 OVLD PORT 0 DCH 11 OVLD PORT 1 AML 12 OVLD PORT 2	Display the status of ports on a card. The status includes overloaded ports.
STAT DCH xx (Where xx = logical D Channel number)	DCH xx: OVLD DES:	Display the status of an overloaded MSDL port running a D Channel Application.
ENL DCH xx (Where xx = logical D Channel number)	DCH_XXX	Failed to enable the D Channel. Refer to Overloaded MSDL port running a DCH Application on page 127.

Fault Clearance Procedures

Overloaded MSDL port running a DCH Application

Cause: The system received an excessive number of messages (equal to or greater than 200 messages in a two second time period) from the MSDL port.

To clear the fault: Manually disable the D-Channel in LD 96 using the command DIS DCH xx, where xx is the D-Channel number. Enable the D-Channel using LD 96 using the command ENL DCH xx.

Overloaded MSDL port running an AML Application

Cause: The system received an excessive number of messages (equal to or greater than 200 messages in a two second time period) from the MSDL port.

To clear the fault: Manually disable the AML Link in LD 48 using the command DIS AML xx, where xx is the AML Link number. Enable the AML Link using LD 48 using the command ENL AML xx.

Overloaded MSDL port running an SDI Application

Cause: The system received an excessive number of messages (equal to or greater than 200 messages in a two second time period) from the MSDL port. One scenario of the overloaded SDI port is the case of a smart-modem setup for "smart" vs. "dumb" mode. The system and the modem can be bouncing the same messages back and forth until the 200 port message threshold is reached.

To clear the fault: Manually disable the link in LD 37 using the command DIS TTY xx, where xx is the SDI number. Enable the AML Link using LD 37 using the command ENL TTY xx.

Chapter 13: MSDL Status Enquiry Message Throttle

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

When a D-channel recovers from data link failure, in a system to system network interface, the "network" (master) side of the "network" side to "user" (slave) side interface sends a Status Enquiry message to the "user" side, for every established B-channel, to request the call state.

The Status Enquiry Message Throttle feature regulates the sending of Status Enquiry messages, by limiting the Status Enquiry messages sent within a 128 millisecond time period.

The Network side of the interface uses a fixed number of Status Enquiry messages that is configurable for each D-channel through a Status Enquiry Message Throttle (SEMT) parameter in LD 17.

By reducing the number of Status Enquiry messages sent in a given 128 msec time period, this feature improves the amount of network congestion experienced after a D-channel recovers from data link failure. This also frees up some timeslots for call processing.

By default the SEMT parameter is 1. The valid input range is 1 to 5.

Operating parameters

This feature applies to DTI and PRI (1.5 Mb) only and not to DTI2 nor PRI2.

This feature supports both the NT6D80 Multi-Purpose Serial Data Link (MSDL) card and the NT5D12 Dual Port DTI/PRI card with the Downloadable D-channel daughterboard for DDP (NTBK51AA/NTBK51CA). ISDN PRI and ISL interfaces are supported.

This feature applies only to system to system interfaces (MCDN inter-networking).

The new prompt, SEMT, only applies to the "network" side interface of the system to system network.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature requires the following packages:

- ISDN Signaling (ISDN), package 145
- ISDN Primary Rate Access (PRA), package 146, or
- ISDN Signaling Link (ISL), package 147
- Multi-Purpose Serial Data Link (MSDL), package 222

Feature implementation

Table 60: LD 17: Configure the Status Enquiry Message Throttle (SEMT) parameter.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CEQU	All input/output devices.
ADAN	aaa DCH xx	Primary D-channel number. Where: aaa = NEW or CHG. xx = 0-63 (For Large Systems)
CTYP	MSDL	Multipurpose Serial Data Link card.
GRP	0-4	Network Group number for Large Multi-Group Systems.
DNUM	0-15	Device number for I/O ports. All ports on the MSDL card share the same DNUM. The MSDL card address settings must match the DNUM value.
PORT	0-3	Port number for the MSDL card.
USR	PRI	Primary Rate Interface. D-channel for ISDN PRA only.
IFC	SL1	SL-1 interface (Meridian 1, CS 1000M)
DCHL		D-channel PRI loop number. Where:
	0-159	For Large Systems
...	...	
OTBF	1-(32)-127	Output Request Buffer
DRAT		D-channel Transmission Rate
SIDE	NET	Network, the controlling switch.
SEMT	(1)-5	Number of Status Enquiry messages sent within 128 msec from the Network side.
RLS	xx	Release ID of the switch at the remote (far) end of the D-channel.

Table 61: MSDL/Daughterboard card system commands on page 132 lists commands for getting the status, enabling, and disabling the MSDL card or Downloadable D-channel Daughterboard card.

Table 61: MSDL/Daughterboard card system commands

Command	Response
STAT MSDL xx	Get status of the newly configured MSDL card. Where: • xx = device number (DNUM) entry for newly configured MSDL card. • xx = Card slot number (CDNO) for the NTBK51AA/ NTBK51CA Downloadable DCH Daughterboard. The card status is output and can be any one of the following: MSDL xx: ENBL MSDL xx: MAN DSBL MSDL xx: SYS DSBL reason **Note:** The "MSDL xx: SYS DSBL reason" message indicates that maintenance is required by the craftsperson and installation can only continue when reason is corrected. Refer to *LD 48 Alphabetical list of commands* "STAT MSDL (x [FULL])" command for a complete list of reasons.
DIS MSDL xx	Disable the MSDL device if Stat command indicates MSDL is in enabled state.
ENL MSDL xx FDL	Enable the MSDL card. Where: xx = D-channel number configured in LD 17. Enabling the MSDL card with this command is only permitted if the card is currently in the Manually Disabled state. **Note:** A series of dots (".") are output which indicate that software download is in progress. Following the download the card will be enabled.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 14: National ISDN 2 TR-1268 Primary Rate Interface

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

This feature is only available in North America. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

The National ISDN-2 TR-NWT-001268 Primary Rate Interface (PRI) feature provides an Integrated Services Digital Network (ISDN) PRI interface to the Public Exchange/Central Office that conforms to portions of the National ISDN-2 (NI-2) specification as developed by the National ISDN users Forum (NIUF) and documented in Bellcore Specification TR-1268.

The system supports the following call services on the NI-2 interface:

- Basic call service
- Circuit-mode bearer capabilities (speech, 3.1 kHz audio, 64 Kbit/s digital, and adapted 56 Kbit/s to 64 Kbit/s digital)
- Enbloc sending
- Channel negotiation
- In-band tone and announcement
- Calling number delivery
- Calling Party Number Privacy, using the Calling Party Name feature (*67)
- A back-up D-channel is provided to improve the reliability of an ISDN PRI interface that consists of more than one Digital Signal Level 1 (DS1) facility. The primary and back-up D-channels reside on the 24th channel of separate DS1 facilities. Both D-channels provide signaling information for the interface, but only one can be in service at any given time.

The system does not support the following TR-1268 functionalities:

- Packet Mode Unrestricted Digital Information bearer capability
- Circuit Mode Unrestricted Digital Information at n x 64 Kbit/s, H0 and H11 channels bearer capability (due to the lack of hardware support of providing contiguous timeslots)
- Up to two Calling Party Number information elements for terminating calls
- Up to two redirecting numbers provided for originating and terminating calls
- Subaddressing
- Calling party number privacy on subscription basis
- Call-by-Call Service Selection, and
- Switched DS1/Switched Fractional DS1 Service.

Operating parameters

The existing Network Call Redirection limitation on unsupported interface applies to the NI-2 interface. The NI-2 interface generates the Redirecting Number (RN) Information Element (IE) of the most recent instance of redirection of an internal call forward call. If the system receives an RN IE at the NI-2 interface, it passes it along. If there are more than one RN IEs, the later ones are treated as duplicates and are discarded.

A maximum of 16 DS1 loops can be supported when both the primary and backup D-channels are configured (that is, 16 x 24 - 2 = 382 B-channels); however, the system is limited to 254 trunks in a single route. Stepping to a second route is permitted only if the system is supported by a far end switch.

The ISDN NI-2 TR-1268 PRI feature requires a DTI/PRI card and a D-channel Handler card.

Feature interactions

Integrated Service Access (ISA)

Integrated Service Access is not supported on this interface.

ISDN Signaling Link (ISL)

ISDN Signaling Link is not supported on this interface.

Feature packaging

The ISDN NI-2 TR-1268 PRI Basic Call feature is contained in North American National ISDN Class II Equipment (NI2) package 291.

The following packages are also required to activate this feature:

- Integrated Services Digital Network (ISDN) package 145
- 1.5 Mbit Primary Rate Access (PRA) package 146
- Multi-purpose Serial Data Link (MSDL) package 222

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 62: LD 17: Configure the primary D-channel. on page 136
2. Table 63: LD 17: Configure the backup D-channel. on page 136
3. Table 64: LD 16: Use this overlay to define a route data block (for ISDN PRI). on page 137

The following two service changes are required for this feature: define a new interface type for a given D-channel; and define the download.

Table 62: LD 17: Configure the primary D-channel.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	CFN	Configuration Record.
ADAN	NEW CHG OUT DCH xx	Add, change, or remove primary D-channel.
CTYP	MSDL	Supported only on Multi-purpose Serial Data Link (MSDL) or Downloadable D-channel cards.
…		
USR	PRI	D-channel mode.
IFC	NI2	NI-2 TR-1268 interface type.
CO_TYPE	(STD) ATT	Central Office switch type (prompted only if IFC = NI2). STD = Totally compatible with Bellcore standard. ATT = AT&T 5ESS.
PRI	lll nn	lll = PRI loop using the same D-channel (0,1,...159) nn = Interface identifier (2,3,...15)

Table 63: LD 17: Configure the backup D-channel.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	CFN	Configuration Record.
ADAN	NEW CHG OUT BDCH yy	Add, change or remove backup D-channel data.
PDCH	xx	Associated primary D-channel.
CTYP	MSDL	Card type.
…		

Table 64: LD 16: Use this overlay to define a route data block (for ISDN PRI).

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route data block.
…		
DGTP	PRI	Digital route type.
IFC	NI2	New DCH interface ID.

Feature operation

No specific operating instructions are required to use this feature.

Chapter 15: Network ACD

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Network ACD allows call centers with multiple locations to solve the problem of fluctuating call traffic. The Network ACD feature uses Integrated Services Digital Network (ISDN) to efficiently and quickly route calls to available agents within a network of systems. Using the timed overflow routing tables associated with ACD, customers can specify ACD-DNs within the system network to which calls should be directed.

NACD is cost effective because calls remain in queue at their original location while waiting for an agent to become available in either the source queue or one of the target queues located throughout the network. Only when an agent becomes available in a remote queue will the call actually be sent over an ISDN voice channel. Prior to the call being sent, communication between locations is handled through the ISDN D-Channel.

The management report information on package C reflects the changes introduced by the NACD feature.

ACD-MAX supports the NACD feature. Three new reports and three additional management displays are provided to allow customers to determine call traffic patterns and service levels throughout the network. Centralization of this information will be provided with the introduction of the Network Administration Center. Network Administration Center requires an ACD-MAX in each network location and provides reports and displays on the entire NACD environment.

For correct display on ACD-MAX, NACD supports only a UDP numbering plan. CDP will be supported at a later date. It is important to note that the system regular users can operate using one dialing plan (i.e. CDP or UDP) while the NACD operates using another numbering scheme (i.e. UDP with location codes).

Operating parameters

This feature is currently incompatible with the similar Network ACD feature on the SL-100.

NACD is not supported on Package D, PDP 11 - Generic 9000 software.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature requires Network Automatic Call Distribution (NACD) package 207. The following packages are also required:

- Basic Routing (BRTE) package 14
- Digit Display (DDSP) package 19
- Basic Queuing (BQUE) package 28
- Network Class Of Service (NCOS) package 32
- Network Signaling (NSIG) package 37
- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution, Package B (ACDB) package 41
- Automatic Call Distribution, Package A (ACDA) package 45
- Automatic Answerback (AAB) package 47
- Network Alternate Route Selection (NARS) package 58 or
- Coordinated Dialing Plan (CDP) package 59
- Flexible Call Back Queuing (FCBQ) package 61

- 1.5 Mbit Digital Trunk Interface (PBXI) package 75 or
- 2.0 Mbit Digital Trunk Interface (PBXI) package 129
- Timed Overflow Queuing (TOF) package 111
- Integrated Services Digital Network (ISDN) package 145
- International Primary Rate Access (PRI) package 146 or
- 2.0 Mbit Primary Rate Access (PRI2) package 154 or
- ISDN signaling Link (ISL) package 147
- Advanced ISDN Network Services (NTWK) package 148
- ACD Enhanced Overflow (EOVF) package 178

Feature implementation

There are no specific implementation procedures for this feature.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 16: Network Application Protocol Link Enhancement

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

This enhancement of the ISDN Network Application Protocol (ISDN NAP) feature for Meridian Mail services provides improved fault-detection responses. When a NAP link fails, a predefined time period is allowed to pass before the link is declared 'out-of-service'. Restoration of the link within this recovery time period will result in uninterrupted service.

The signaling from the caller's phone is ignored during the link failure. However, calls which were already established will remain established during the recovery period. Should the link be declared 'out of service', only those established calls which use trunks without disconnect supervision will not be maintained. (Such calls will be requeued to the front of the waiting queue.)

When a link is in the recovery period, calls ringing to an agent are held in the ringing state, until either the recovery period ends or the link is reestablished. Incoming calls requiring Meridian Mail services are placed in the ACD queue, linked to an agent (if possible) and given ringback tone.

When a link is declared 'out of service', calls which are ringing at an agent are requeued. Requeued calls and incoming calls on the out-of-service link receive night-service treatment.

Normal operations resume when the link is restored.

Operating parameters

This feature applies only to the ISDN environment.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature requires the following packages:

- ISDN Application Protocol Link for Third-party Vendors (IAP3P) package 153, which is dependent on
  - Basic Automatic Call Distribution (BACD) package 40

Feature implementation

There are no specific implementation procedures for this feature.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 17: Network Attendant Service

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Network Attendant Service (NAS) provides stand-alone attendant capabilities throughout a network. Any node in the network can have its attendant services located part-time or full-time at any other node in the network.

The activation of Network Attendant Service is controlled by the NAS key on the Attendant Console. When a call is presented to an attendant and the NAS key is not activated, the call receives normal attendant service. If the NAS key is activated, the call receives alternate treatment, based on one of the NAS conditions described below.

Network Attendant Service schedule

The NAS schedule allows a prioritized list of attendant alternatives (attendant locations) to be defined for up to 31 half-hour time periods. Each period can have up to four alternate attendants defined against it. During one of these time periods, a request for attendant service will use one of the alternatives, according to the specified order - the first attendant alternate is attempted, and if all attendants are in Position Busy, the following alternate in the sequence is attempted, and so on.

If none of the attendant alternatives are available, an attempt is made to give local attendant service, which can lead to the application of local NIGHT service.

Night Service

Night Service treatment is defined individually for each node.

With the introduction of NAS routing, identifying whether or not a system is in Night Service becomes more complex.Table 65: Determination of Night Service on page 146 shows when Night Service treatment is in effect. When all the conditions in a vertical column are met, the system is considered to be in Night Service.

Table 65: Determination of Night Service

Local Attendants exist	No	No	No	Yes	Yes	Yes
Local Night active				Yes	Yes	Yes
NAS key active	No	Yes	Yes	No	Yes	Yes
No alternatives in current NAS schedule		Yes			Yes	
All alternatives in current NAS schedule tried			Yes			Yes

Status of local attendants

When NAS routing is active and there is an available attendant at the local switch, the call terminates at the local attendant, if one is available. If a local attendant is not available, the call can either be placed in the local attendant queue (if the Call Waiting threshold has not been exceeded and the console Call Waiting lamp is not flashing), or can receive local NIGHT service.

Alternate routing to attendant positions

Calls can be routed from one attendant to another attendant location in the network. Each node can be programmed with the attendant DNs for up to seven other switches. Up to four of these seven attendant DNs can be used as alternatives for any one time period. Each of the four attendant alternatives for each time period can have Drop Back Busy and/or Off-hook Queuing options configured.

If a call is to be routed to an alternate attendant at another node and all trunks to the other node are busy, the call is queued for an available route to the alternate (if the alternate has the Off-hook Queuing feature). The call remains queued for a specified time, which, upon expiring, causes the call to be directed to the next alternate attendant.

The operation of NAS routing, as controlled by the activation of the NAS key, is summarized in Table 66: NAS Routing Possibilities on page 147.

Table 66: NAS Routing Possibilities

	NAS Key	Home Attendant	Night Key	CW Lamp	Trunks to Remote	Action
1	Dark	All Busy	Dark	X	X	Queue to Home Attendant
2	Dark	Not Busy	Dark	Dark	X	Select Home Attendant
3	Dark	X	Lit	X	X	Route to Home Night
4	Lit	Not Busy	Dark	Dark	X	Select Home Attendant
5	Lit	All Busy	Dark	No Flash	X	Queue to Home Attendant
6	Lit	All Busy	Dark	Flash	Not Busy	Route to Remote Attendant
7	Lit	All Busy	Dark	Flash	All Busy	Queue to Home Attendant
8	Lit	X	Lit	X	Not Busy	Route to Remote Attendant
9	Lit	X	Lit	X	All Busy	Queue to route

Drop Back Busy

When a call reaches a Remote node, no attendant is available, and NAS routing or Night Service at that switch is about to be performed (if the Drop-back busy option was set at the originating switch and sent with the call), the call is treated by the originating switch as though no attendant is available at the Remote switch. Another alternative is selected from the originating switch.

Note:

Drop Back Busy (DBB) and Remote Virtual Queuing (RVQ) are both packaged under the Originating Routing Control/Remote Virtual Queuing (ORC-RVQ) package 192. If RVQ and DBB are both configured, DBB will take precedence over RVQ. If the user wishes to activate RVQ, DBB must be disabled for a route entry in response to the IDBB prompt. If the user wishes to activate DBB, it must be enabled by entering DBI or DBA.

Attendant Off-hook Queuing

During peak periods a call can be prevented from reaching a remote attendant if all possible routes to that attendant are busy. If these routes have off-hook queuing, the call will queue on these routes. If activated in the NAS programming and on the route list for the call, queuing occurs before the system attempts other alternatives. The alternatives are tried after the Off-hook Queuing (OHQ) timer expires.

Network Attendant Service capabilities

The following sections describe the network capabilities that are offered as part of NAS.

Break-in

The Break-in feature allows an attendant to enter an established call anywhere in the network and to offer another call or important message to one of the parties involved in the call. Break-in is provided as a key (BKI) function. The BKI key can be pressed before dialing the DN of the required station (pre-dial) or after (post-dial).

When the BKI key is pressed, the following situations can exist:

- Break-in request recognized — this is a temporary processing state, that occurs when an attendant tries to break-in to a party at another node, and lasts until the signaling protocol for the break-in attempt is completed.
- Break-in ignored — this state occurs if the required party has disconnected at the point of break-in, is idle without the Make Set Busy or Do Not Disturb features active, or is idle with the Call Forward feature active. In all cases, the party is rung, and the attendant can extend the call.
- Break-in allowed — the attendant can break into the required party, consult with the required party, and extend another call to the party if (a) the source is an external call, (b) Camp-on is available on the required party, and (c) the established call is a basic call.
- Break-in denied — break-in is not allowed if any of the above conditions are not met.
- Break-in temporarily denied — the attendant temporarily cannot break-in to the required party, but can try again later. This situation occurs if:
    - the required party is dialing, involved in a consultation call, or is on hold
    - the required party's phone is ringing or receiving an indication tone
    - the required party's phone is connected to a paging, dictation, recorded announcement, or integrated voice messaging trunk
    - the party to be extended is a local party or trunk with warning tone denied Class of Service
    - network blocking to a remote node has been encountered
- Break-in consult only — the attendant can break into the required party, and can consult with the party but cannot extend another call. This situation occurs if:
    - the attendant originates the call
    - the source is an internal call

- the source is an external call and neither Camp-on nor Call Waiting is possible on the required party
- the attendant attempts a pre-dial break-in and the required party is busy with Call Forward active.

Call extension

Restrictions that apply to attendants at local nodes also apply to calls extended across the network to remote node attendants.

Attendant control prevents the calling phone from disconnecting until the attendant releases. Once the attendant releases or extends and releases the call, attendant control is relinquished.

Timed reminder recalls

Timed reminder recalls are attendant-extended calls that return to the attendant when their timers expire. The timers apply to slow answer calls, camped on calls, and call waiting calls.

When the attendant extends the call to a party at another node, the trunks between the attendant and the source and the attendant and the destination are not taken down after the Release key is pressed. This is true even if tromboning has occurred. This allows the attendant node to monitor the outgoing trunk for an answer signal. If no answer signal occurs within the specified time, the call is presented again to an attendant (or to the original attendant, if Recall to Same Attendant is active on the attendant node).

Anti-tromboning is only invoked after the destination has answered and the attendant has released from the call.

Incoming Call Indication

The Incoming Call Indicators (ICI) will operate in the same manner as a stand-alone system for incoming calls from stations or trunks.

New ICI types are introduced for NAS routed calls for each trunk type. The indicators can be the following:

- a dial 0 call (ordinary or fully restricted)
- a recall request
- a line lockout intercept
- Call Redirection (Call Forward No Answer, Call Forward Busy)
- an interpositional call
- a Listed Directory Number (LDN)

- a Message Center call
- NAS trunk types (type of trunk on which the call came into the originating switch. The choices are: NDID, NCO, NTIE, NFEX, and NWAT)

Attendant Display

Three features which pass information useful for attendant display are:

- Calling Line Identification (CLID)
- Network Call Party Name Display
- Network Call Redirection

For incoming calls, the CLID received (if available), is displayed instead of the Trunk Route Access Code and Trunk Member Number. If the call comes from the private ISDN network and there is a name associated with the calling phone, the name is displayed on consoles with alphanumeric displays.

Reason for redirection codes are displayed if the call has been redirected by a feature such as Call Forward All Calls.

Camp-on and Call Waiting

Both Camp-on and Call Waiting allow calls extended to a busy phone a further opportunity to reach that phone. If the call is extended across the network to a busy phone, Camp-on or Call Waiting can be attempted in the same manner as in the stand-alone case.

Tenant Service

If Multi-Tenant (TENS) software package 86 is equipped, the table number in the NAS overlay programming can be referenced to an individual Console Presentation Group. Each tenant can have its own individual NAS routing programmed.

Centralized Attendant Service vs. Network Attendant Service

NAS has some similarities to a previous non-ISDN application called Centralized Attendant Service (CAS). There are significant differences as well.

Note:

NAS and CAS cannot be configured on the same system.

Centralized Attendant Service

- Allows attendants to be centralized at one Main switch connected to Remote switches with Release Link Trunks (RLTs).
- When a remote switch has the CAS feature key activated, incoming calls to the Remote switch are redirected to the Main switch where an attendant answers the call.
- The call comes into the Main switch on an RLT. The attendant can extend the call back to a phone at the Remote switch. The call is routed on the same RLT trunk which was used when the call came into the Main switch.
- Once the call is ringing at the phone, the RLT trunk is released.
- If the phone goes unanswered, the call recalls to the attendant at the Main switch. A Release Link Trunk is used for the recall.
- The CAS feature is activated using a key on a proprietary phone or console at the Remote switch.
- When users at different switches call each other or the attendant places a call to another switch, normal TIE trunks are used.

Network Attendant Service

- NAS allows several switches to have attendants who answer calls which have been redirected by the NAS feature. The switches are connected with Primary Rate Interface (PRI) or ISDN Signaling Link (ISL) connections.
- NAS routing allows a call destined for the local attendant to be diverted to a Remote attendant. This routing is governed by a NAS schedule, a NAS key, or a permanent NAS Active setting which can be programmed.
- NAS calls can result in tromboned trunk connections between the Remote switch and the Attendant switch. These connections remain until the ringing phone answers the call. This can result in two tromboned TIE trunks or channels being held up while a phone is ringing.
- If anti-tromboning has been programmed, the tromboning is corrected after the phone is answered.
- If the phone goes unanswered, the call recalls to the attendant at the Main switch. A PRI channel or ISL trunk is used for the recall.
- A NAS key can be programmed as an option on an Attendant Console.
- NAS calls and normal user calls all use the same PRI/ISL trunks.

There are three additional differences between NAS and CAS:

- NAS routing is used when calls waiting in the local attendant queue exceed one of two thresholds. CAS routes all calls to the Main CAS switch.
- NAS chooses an attendant from up to four alternatives for each time period. With CAS, each Remote site has only one Main switch to which to route calls.
- NAS routing can also be based on the status of trunks to other nodes and Night Service indicator status. These factors do not affect call routing with CAS.

Operating parameters

NAS and the Centralized Answering Position (CAP) capability are mutually exclusive. A system can not have an actual attendant console. Instead, the system can be configured to use a Centralized Answering Position (using a Meridian 2616 digital phone.) The CAP Directory Number (DN) is the customer Night DN. Since no attendant is configured, the customer is viewed to be in Night Service and any calls for the attendant are directed to the CAP.

Note:

An attendant answering position must be an attendant console, and not a Meridian digital phone.

NAS and Centralized Attendant Service packages are mutually exclusive and can not be packaged together.

NAS and Attendant Overflow Position packages are mutually exclusive and can not be packaged together.

Trunk Group Busy applies only to trunk groups on the node where the attendant resides.

The Uninterrupted Line Connection feature continues to work on a stand-alone switch basis; however, Network-wide Break-in, based on warning tone Class of Service, cannot be guaranteed. Only one Attendant at a time is allowed to break into a connection. Break-in is allowed for phones only, not trunks or other attendants. Attendant Control is not provided if the connection is a result of a Network Break-in.

Unsupported features

NAS does not support:

- Supervisory Console
- Charge Account
- Do-Not-Disturb and Group Do-Not-Disturb.

The following functions and features are not supported across the network:

- Barge-in
- Busy Verify
- Emergency transfer.

Feature interactions

Attendant Interposition Call

An attendant is not able to call a specific attendant on another node by dialing the attendant DN followed by the attendant number. The attendant dials the Network Alternate Route Selection (NARS), Coordinated Dialing Plan (CDP), or Listed Directory Number (LDN) the same way a phone dials to reach the attendants at another node.

Busy Verify

Pre-dial Break-in provides equivalent functionality but has several advantages over Busy Verify. Busy Verify does not operate on a network-wide basis.

Call Forward, Break-In and Hunt Internal or External Network Wide

When a call is transferred, a new facility message is sent to the transferred party's node to transport the terminal indicator parameter or the access trunk information parameter.

DPNSS1 Route Optimization/MCDN Trunk Anti-Tromboning Interworking

If tromboning trunks are removed on the MCDN side of a RO/TAT Interworking gateway scenario by the Network Attendant Service feature (since NAS has presence over TAT), the RO/TAT Interworking functionality is not invoked. The result is that, if NAS is equipped, attendant-extended calls that are in a tromboning state are optimized on the MCDN side, but DPNSS1 trunks are not optimised on the DPNSS1 side of the RO/TAT Interworking gateway scenario.

EuroISDN Trunk - Network Side

NAS signaling is not supported on a EuroISDN Trunk - Network Side connectivity. However, NAS will interwork with an incoming call from the EuroISDN Trunk - Network Side (routing and call handling).

INIT ACD Queue Call Restore

Call information associated with Network Attendant Service is lost after system initialization and call restoration.

ISDN QSIG Basic Call

ISDN QSIG Basic Call interacts with Network Attendant Services (NAS) as if the call is going to a route without NAS being equipped.

Listed Directory Numbers, Network-wide

This feature enables LDNs to be recognized network- wide when NAS is used. Up to six LDNs can be defined on each system. The same LDNs must be configured in multiple nodes. The LDN which users dial can be programmed as a CDP number, for example, and input in the NAS overlay as the ID of remote attendants.

Recall to Same Attendant

This feature operates on a network-wide basis for the following call types:

- Slow Answer Recall
- Camp-on Recall, and
- Call Waiting Recall.

The operation of this feature is affected by the programming for the option in the Customer Data Block of the system where the attendant answering the call resides.

Virtual Network Services

As stated earlier, NAS and CAS cannot be configured together on the same system. Since VNS requires NAS, this means that VNS and CAS cannot be configured together on the same system, either.

Feature packaging

This feature requires the following packages:

- Basic Routing (BRTE) package 14
- Basic Queuing (BQUE) package 28
- Network Class of Service (NCOS) package 32
- Network Automatic Routing System (NARS) package 58 or
- Coordinated Dialing Plan (CDP) package 59
- Flexible Call Back Queuing (FCBQ) package 61
- Attendant Break-In/Trunk Offer (BKI) package 127
- Integrated Services Digital Network (ISDN) package 145
- Advanced ISDN Network Services (NTWK) package 148
- International Primary Access (PRA) package 146 or
- 2.0 Mbit Primary Rate Interface (PRI2) package 154 or
- ISDN Signaling Link (ISL) package 147
- Network Attendant Services (NAS) package 159
- ISDN Supplementary Features (ISDNS) package 161
- Originating Routing Control/Remote Virtual Queuing (ORC-RVQ) package 192 for Drop Back Busy (please see note under "Drop Back Busy" description.)

Example of NAS implementation

Figure 15: A simple application of NAS functionality in a private ISDN PRI network on page 156 illustrates a simple application of the NAS functionality in a private ISDN PRI network connecting three systems. Although this example uses NARS, the same functionality can be accomplished using CDP.

Each system has the translations in place for a HLOC and the two LOC codes for the other two system locations. This programming was done in the NARS database. The route lists required in order to process these types of calls have been programmed also.

The INAC implementation was part of the basic ISDN/Networking programming.

The NAS programming involves the configuration of the D-channel for NAS functionality, the ID of the other attendants to be used, a list of the sequence in which these attendants are to be scanned for availability and the time periods for each list.

System B, in this example, is the location where attendants should be available 24 hours a day. During the day, the other two locations are programmed to use System B as their first choice backup and then as a second choice System A uses System C and System C uses System A. At night, Systems A and C use System B as the only backup. If it is unavailable, calls will be given Night Service.

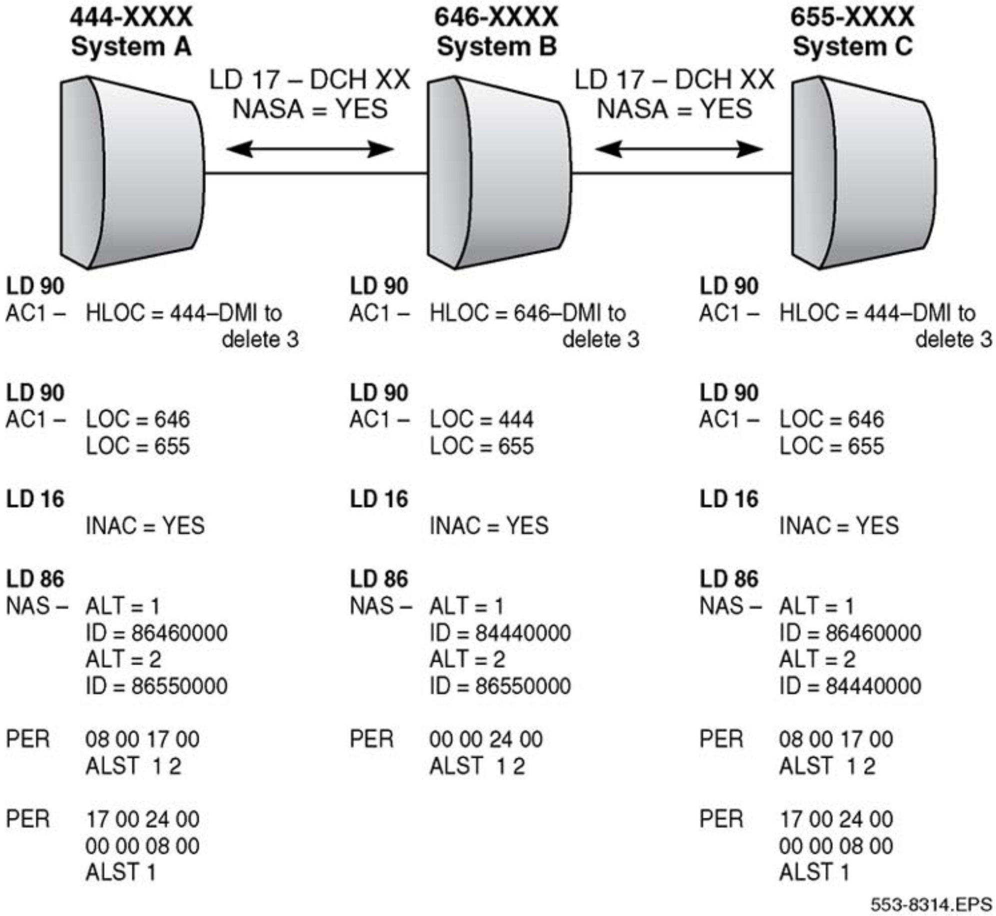

Figure 15: A simple application of NAS functionality in a private ISDN PRI network

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 67: LD 12: Configure Attendant Consoles with NAS keys. on page 157
2. Table 68: LD 15: Enable or disable network attendant control, Recall to Same Attendant, NAS routing, and define a TRK ICI key. on page 157

3. Table 69: LD 17: Configure the D-channel interface (DCHI) for NAS. on page 158
4. Table 70: LD 86: Configure NAS routing. on page 158
5. Table 71: LD 93: Assign a NAS routing table to Console Presentation Groups. on page 159
6. Table 72: LD 16: Allow or deny pre-answer tromboning (allow or deny an incoming call to be directly routed back on the same route). on page 160

Table 67: LD 12: Configure Attendant Consoles with NAS keys.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	2250	Attendant Console type.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
KEY	xx NAS	xx is the key number assigned the NAS function. Each Attendant Console can have only one NAS key defined. This key is optional.

Table 68: LD 15: Enable or disable network attendant control, Recall to Same Attendant, NAS routing, and define a TRK ICI key.

Prompt	Response	Description
REQ	CHG	Change existing data block.
TYPE	NET	Networking Data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
- OPT	aaa	Options.
- AC2	aaa	Access Code 2 as defined in LD 86.
- ISDN	YES	Integrated Services Digital Network
...		
- NAS	(YES) NO	Specifies whether to (allow) or deny attendant control for call extension.
...		
- ICI	xx NCO NDID NTIE NFEX NWAT	Respond with the key number, from 0 to 19, followed by a space, followed by the trunk type. Network CO

Prompt	Response	Description
		trunk Network DID trunk Network TIE trunk Network FEX trunk Network WAT trunk
- RTSA	(RSAD) RSAA RSAX	Recall to Same Attendant Denied Recall to Same Attendant Allowed Recall to Same Attendant allowed, with queuing on busy attendant.

Table 69: LD 17: Configure the D-channel interface (DCHI) for NAS.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ADAN	Action Device and Number.
DCHI	xxx	Respond with DCHI number for which NAS signaling is to be allowed or restricted.
NASA	(NO) YES	Specifies whether DCHI is to be allowed or (denied) NAS signaling.

Table 70: LD 86: Configure NAS routing.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
FEAT	NAS	Specifies type of data to be changed.
TBL	0–63	Routing table number, from 0 to 63. Without Multi-Tenant Service, 0 is the customer routing table. With Multi-Tenant Service enabled, NAS tables 1-63 can be associated with CPGs 1-63.
ALT	1–7	An alternative attendant or routing table, from 1 to 7. (To clear an old number, type an X before typing the new number. The old number cannot be cleared if it is associated with a schedule period. Reach TODS by pressing the return key.)
ID	xxxxxxxxxxxxxxxx	The dialed digits (including the network access code) needed to reach an attendant associated with the alternative number. Respond with a string of up to 16 digits to change the attendant ID; press the return key

Prompt	Response	Description
		to leave the ID unchanged, exit the prompt, and return to ALT.
TODS	0–31	Specifies a schedule period, from 0 to 31, where 0 is the default to handle all time periods not defined in 1 through 31. Type an X before a period number to remove the schedule period. (Typing an X before a 0 clears all associated alternatives, leaving the default treatment as local attendant treatment.) Press the return key to continue the NAS feature setup process.
- PER	HR MIN HR MIN	Specifies the start and stop times for the period using 24-hour format. Start time must be before the stop time, and minutes can be only 00 or 30. Press the return key to leave times unchanged and move to the DAYS prompt.
- DAYS	D D.É D	Specifies applicable days of the week for the time period. Respond by inputting a number representing each day for which the schedule is active (where 1 = Monday, 2 = Tuesday,...7 = Sunday). Type an X before the day number to deactivate the schedule period for that day. No more than seven entries are permitted on an input line. Press the return key to leave this schedule unchanged and move to the next prompt. (If not otherwise specified, a schedule period is assumed valid for all days.)
ALST	xxxx	Alternative list to be used for the schedule period. Respond with up to four alternative numbers in the order in which they are to be attempted. (These numbers are defined using ALT.)
DBK	Z Z Z Z	Alternatives for which "drop back busy" is to be active during this period. Respond with four entries of Y (allow) or N (deny) for the alternative evoked by the previous prompt. Responses are applied in sequence.
QUE	Z Z Z Z	Specifies alternatives for which queuing to a route is to be allowed during this period. Respond with four entries of Y (allow) or N (deny) for the alternatives evoked by ALST. Responses are applied in sequence. If the response is Y, off-hook queuing must already be configured for calls to be queued on this route.

Table 71: LD 93: Assign a NAS routing table to Console Presentation Groups.

Prompt	Response	Description
REQ	NEW	Add new data.

Prompt	Response	Description
	CHG	Change existing data.
TYPE	CPG	Console Presentation Group.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
CPG	1-63	Console Presentation Group number.
CPGS	(NO) YES	Customer Presentation Group Services.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
TEN	1-511	Tenant number
NTBL	(0) - 63	NAS routing table to be used for calls directed to this Attendant Console Group (ACG)/Console Presentation Group (CPG).

Table 72: LD 16: Allow or deny pre-answer tromboning (allow or deny an incoming call to be directly routed back on the same route).

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
TKTP	aaa	Trunk Type requires response when REQ = NEW.
TRMB	(YES) NO	Tromboning. NO = Tromboning denied. Incoming trunk call on route can not be routed back on same route. YES = Tromboning allowed. Incoming trunk call on route can be routed back on the same route. Only applies to calls routed using NARS/BARS or CDP. Does not apply to calls redirected by Hunt, Forward All Calls, or Forward No Answer.

Note:

The anti-tromboning capabilities programmed in LD 16 only apply to attendant extended calls.

NAS performs tromboning when required regardless of the LD 16 programming. However, if redundant (or tromboned) trunk connections are to drop after the phone is answered, this prompt must be set to NO across the network where this might occur.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 18: Network Break-in and Force Disconnect

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Network Break-in and Force Disconnect feature allows an analog (500/2500-type) or a digital phone to perform the following functions:

- break-in to an established two-party call
- force disconnect an established two-party call

Attendant Break-in / Network Break-in

With Network Break-in, a phone can break-in to an established two-party call. When the phone initiates a break-in operation, it is placed in conference with the other two parties. A warning tone can be provided to all parties. The warning tone option must be allowed in LD 15 for the wanted party's customer group.

The user of the overriding phone can initiate the break-in operation using one of the following:

- Priority Override Network Wide (PONW) key for Meridian Digital phones. The PONW lamp on the overriding phone provides the status of the break-in operation.
- Priority Override Network Wide (PONW) Flexible Feature Code (FFC) for analog (500/2500 type) phones

Network break-in applies to both pre- and post-dial operations. For a pre-dial operation, the user of the overriding phone presses the PONW key or dials the PONW FFC prior to dialing the wanted party's DN.

For a post-dial operation, the user of the overriding phone dials the wanted party's DN. When they receive a busy tone, they then press the PONW key or dial the PONW FFC.

Network Force Disconnect

Network Force Disconnect allows a phone to disconnect an established two-party call. A call is then established between the overriding phone and the wanted phone. A single warning tone can be provided to all parties before the disconnect operation takes place. The warning tone option must be allowed in LD 15 for the wanted party's customer group.

The user of the overriding phone can initiate the force disconnect operation using one of the following:

- Forced Disconnect (FDIS) key for Meridian Digital phones The FDIS lamp on the overriding phone provides the status of the force disconnect operation
- Forced Disconnect Flexible Feature Code (FFC) for analog (500/2500 type) phones

Network Force Disconnect applies to both pre- and post-dial operations. For a pre-dial operation, the user of the overriding phone presses the FDIS key or dials the PONW FFC prior to dialing the wanted party's DN.

For a post-dial operation, the user of the overriding phone dials the wanted party's DN. When they receive busy tone, they then press the FDIS key or dial the FDIS FFC.

Network Break-in and Force Disconnect post-dial example

As illustrated in Figure 16: Example of a network break-in and force disconnect operation on page 165, Node X and Node Y are two systems connected by a Meridian Customer Defined Network (MCDN) Primary Rate Interface (PRI). Phone A, a Meridian Digital phone on Node X, is the overriding party. Phones B and C are in an established two-party call on Node Y. Phone B is the wanted party and Phone C is the unwanted party.

Phone A dials Phone B and receives a busy tone. Phone A presses the PONW key. Phone A enters into a conference with Phones B and C. A warning tone is provided to all three parties.

Phone A presses the FDIS key. Phone C is disconnected. Phones A and B are placed in a simple, two-party call.

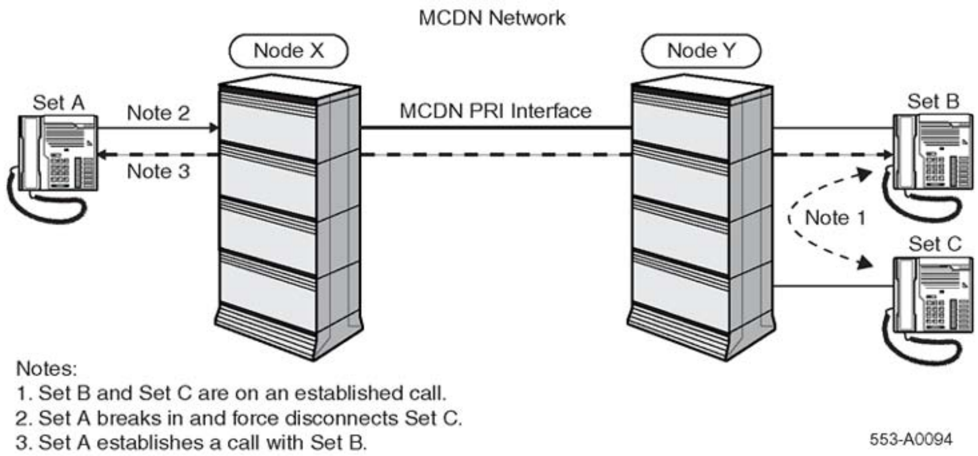

Figure 16: Example of a network break-in and force disconnect operation

Priority Levels

Priority Levels (PLEVs) are configured on an individual phone basis. A phone can break-in to or disconnect an established call only if it has a Priority Level greater than or equal to the Priority Levels of the wanted and unwanted parties. If the unwanted party is an external trunk call, the PLEV of the route applies.

Table 73: Priority Levels on page 165 lists the various PLEVs that can be assigned to a phone or route.

Table 73: Priority Levels

Priority Levels	Overriding Party	Wanted/Unwanted Parties
0	Cannot override	Cannot be overridden
1	Cannot override	Cannot be overridden
2	Can override level 2	Can be overridden by levels 2-7
3	Can override levels 2 and 3	Can be overridden by levels 3-7
4	Can override levels 2-4	Can be overridden by levels 4-7
5	Can override levels 2-5	Can be overridden by levels 5-7
6	Can override levels 2-6	Can be overridden by levels 6 and 7
7	Can override levels 2-6	Cannot be overridden

Priority Levels	Overriding Party	Wanted/Unwanted Parties
	Assign level 7 to ACD supervisors only	

Operating parameters

This feature applies to analog (500/2500-type) and digital phones.

The Network Break-in and Force Disconnect feature is supported when the overriding and wanted parties are:

- on the same node
- on different nodes and connected by an MCDN interface

The unwanted party can be any of the following. Refer to Figure 16: Example of a network break-in and force disconnect operation on page 165:

- an analog (500/2500-type) phone or digital phone located on the same node as the wanted party (Node Y)
- an analog (500/2500-type) phone or digital phone located on a different node (Node X) and connected by an MCDN interface to the wanted party's node (Node Y)
- an external user in conversation with the wanted party over Direct Inward Dialing (DID), TIE, or Central Office trunks (COT). The external interface to Node Y can be analog trunks or ISDN CO connectivity.

If the force disconnect request is rejected, an overflow tone is provided. For digital phones, the PONW/FDIS lamp winks and overflow tone is provided.

If the wanted party's phone is idle when the pre-dial operation begins, the pre-dial operation is cancelled and the wanted party's phone rings.

Feature interactions

Attendant Call

In a stand-alone environment, a phone cannot break-in to an attendant call. In a networking environment, however, Network Attendant Service (NAS) must be enabled to avoid a phone breaking in to an attendant call.

Automatic Call Distribution

Any phone with a PLEV of 7 (except for a 500 ACD agent phone) can be used to break-in to an ACD call. Knowing the Agent's position ID is required.

No phone can be used to break-in to a supervisor's call.

An ACD phone goes in Not Ready (NRD) state when it invokes the Network Break-in and Forced Disconnect feature by pressing the Priority Network Override (PONW) or Force Disconnect (FDIS) key.

The ACD phone is removed from the idle agent's queue and is then no longer serving the queue. After the call is released, the phone remains in the NRD state. You have to manually remove the phone from the NRD state by pressing the NRD key again. If the phone does not have an NRD key, you have to press the ACD key to log into the phone.

A conference is set up if:

- Supervisor Disconnects: Agent and the Customer are in a call
- Agent Disconnects: Supervisor and Customer are in a call
- Customer Disconnects: Supervisor and Agent are in a call

A post-dial operation for the Network Break-in and Forced Disconnect on an ACD agent is not allowed.

An FDIS operation on an ACD agent is not allowed.

A speech path is always established as a two-way speech path.

Call Detail Recording

The Network Break-in and Force Disconnect feature does not affect Call Detail Recording (CDR) records. On the CDR records, Network Break-in is treated as a normal conference and Force Disconnect is treated as normal call clearing.

Call Forward

Call Waiting

Camp on

Hunt

Post-dial operations do not override the Call Forward, Call Waiting, Camp on, or Hunt features configured on the wanted party's phone.

Pre-dial operations override the Call Forward, Call Waiting, Camp on, and Hunt features configured on the wanted party's phone.

If Call Forward or Hunt is performed on a local phone or to a phone on a different MCDN node, then post-dial/force disconnect occurs on the redirected phone (if the break-in conditions are met).

If there is a call waiting or camped on the wanted party's phone, the pre-dial operation can still break-in or force disconnect.

Call Park

Network break-in or force disconnect operations cannot be performed on a parked call.

Conference

Network break-in or force disconnect operations cannot be performed on a phone that is in conference. However, if the originator of a conference is on a different node, it can break-in and force disconnect the unwanted party from the conference. A call is then established between the overriding party and the wanted party.

Do Not Disturb

Network break-in or force disconnect operations cannot be performed if Do Not Disturb (DND) is configured on the phone.

Make Set Busy

Network break-in or force disconnect operations cannot be performed if Make Set Busy (MSB) is configured on the phone.

Meridian Mail

Network break-in or force disconnect operations do not occur when the wanted party is using Meridian Mail or Avaya CallPilot.

Orbit Prevention

When Orbit Prevention is enabled, if a call is forwarded to a phone on a different MCDN node, it removes the Call Forward operation for the trunk-to-trunk call for a specified period of time. During this period of time, the post-dial operation cannot be performed.

The Flexible Orbiting Prevention Timer (FOPT) is set to 6 seconds by default. Most calls will be released within this time if the post-dial operation is performed after the timer expires. As a result, the FOPT should be set to a lower value.

Priority Override

The Priority Override feature is independent of the Network Override and Force Disconnect feature.

Ring Again

When the wanted party's phone is busy, the overriding phone can either trigger ring again or post-dial break-in/force disconnect.

Virtual Network Services

Virtual Network Services (VNS) supports the Network Break-in and Force Disconnect feature.

Feature packaging

The Network Break-in and Force Disconnect feature introduces Priority Network Override (PONW) package 389.

Network Break-in and Force Disconnect also requires the following existing packages:

- ISDN Signaling (ISDN) package 145
- Primary Rate Access (PRA) package 146
- Primary Rate Interface2 (PRI2) package 150
- Multi-Serial Data Link (MSDL) package 222

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. LD 17 - Configure the Release ID for the D-channels.
2. LD 15 - Allow or deny the Break-in Warning Tone.
3. LD 16 - Configure the Priority Level (PLEV) for the route.
4. LD 10 - Configure break-in warning tone options and PLEV values for analog (500/2500 type) phones.
5. LD 11 - Configure break-in and force disconnect Classes of Service, function keys, warning tone options, and PLEV values.
6. LD 57 - Configure the Flexible Feature Codes (FFCs).

Table 74: LD 17: Configure the Release ID for the D-channels.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	Action Device and Number.
ADAN	CHG DCH xx	Change D-channels.
RLS	xx	Software Release ID of the switch at the far-end of the D-channel, where xx is 25 or higher.

Table 75: LD 15: Allow or deny the Break-in Warning Tone.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	FTR	Feature data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
…		
OPT	(BWTD) BWTA	Break-in Warning Tone Denied (default). Break-in Warning Tone Allowed.

Table 76: LD 16: Configure the Priority Level for the route.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
PLEV	0-(2)-7	Priority Level.

Table 77: LD 10: Configure Break-in warning tone options and PLEV values for analog (500/2500-type) phones.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	500	Type of phone.
CLS	(NOVD) NOVA	Network Override/Break-in Denied (default). Network Override/Break-in Allowed.
CLS	(FDSD) FDSA	Force Disconnect Denied (default) Force Disconnect Allowed
PLEV	0-(2)-7	Priority Levels.

Table 78: LD 11: Configure break-in and force disconnect Classes of Service, function keys, warning tone options, and PLEV values.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	a... a	Telephone type. Type **?** for a list of possible responses.
CLS	(NOVD) NOVA	Network Override/Breakin Denied (default). Network Override/Breakin Allowed.
CLS	(FDSD) FDSA	Force Disconnect Denied (default) Force Disconnect Allowed
KEY	PONW	Priority Override/Breakin Networkwide Key.
KEY	FDIS	Force Disconnect Key.

Prompt	Response	Description
PLEV	0-(2)-7	Priority Levels.

Table 79: LD 57: Configure the Flexible Feature Codes (FFCs).

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	FFC	Flexible Feature Code.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
…		
CODE	PONW	FFC Type.
PONW	xxxx	Activate PONW.
CODE	FDIS	FFC Type.
FDIS	xxxx	Activate FDIS.

Feature operation

This section describes the procedures for performing the network break-in and force disconnect operations on both Meridian Digital and analog (500/2500 type) phones. The feature operation is described using Phones A, B, and C from Figure 16: Example of a network break-in and force disconnect operation on page 165 on Figure 16: Example of a network break-in and force disconnect operation on page 165.

Network Break-in operation

Post-dial operation for Meridian Digital phones

Table 80: Post-dial network break-in operation for a Meridian Digital phone on page 173 shows the post-dial network break-in operation for a Meridian Digital phone.

Table 80: Post-dial network break-in operation for a Meridian Digital phone

Actions	Response	Phone A PONW lamp status
Phones B and C are involved in a two-party call.	—	—
Phone A dials Phone B.	Phone A receives a busy tone.	—
Phone A presses the PONW key.	Phone A enters into a Conference with Phones B and C. If configured, a warning tone is provided to all three parties.	PONW key lamp is lit.
If Phone C disconnects…	Phones A and B are placed in a simple, two-party call. The warning tone is removed.	PONW key lamp goes dark.
If Phone B disconnects…	Phone C is disconnected. The warning tone is removed. Phone B rings.	Meridian PONW key lamp goes dark.

Pre-dial operation for Meridian Digital phones

Table 81: Pre-dial network break-in operation for a Meridian Digital phone on page 173 shows the pre-dial network break-in operation for a Meridian Digital phone.

Table 81: Pre-dial network break-in operation for a Meridian Digital phone

Actions	Response	Phone A PONW lamp status
Phones B and C are involved in a two-party call.	—	—
Phone A presses the DN key and then presses the PONW key.	Phone A receives dial tone.	The PONW key lamp flashes. This indicates the pre-dial mode.
Phone A dials the DN of Phone B	Phone A enters into a conference with Phones B and C. If configured, a warning tone is provided to all three parties.	The PONW key lamp is lit.
If Phone C disconnects…	The warning tone is removed. Phones A and B are placed in a simple, two-party call.	The PONW key lamp goes dark.
If Phone B disconnects…	Phone C is disconnected. The warning tone is removed. Phone B rings.	The PONW lamp goes dark.

Post-dial operation for analog (500/2500 type) phones

Table 80: Post-dial network break-in operation for a Meridian Digital phone on page 173 shows the post-dial network break-in operation for analog (500/2500 type) phones.

Table 82: Post-dial network break-in operation for an analog (500/2500 type) phone

Actions	Response
Phones B and C are involved in a two-party call.	—
Phone A dials Phone B.	Phone A receives a busy tone.
Phone A presses the Flash key and dials the PONW FFC code.	Phone A enters into a Conference with Phones B and C. If configured, a warning tone is provided to all three parties.
If Phone C disconnects	Phones A and B are placed in a simple, two-party call. The warning tone is removed.
If Phone B disconnects	Phone C is disconnected. The warning tone is removed. Phone B rings.

Pre-dial operation for analog (500/2500 type) phones

Table 83: Pre-dial network break-in operation for an analog (500/2500 type) phone on page 174 shows the post-dial network break-in operation for analog 500/2500 type) phones.

Table 83: Pre-dial network break-in operation for an analog (500/2500 type) phone

Actions	Response
Phones B and C are involved in a two-party call.	—
Phone A dials the PONW FFC and then Phone B's DN.	Phone A receives dial tone and then enters a conference with Phones A and B. If configured, a warning tone is provided to all three parties.
If Phone C disconnects	The warning tone is removed. Phones A and B are placed in a simple, two-party call.
If Phone B disconnects	Phone C is disconnected. The warning tone is removed. Phone B rings.

Network Force Disconnect operation

Post-dial network force disconnect operation for Meridian Digital phones

Table 84: Post-dial network force disconnect operation for a Meridian Digital phone on page 175 shows the post-dial network force disconnect operation for a Meridian Digital phone.

Table 84: Post-dial network force disconnect operation for a Meridian Digital phone

Actions	Response	Phone A PONW lamp status
Phones B and C are involved in a two-party call.	—	—
Phone A dials Phone B.	Phone A receives a busy tone.	—
Phone A presses the FDIS key.	If configured, a single warning tone is provided and Phone C is disconnected. Phones A and B are placed in a simple, two-party call.	The FDIS key lamp remains lit during the single warning tone period. It goes dark when Phone C is disconnected.
OR		
If Phone A initiates a break-in operation first (either pre-dial or post-dial)	Phone A enters into a conference with Phones B and C. If configured, warning tone is provided.	The PONW lamp is lit.
Phone A presses the FDIS key.	Phone C is disconnected and the warning tone is removed. Phones A and B are placed in a simple, two-party call.	The PONW lamp goes dark.

Pre-dial network force disconnect operation for Meridian Digital phones

Table 85: Pre-dial network force disconnect operation for a Meridian Digital phone on page 176 shows the pre-dial network force disconnect operation for a Meridian Digital phone.

Table 85: Pre-dial network force disconnect operation for a Meridian Digital phone

Actions	Response	Phone A PONW lamp status
Phones B and C are involved in a two-party call.	—	—
Phone A presses the DN key and then the FDIS key.	Phone A receives dial tone.	The FDIS lamp flashes. This indicates the pre-dial mode.
Phone A dials the DN of Phone B.	If configured, a single warning tone is provided and Phone C is disconnected. Phones A and B are placed in a simple, two-party call.	The FDIS lamp remains lit during the single warning tone period. It goes dark when Phone C is disconnected.

Post-dial force disconnect operation for analog (500/2500 type) phones

Table 86: Post-dial network force disconnect operation for an analog (500/2500 type) phone on page 176 shows the post-dial network force disconnect operation for an analog (500/2500 type) phone.

Table 86: Post-dial network force disconnect operation for an analog (500/2500 type) phone

Actions	Response
Phones B and C are involved in a two-party call.	—
Phone A dials Phone B.	Phone A receives a busy tone.
Phone A presses the Flash key and then dials the FDIS FFC code.	If configured, a single warning tone is provided and Phone C is disconnected. Phones A and B are placed in a simple, two-party call.
OR	
If Phone A initiates a break-in operation first (either predial or postdial)	Phone A enters into a conference with Phones B and C. If configured, a warning tone is provided.
Phone A presses the Flash key and then dials the FDIS FFC.	Phone C is disconnected and the warning tone is removed. Phones A and B are placed in a simple, two-party call.

Pre-dial Network force disconnect operation for analog (500/2500 type) phones

Table 87: Pre-dial network force disconnect operation for an analog (500/2500 type) phone on page 177 shows the pre-dial network force disconnect operation for an analog (500/2500 type) phone.

Table 87: Pre-dial network force disconnect operation for an analog (500/2500 type) phone

Actions	Response
Phones B and C are involved in a two-party call.	—
Phone A dials the FDIS FFC and then dials Phone B's DN.	Phone A receives a dial tone. If configured, a single warning tone is provided and Phone C is disconnected. Phones A and B are placed in a simple, two-party call.

Chapter 19: Network Call Party Name Display/Network Name Delivery

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Network Call Party Name Display

Network Call Party Name Display (NCPND) provides a network-wide visual display of names and phone numbers to both parties of a call. For phones equipped with an alphanumeric display, NCPND provides the display of the calling party's name on the terminating phone and the called party's name on the calling phone. The name and number display lasts for the duration of the call.

The sending of the names over the private network is an option set up on a per route basis. The name is provided by Call Party Name Display (CPND) configured in each switch. For call redirections, a phone option provides a display of the redirecting name instead of the calling name.

The following phones and attendant consoles are supported:

- M2317 digital phones
- all Meridian Modular Telephones with digit display
- Avaya 2250 Attendant Consoles

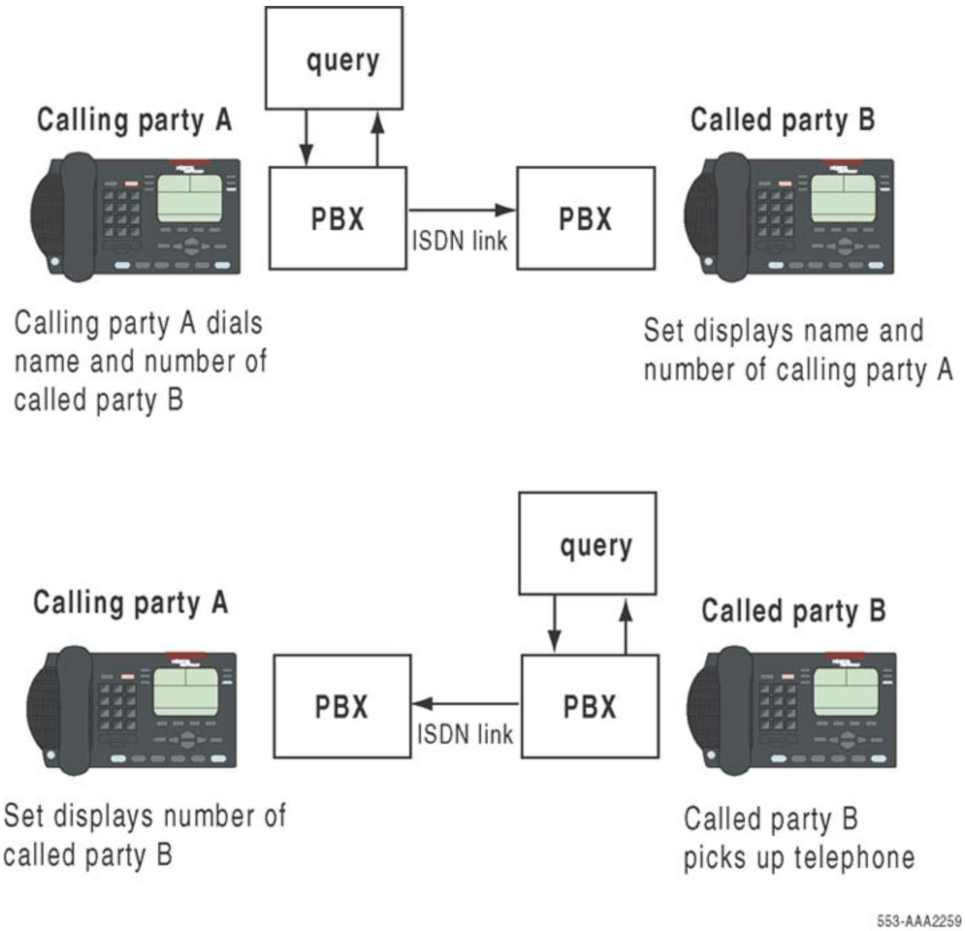

Figure 17: NCPND displays

Network Name Delivery

Network Name Delivery (NND) is the method used to send the names and numbers across the network. Network Name Delivery provides network-wide name display in compliance with the Meridian Customer Defined Networking (MCDN) protocol. It allows interworking among systems and a DMS-100/250 Central Office.

Operating parameters

The following list describes the Network Name Delivery operating parameters.

- For system to system, the maximum number of characters in a displayed name is 24. When connecting to a Central Office, 15 characters only are supported. Names exceeding this length are truncated.
- Name Delivery is supported for Call Pickup, Call Transfer, Hunt, and Call Forward All Calls/No Answer/Busy.
- A CPND enhancement allows the display of the redirecting name on the terminating phone instead of the calling name by a service change option only if the first redirecting party is on the terminating switch.
- In all cases, when the name is available, the called party name is displayed on the caller's display during the ringing phase. This is an enhancement over ND1 which displays names on connect.

Feature interactions

The same feature interactions apply as those for Call Party Name Display; refer to the Call Party Name Display description in *Avaya Features and Services Fundamentals, NN43001-106.*

Feature packaging

This feature requires the following packages:

- Calling Party Name Display (CPND) package 95
- Integrated Services Digital Network (ISDN) package 145
- ISDN Primary Rate Interface (PRI) package 146 or
- 2.0 Mbit Primary Rate Access (PRI2)

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 88: LD 95: Configure the Calling Party Name Display. on page 182
2. Table 89: LD 16: Enable NCPND for each required trunk route. on page 182
3. Table 90: LD 17: Indicate the remote capability (which Network Name Delivery protocol is supported by the remote node/switch on this DCH interface). on page 183

Table 88: LD 95: Configure the Calling Party Name Display.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	CPND	Calling Party Name Display.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
- NITC	aaaa (NI)	Non-Hot Line call. Indicates that the Hot Line call terminated as a normal call.

Table 89: LD 16: Enable NCPND for each required trunk route.

Prompt	Response	Description
REQ	CHG	Change.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.

Prompt	Response	Description
...		
- ISDN	YES	ISDN option.
...		
- - NCNA	(YES) NO	Allow Network Call Name Display.

Table 90: LD 17: Indicate the remote capability (which Network Name Delivery protocol is supported by the remote node/switch on this DCH interface).

Prompt	Response	Description
REQ	CHG	Change
TYPE	ADAN	Type of data block
ADAN	CHG DCH xx	Change D-channel.
...		
- RCAP	ND1 ND2	Network Name Delivery method 1 (ND1). Network Name Delivery method 2 (ND2).

Feature operation

No specific operating procedures are required to use this feature.

Chapter 20: Network Call Redirection

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Network Call Redirection feature provides Network Call Forward No Answer (NCFNA) and Network Call Forward All Calls (NCFAC) over an ISDN PRA or ISL network. Calls can also be transferred over the network, but the CLID display will not reflect the transfer.

The Network Call Redirection (NCRD) feature is based on the stand-alone Call Redirection feature. Stand-alone Call Redirection permits redirection within a single system. Using Network Call Redirection, calls are redirected over more than one system. The user cannot tell the difference between a call-redirected and a network call-redirected call. The CLID digit and the name displays are the same for both call scenarios.

NCRD supports system to system connections. The private numbering plans, the Uniform Dialing Plan (UDP), and the Coordinated Dialing Plan (CDP) are supported by both network configurations.

For NCFNA, the call can pass through (hop) only one switch. However, as shown in Figure 18: Network configurations for NCFAC and NCFNA on page 186, a multiple-hop configuration is permitted for NCFAC.

The number of times a call is redirected depends on the Class of Service of the redirecting phone. If the redirecting phone has a Class of Service with second-level NCFNA denied, only one NCFNA is allowed. If a second NCFNA attempt is made, it is rejected and the call continues to ring at the first redirected station. If the redirecting phone has a Class of Service with second-level NCFNA allowed, the call can have an additional CFNA redirection.

Note:

A redirected call over PRA that terminates on a busy phone cannot activate the Network Ring Again (NRAG) feature. Also, CLID name display is not supported in call transfer, call forward busy, hunt, or call pickup.

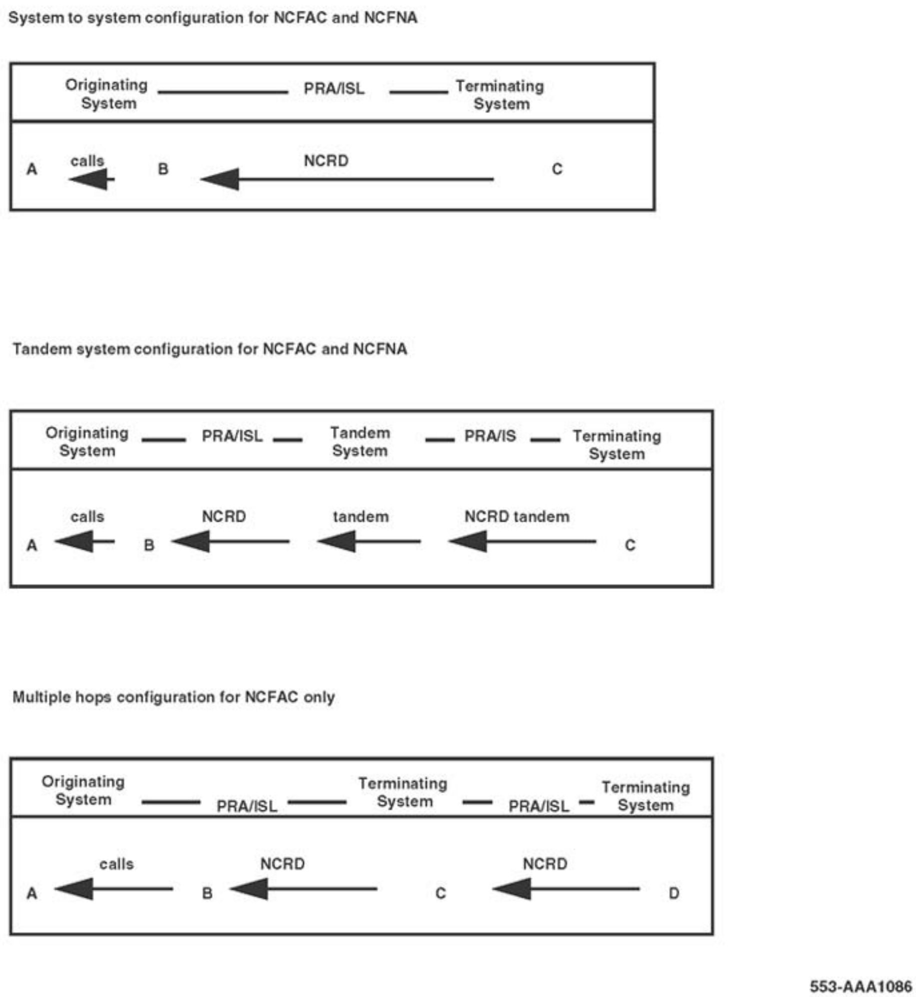

Figure 18: Network configurations for NCFAC and NCFNA

Call redirection terminology

There are four parties involved in a call redirection: the originating party, the originally called party, the redirecting party, and the terminating party.

If A calls B and B redirects the call to C, then:

A is the originating party

B originally called party and the redirecting party

C is the terminating party

With additional redirections, the terminology changes. For example, if A calls B and B redirects the call to C and C redirects the call to D and D redirects the call to E, then:

A is the originating party

B is the originally called party

C is the no name party

D is the redirecting party

E is the terminating or redirection party

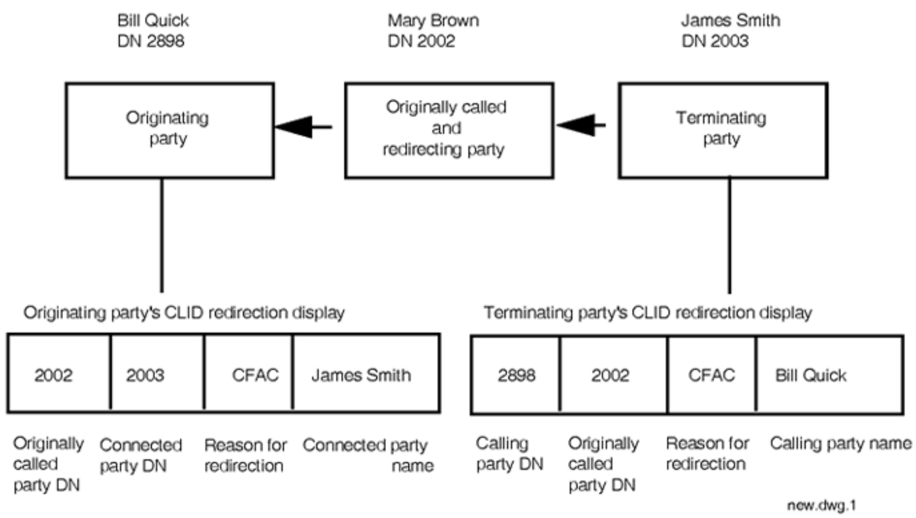

Figure 19: Simple redirection

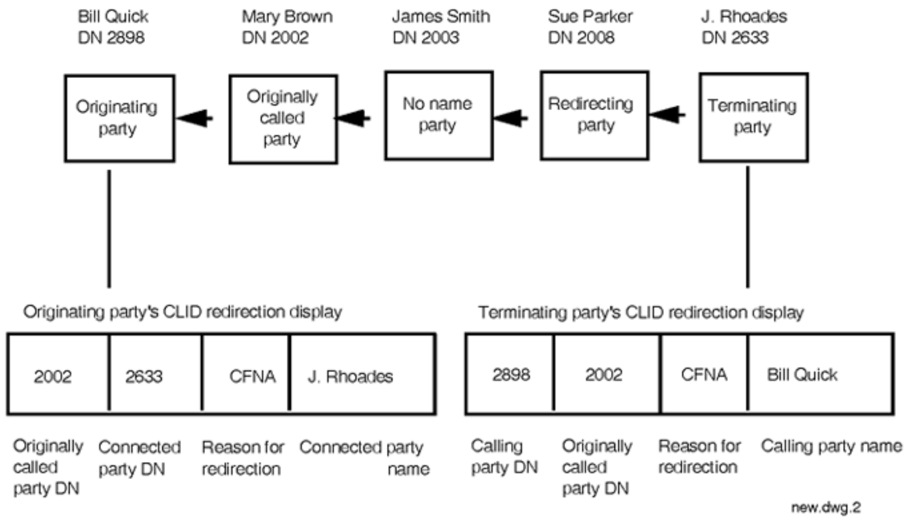

Figure 20: Multiple redirections

Notifying originating party of redirection

As shown in Figure 21: Originating party CLID redirection display on page 188, if the originating party is a subscriber to the Calling Line Identification (CLID) service, their phone displays a Call Redirection reason. This format is like that of internal call redirection CLID.

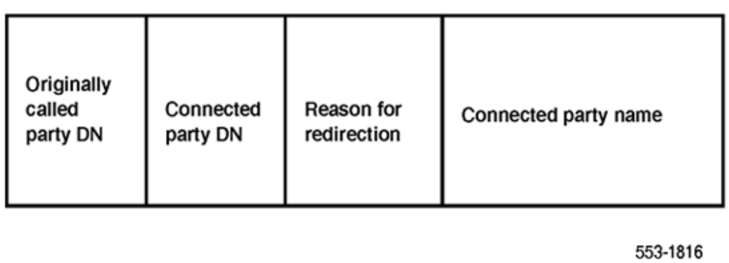

Figure 21: Originating party CLID redirection display

The reason field of the CLID display indicates why the call is redirected out of the original called party, that is either NCFAC or NCFNA. The reason mnemonic displayed is assigned by the customer in LD 95. See the PRA Administration document for a procedure about how to program the Network Call Redirection (NCRD) feature.

If the originally called party information is not available, the redirecting party DN is displayed in place of the originally called DN. For single call redirection, the originally called party is also the redirecting party.

Notifying terminating party of redirection

As shown in Figure 22: Terminating party CLID redirection display on page 189, if the terminating party is a subscriber to the CLID service, their phone displays a call redirection reason. The display format for the terminating party is the same as that for an internal Call Redirection.

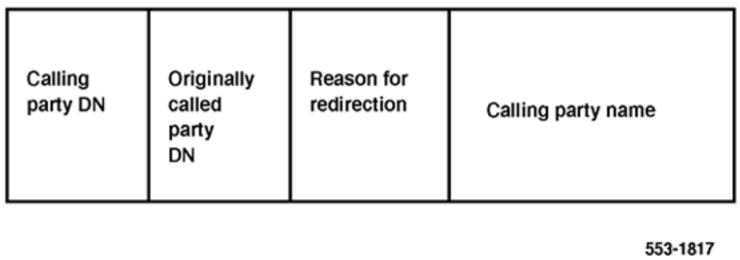

Figure 22: Terminating party CLID redirection display

If the originating party information is not available, the redirecting party DN is displayed instead.

Redirection tones

The tone the originating party receives is determined by the cause of the redirection. When a call cannot terminate because the forward-to DN is busy and none of the redirections are due to Network Call Forward No Answer (NCFNA), the originator receives a busy tone. However, if one redirection is due to NCFNA, an attempt is made to re-ring the phone that initiated the NCFNA.

When the call cannot terminate for any reason other than the forward-to DN is busy and no redirections are due to NCFNA, the originator receives an overflow tone. Again, if one redirection is due to NCFNA, an attempt is made to re-ring the phone that initiated the NCFNA.

A redirection counter value is passed with the call-forwarding information. When the redirection counter maximum is exceeded, there are two scenarios. If all call redirections are due to Network Call Forward All Calls (NCFAC), the calling party receives an overflow tone. If one of the redirections is due to NCFNA, an attempt is made to re-ring the phone that initiated the NCFNA.

Network Call Redirection configurations

The following figures are examples of typical Call Redirection configurations. The text associated with each figure explains the scenarios. These scenarios are shown:

- Intranode NCFAC
- Internode Tandem NCFAC
- Tandem NCFAC and Intranode redirection
- Tandem NCFAC
- NCFNA
- Tandem NCFNA

Note:
Call Redirection is supported only in system to system call connections.

Intranode NCFAC redirection

As shown in Figure 23: NCFAC intranode redirection on page 191, the following occurs in a NCFAC scenario:

- Station A calls Station B on another node. Station B has the Call Forwarding All Calls feature and forwards to Station C.
- The call is then forwarded to Station C. Station C resides in the same terminating node as Station B.
- The terminating node, Station C, sends the CLID display information to Station A. When Station C answers the call, a message is sent to the originating node, Station A.

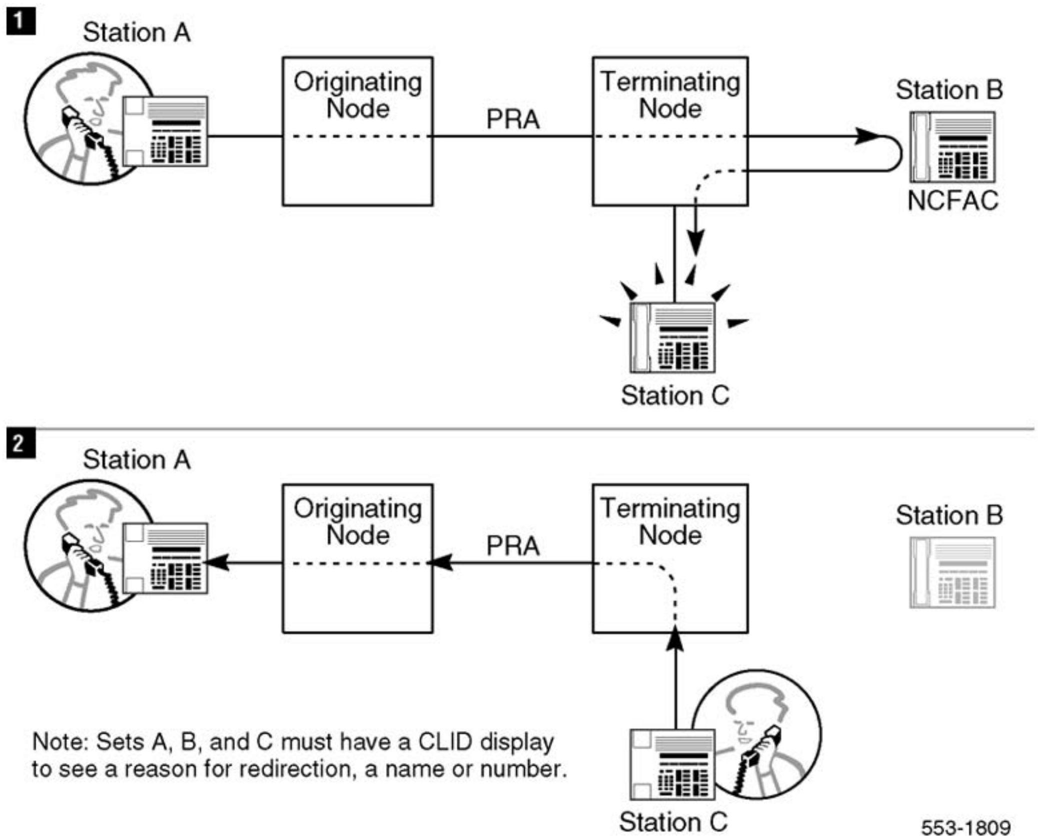

Figure 23: NCFAC intranode redirection

Internode NCFAC redirection

As shown in Internode NCFAC, the following occurs in an internode NCFAC redirection scenario:

- Station A generates a call to Station B. Station B has the Call Forwarding All Calls feature and forwards to Station C. Station C is located on another switch, making this an internode call.
- A message that contains the called number, calling number, original called number, original redirection reason, and the redirection counter is sent with the call.
- When Station C answers the call, a message is sent to the originating node indicating this response.

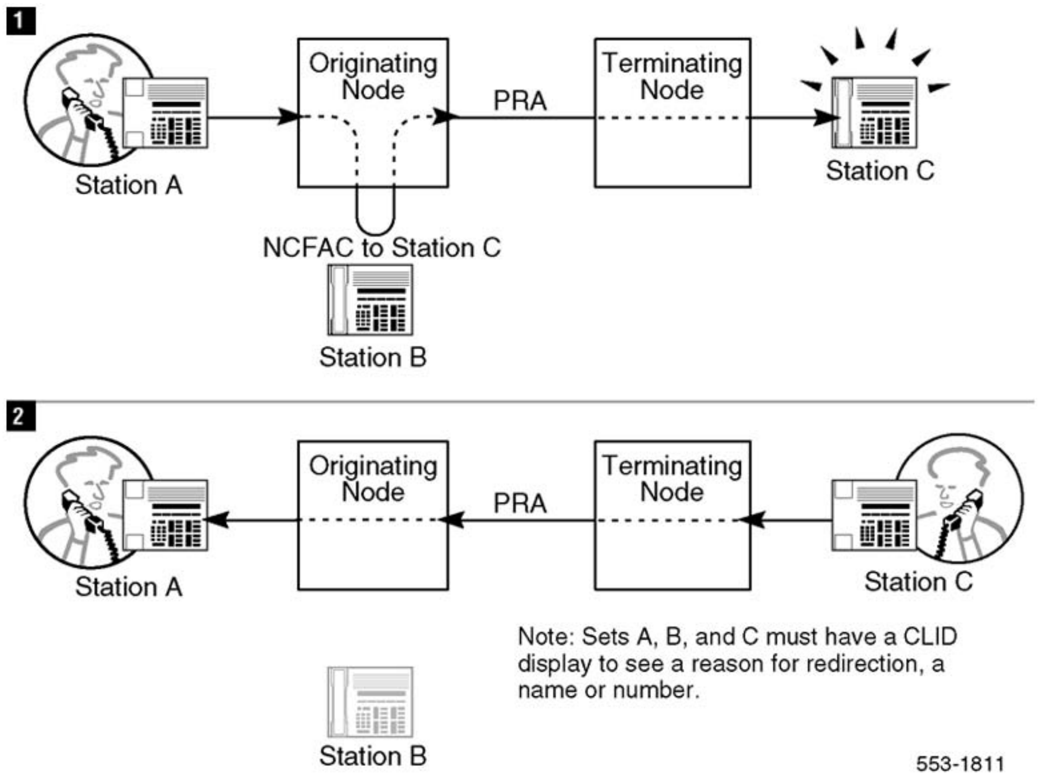

Figure 24: Internode NCFAC

Tandem NCFAC redirection

As shown in Tandem NCFAC, the following scenario occurs in tandem NCFAC redirection.

- Station A generates an internode call to Station B. Station B has the Call Forwarding All Calls feature and forwards to Station C on another switch.
- The call is translated at the tandem node and then forwarded to Station C at the terminating node.
- The message that accompanies the call from the tandem to the terminating node contains the called number (Station C), the calling number (Station A), original called number (Station B), the original reason for redirection (NCFAC), and the redirection counter that has a value of 1.
- The terminating node sends a message to the originating node that contains the call forwarding information along with an indication of ringing Station C.
- When Station C answers the call, a message indicating this response is sent first to the tandem node and then relayed to the originating node.

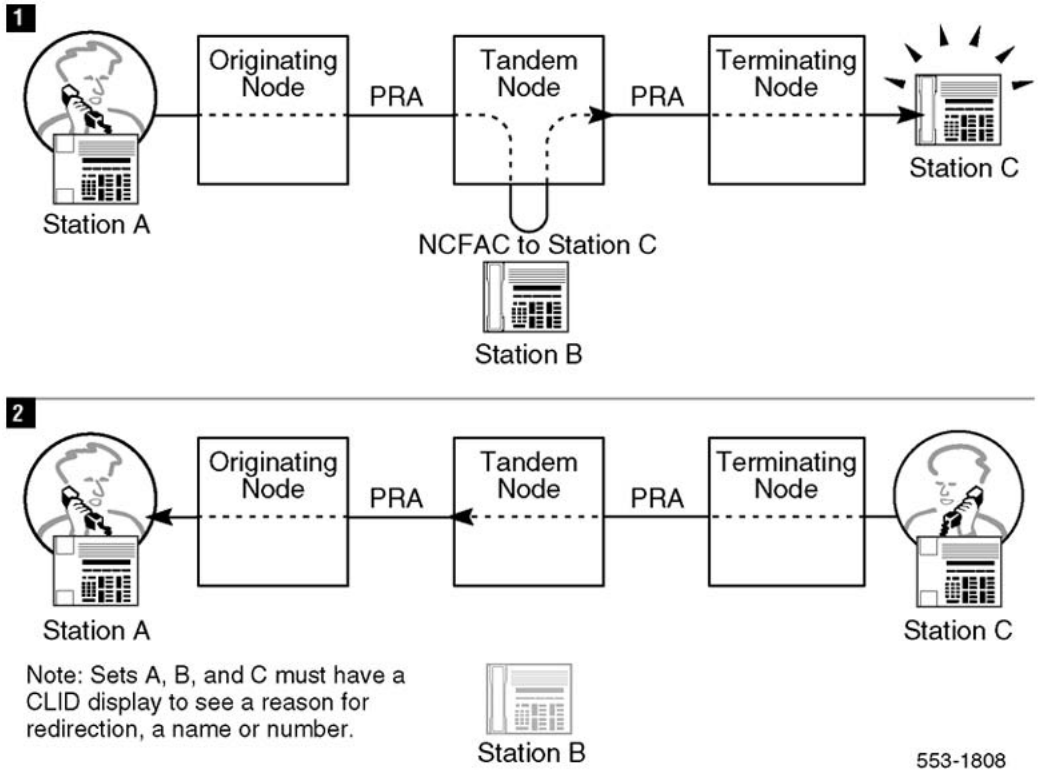

Figure 25: Tandem NCFAC

Tandem NCFAC and intranode redirection

The following occurs in a tandem NCFAC. This is followed by an intranode redirection scenario, as shown in Tandem NCFAC intranode.

- Station A generates an internode call to Station B. This Station B has the Call Forwarding All Calls feature and forwards to Station C on another node. In this scenario, Station C has the Call Forwarding All Calls feature and forwards the call to station D on the same node.
- The call is forwarded from the tandem node to the terminating node for Station C. The CLID information is also sent as a message along with the call. This information includes the called number (Station C), the calling number (Station A), the original called number (Station B), the original redirection reason (CFAC or NCFAC), and the redirection counter (1).
- The call is then forwarded to station D within the terminating node. The terminating node sends the call forwarding information to the originating node (Station A).
- The redirection counter is still 1 since there was a single network redirection.
- Station D answers and a message is sent notifying the originating node of this response.

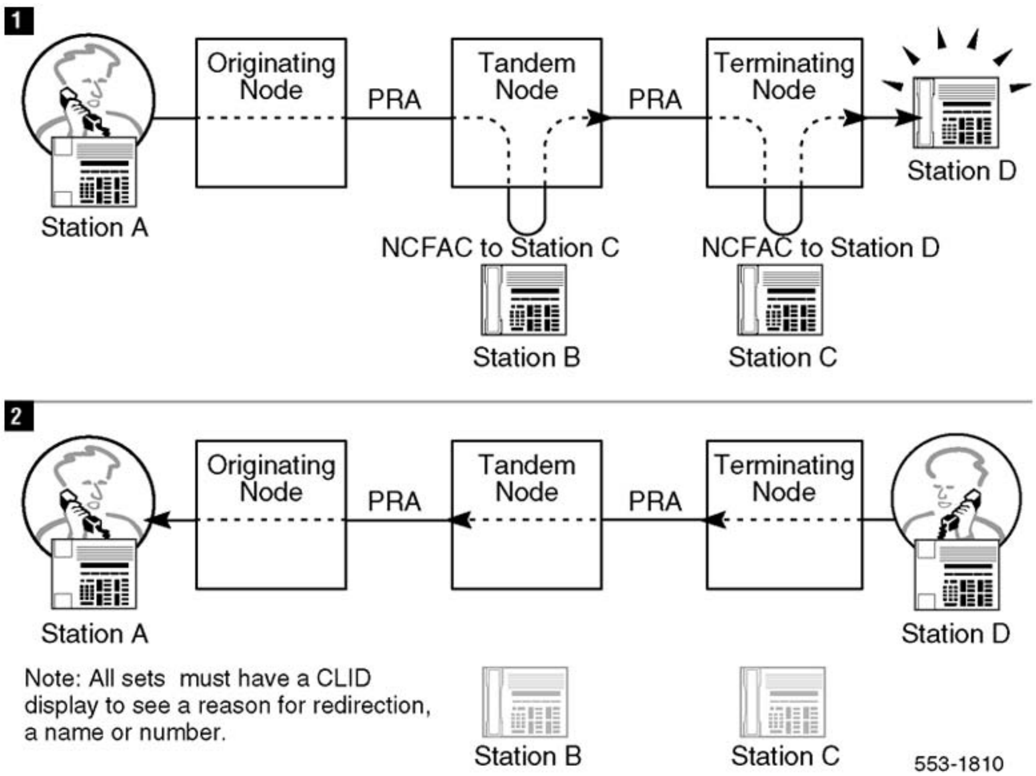

Figure 26: Tandem NCFAC intranode

NCFNA redirection

As shown in NCFNA, the following occurs in an NCFNA redirection scenario.

- Station A generates an internode call to Station B which has the Call Forwarding No Answer feature and forwards to Station C.
- The call is transferred to Station C when the ringing (or alerting) phase times out. The terminating node sends a message to the originating node that contains the redirection number (Station C) and the redirection reason (NCFNA).
- When Station C answers the call, the terminating node generates a message to the originating node indicating this response.

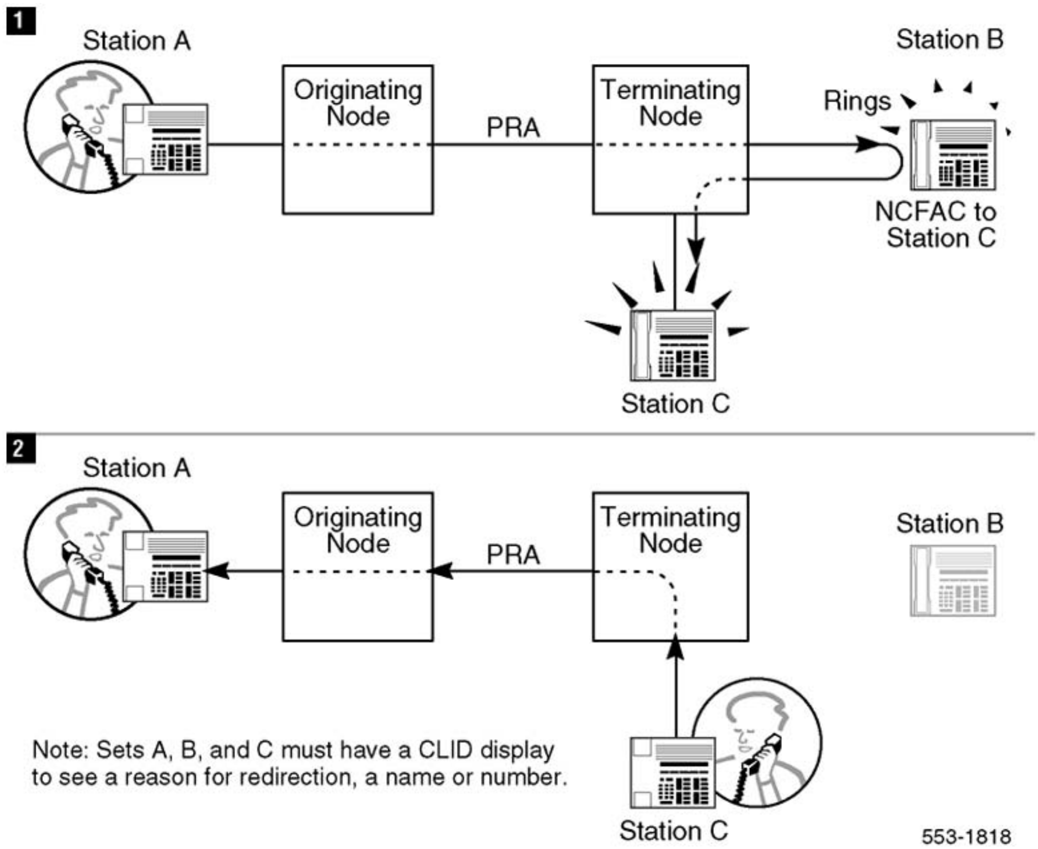

Figure 27: NCFNA

Tandem NCFNA redirection

As shown in Tandem NCFNA, the following occurs in a tandem NCFNA redirection scenario.

- Station A generates an internode call to Station B which has the Call Forwarding No Answer feature and forwards to Station C.
- The call is transferred to Station C when the ringing (alerting) phase times out.
- The message sent to the terminating node contains the called number (Station C), calling number (Station A), original called number (Station B), original reason for redirection (NCFNA), and the redirection counter with a value of 1.
- The terminating node sends a message to the tandem node which relays the message to the originating node with the redirection number (Station C) and the reason for redirection.

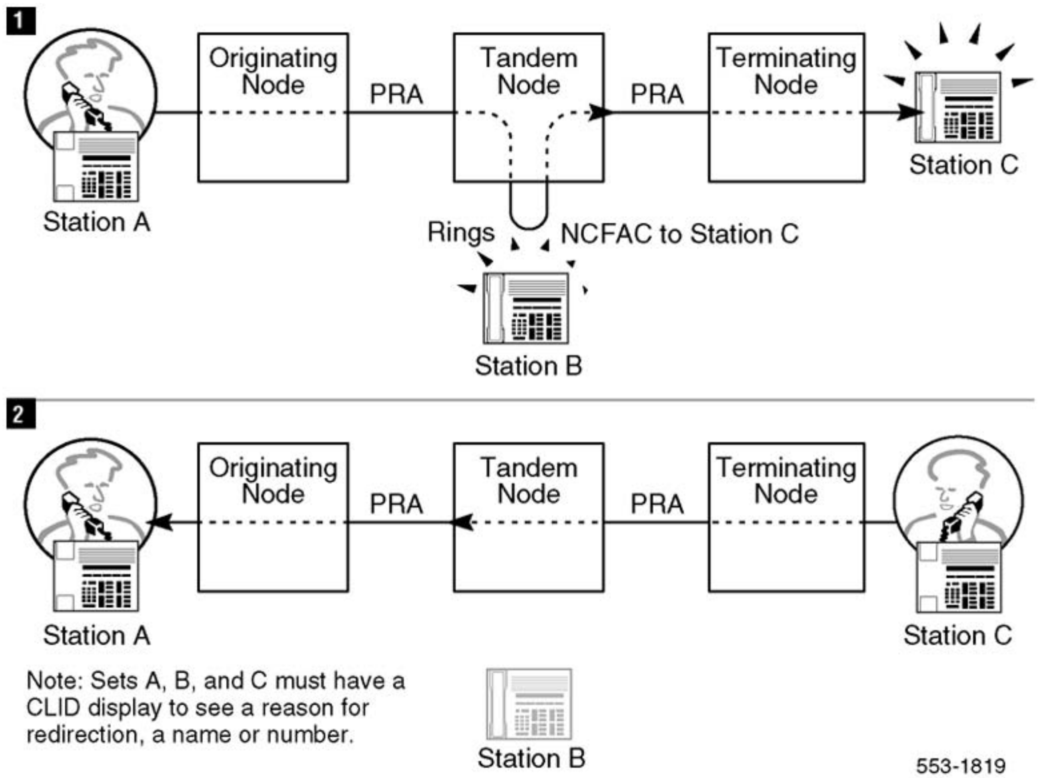

Figure 28: Tandem NCFNA

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

Call Forward, Break-In and Hunt Internal or External Network Wide

The treatment of a call following a call transfer (Call Forward/Hunt by Call Type) is based on the transferring phone and the call originator's phone. The phone display on network call modification or redirection does not change.

DPNSS1 Route Optimisation/MCDN Trunk Anti-Tromboning Interworking

If Network Call Redirection is not configured in a DPNSS1/MCDN gateway, the displays are updated normally, since the RO/TAT Interworking feature is not affected.

If Network Call Redirection is not configured in an MCDN/DPNSS1 gateway, the displays are not updated on the bridged phones on the MCDN side. However, if the bridged phones are on the same node, the displays are updated, even though NCRD is not configured.

EuroISDN Trunk - Network Side

It is possible to have a phone Call Forward, Call Forward No Answer or Hunt to an external number over a EuroISDN Trunk - Network Side connectivity ISDN PRI or ISDN BRI trunk. It is also possible to transfer or conference a call to an external number over a EuroISDN Trunk - Network Side connectivity ISDN PRI or ISDN BRI trunk. Access restrictions can block some transfers from being completed.

Notices of call redirection or call modification are not transmitted over a EuroISDN Trunk - Network Side connectivity.

INIT ACD Queue Call Restore

Call information associated with Network Call Redirection is lost after system initialization and call restoration.

ISDN QSIG Basic Call

When a call is terminated on the system and Network Call Redirection (NCR) is active, the QSIG Basic Call can still operate; however, the original called number and redirection number IE that are used by NCR will not be sent on the QSIG interface.

Non-ISDN Trunks

If the call is forwarded over DTI/Analog trunks, the redirection information will not be carried over, as DTI/Analog trunks do not have the ability to carry redirection information.

If the call is CFNA over DTI/Analog trunks, and if the call cannot terminate on the forwarded to party, the call drops.

Feature packaging

There are no packaging requirements specified for this feature.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

Table 91: LD 15: Forward calls to a forwarding DN.

Prompt	Response	Description
REQ	CHG	Change existing data block.
TYPE	CDB RDR	Customer Data Block. Call Redirection data (Gate opener).
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
- FNAD	FDN	Call forward no answer DID calls—Flexible CFNA DN.
- FNAT	FDN	Treatment for External CFNA calls (non-DID—when FDN is selected, CFCT handles the call.
- FNAL	FDN	Requests treatment for CFNA—when FDN is selected, DID calls are forwarded.

Table 92: LD 16: Allow Network Call Redirection.

Prompt	Response	Description
REQ	CHG	Change
TYPE	RDB	Route Data Block
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
NCNA	(NO) YES	Network Call Name is (is not) allowed.
NCRD	(NO) YES	Network Call Redirection. Allows network call redirection messages to be sent (or blocks messages if NCRD= NO)
		Network Call Redirection can occur without answering YES to the NCRD prompt. This prompt only controls the sending of Network Call Redirection messages, not the actual redirection of the call. The message supplied when NCRD = yes provides the information for the CLID display. When NCRD is NO, the call is redirected without the CLID redirection information.
TRO	(NO) YES	Trunk Optimization
		TRO economizes trunk use throughout the network as part of the NCRD feature.

Table 93: LD 95: Display the reason calls are redirected.

Prompt	Response	Description
REQ	CHG	Change
TYPE	CPND	Call Party Name Display data block
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		

Prompt	Response	Description
DES	(NO) YES	Designator for Multiple Appearance DNs allowed.
RESN	YES	Allow display of reason for redirecting calls
CFWD	(F) xxxx	Display mnemonic for (Network) Call Forward All Calls. Default is "F." Enter the mnemonic that represents NCFAC on a phone's CLID display.
CFNA	(N) xxxx	Mnemonic for (Network) Call Forward No Answer display. Enter the mnemonic that represents NCFNA on a phone's CLID display. Default is "N."
HUNT	(B) xxxx	Mnemonic for Network Hunting display
PKUP	(P) xxxx	Mnemonic to allow Call Pickup display
XFER	(T) xxxx	Mnemonic for Call Transfer display

Table 94: LD 95: Give each DN a name.

Prompt	Response	Description
REQ	CHG	Change
TYPE	NAME	Call Party Name Display name entry
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
DIG	xxx xx	An existing Dial Intercom Group number (0-253) and member number (0-99)
NAME	aaa...a	CPND name using ASCII characters. The DIG prompt is reprompted. Enter <CR> to get the DN prompt.
DN	xxxx	DN of eligible type.

Table 95: LD 10: Enable the appropriate feature in the data block.

Prompt	Response	Description
REQ	CHG	Change
TYPE	500	Analog (500/2500-type) phone
HUNT	xxxx	Hunt DN for internal calls.
FTR	EFD xxx	External Flexible call forward DN.
		Only allowed if LD15 is properly configured: FNAD = FDN FNAL = FDN FNAT = FDN

Prompt	Response	Description
		If the DNXP package is equipped, up to 7 digits are allowed; otherwise, only 4 digits can be entered. Accepted only if CLS is MWA or FNA.
	EHT xxxx	External Hunt DN.
		Only allowed if CLS = CFTA.
		Same digits defined as above.
	FDN xxxxxxx	Flexible Call Forward No Answer DN (cannot be an LDN).
		Same digits defined as above.

Table 96: LD 11: Enable the appropriate feature in the data block.

Prompt	Response	Description
REQ	CHG	Change
TYPE	xxxx	Enter phone type
FDN	x..x	Flexible CFNA DN where xx is the MCDN. The FDN value should include AC1/AC2 when applicable (up to 13 digits).
EFD	xxxx	Network CFNA DN for External calls.
HUNT	xxxx	Network Hunt DN for calls with CLS = CFTD.
EHT	xxxx	Network Hunt DN for External calls.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 21: Network Call Transfer and Network Extended Calls

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Network Call Transfer and Attendant Extended Calls display the calling party name and number to the "Transferred to "extended to" party across the network. Also, if NCPND is optioned, the calling party's display is updated to show the connected party's name and number.

Note:

Network Call Transfer over PRI does not provide the ESN Network Transfer feature. This feature eliminates tandem trunk connections that double back over the same route. PRI Network Transfer allows calls to be blindly transferred across the ISDN network.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature is included in base System Software.

Feature implementation

There are no specific implementation procedures for this feature.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 22: Network Drop Back Busy and Off-hook Queuing

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Network Drop Back Busy (DBB) feature allows network calls that are blocked at a tandem node to be rerouted (dropped back) to the originating node. The calls are then directed over an alternate route. The Network Off-Hook Queuing (OHQ) feature allows Off-Hook Queuing to be configured at a tandem node, thereby allowing Off-Hook Queuing at that node.

Both DBB and OHQ give the originating node control over the routing of all outgoing network calls.

The DBB and OHQ capabilities are only supported over an ISDN network. When DBB and/or OHQ is configured, an ISDN call to a tandem node might encounter one of the following conditions.

Table 97: Conditions and treatments of an ISDN call to a tandem node, with DBB and/or OHQ configured

Configuration	Condition	Treatment
IDBB	All routes in initial (I) set busy	Drop back to originating node.
IDBB	All routes in "I" set and extended (E) set busy	If all routes in "I" set busy, attempt routing over "E" set. If all routes in "E" set are busy, drop back to originating node. This is the default configuration.
OHQ, IDBB	All routes in "I" set busy	Off-hook queue. If OHQ timer times out, drop back to originating node.
OHQ, IDBB	All routes in "I" set and "E" set busy	Off-hook queue to "I" set. When OHQ timer times out, attempt routing over "E" set. If all routes in "E" set are busy, drop back to originating node.

An Initial set of routes (I set) are those routes in a route list which have been customer-defined for a node as being inexpensive. The system attempts to complete a call over these routes before testing for queue eligibility. An Extended set of routes (E set) are those routes in a route list that are not part of the initial set. These routes are usually designated as expensive. The system attempts to complete a call over the E Set routes only when the I set queuing times out.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

Off-Hook Queuing

Message Intercept

If the Message Intercept feature is equipped, a caller in an off-hook queue can receive the message intercept voice response rather than the Off-Hook Queuing tone.

Drop Back Busy

Remote Virtual Queuing

Drop Back Busy (DBB) and Remote Virtual Queuing (RVQ) are both packaged under Originating Routing Control/Remote Virtual Queuing (ORC-RVQ) package 192. If DBB and RVQ are both configured, DBB will take precedence over RVQ. If the user wishes to activate RVQ, DBB must be disabled for a route entry in response to the IDBB prompt. If the user wishes to activate DBB, it must be enabled by entering DBI or DBA. Refer to the "Feature administration" section in this feature module for more information.

Network Attendant Service

Network Attendant Service (NAS) routing takes precedence over DBB.

Feature packaging

This feature requires the following packages:

- Basic Routing (BRTE) package 14
- Network Class of Service (NCOS) package 32
- Network Alternate Route Selection (NARS) package 58
- Flexible Call Back Queuing (FCBQ) package 61

- Off-hook Queuing (OHQ) package 62 for Off-Hook Queuing
- Integrated Services Digital Network (ISDN) package 145
- 2.0 Mbit Primary Rate Access (PRI2) package 154
- Network Attendant Service (NAS) package 159
- ISDN Supplementary (ISDNS) package 161
- Originating Routing Control/Remote Virtual Queuing (ORC-RVQ) package 192 for Drop Back Busy

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 98: LD 87: Allow OHQ Network Class of Service for the customer. on page 208
2. Table 99: LD 86: Configure the originating node for Remote Virtual Queuing. on page 209

Note:

Drop Back Busy (DBB) and Remote Virtual Queuing (RVQ) are both packaged under the Originating Routing Control/Remote Virtual Queuing (ORC-RVQ) package 192. If DBB and RVQ are both configured, DBB will take precedence over RVQ. If the user wishes to activate RVQ, DBB must be disabled for a route entry in response to the IDBB prompt. If the user wishes to activate DBB, it must be enabled by entering DBI or DBA.

Table 98: LD 87: Allow OHQ Network Class of Service for the customer.

Prompt	Response	Description
REQ	CHG	Change existing data
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	NCTL	Network Control
SOHQ	YES	Allow system (customer) Off-hook queuing
- OHTL	nn	Off-hook queue time limit

Prompt	Response	Description
SCBQ	(NO) YES	Allow (disallow) system (customer) Call Back queueing
...		
NCOS	nn	Network Class of Service number. The originating phone must have the same value.
- OHQ	(YES) NO	Off Hook Queuing (allowed) not allowed for this NCOS Both RVQ and OHQ can be enabled on a system. Only one can be activated at a time.
- CBQ	(NO) YES	Call Back Queueing allowed (not allowed) for this NCOS
- RETT	2-(10)-30	Remote Virtual Queuing Retry Timer (Time between searches, in seconds)
- RETC	4-(5)-16	Remote Virtual Queuing Retry Counter (Number of times RVQ searches the initial set before moving on to the extended set)

Table 99: LD 86: Configure the originating node for Remote Virtual Queuing.

Prompt	Response	Description
REQ	CHG	Change
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	RLB	Route List Data Block.
RLI	nn	Route List Index.
ENTR	nn	Route List entry number.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...	...	...
IDBB	(DBD) DBI DBA	Enter DBB (Drop Back Busy Disabled). This will disable Drop Back Busy, and enable Remote Virtual Queuing for the customer. Drop Back if Initial set is busy. Drop Back if all routes are busy.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 23: Network and Executive Distinctive Ringing

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Network Distinctive Ringing (NDRG) allows a distinctive ringing cadence to be configured throughout a system network. Distinctive ringing is defined on a route basis. There are four NDRG distinctive ringing cadence indices that can be defined for a route. These indices are contained in the Flexible Tone and Cadences (FTC) table. If one of these indices has been defined for a route and an incoming trunk call over that route terminates on the local node, the terminating phone receives distinctive ringing. If the incoming call tandems to another node through an Integrated Services Digital Network (ISDN) TIE trunk, the terminating phone at the terminating node receives distinctive ringing. This occurs if the TIE trunk has been marked as distinctive and if the NDRG feature is equipped at the terminating node; otherwise, normal ringing is given.

Executive Distinctive Ringing applies to both network and stand-alone environments. This feature allows a Class of Service to be entered for a phone, marking the phone as "executive". When a call is made from an executive phone, the called phone is rung distinctively. This feature uses the distinctive cadences introduced by the Network Distinctive Ringing (NDRG) feature.

One of five Classes of Service can be entered – EXR1, EXR2, EXR3, EXR4, or EXR0. EXR is the Class of Service mnemonic that marks the phone as executive, and the digits one to four indicate which of the four distinctive ringing cadences is to be applied. EXR0 is the default; it marks a phone as normal.

Operating parameters

Both Network Distinctive Ringing and Executive Distinctive Ringing can be equipped for a phone. In this case, a cadence that is selected for NDRG can also be selected for EDRG.

Within a network, if there are five routes marked as distinctive, and if an incoming call tandems between two nodes that are connected by a single TIE trunk, the terminating node can provide unique distinctive ringing for only four of the five routes. The originating node can provide unique distinctive ringing to all five routes since each route can use a different Flexible Tone and Cadence (FTC) table.

Feature interactions

Incoming trunk

An incoming trunk call that is redirected or attendant-extended will ring distinctively at the terminating phone, according to the cadence index of the originating trunk route. If the terminating phone is located at another node, it will ring distinctively according to the cadence index of the originating trunk route (if the NDRG feature is equipped at the terminating node).

Buzz

Network Distinctive Ringing and Executive Distinctive Ringing do not affect the buzzing of a phone.

Conference

If a new party is to be included in an established conference, the ringing that is applied to the phone of the new party depends on the phones of the established parties. The system scans the trunks and phones of the conferees for a trunk marked as distinctive or a phone designated as executive. The ringing cadence of the new phone depends on the highest index found by the scan.

Feature packaging

This feature requires the following packages:

- Distinctive Ringing (DRNG) package 74
- Flexible Tones and Cadences (FTC) package 125
- Integrated Services Digital Network (ISDN) package 145
- Network Attendant Service (NAS) package 159
- Integrated Services Digital Network Supplementary Features (ISDNS) package 161
- Executive Distinctive Ringing (EDRG) package 185

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

Table 100: LD 10: Define the distinctive ringing cadence for analog (500/2500-type).

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	500	Type of phone
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
CLS	(EXR0) EXR1 EXR2 EXR3 EXR4	Executive Distinctive Ringing Off 0. Executive Distinctive Ringing On 1. Executive Distinctive Ringing On 2. Executive Distinctive Ringing On 3. Executive Distinctive Ringing On 4.

Table 101: LD 11: Define the distinctive ringing cadence/tone to be used for Meridian digital phones.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	a...a	Telephone type. Type **?** for a list of possible responses.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
CLS	(EXR0) EXR1 EXR2 EXR3 EXR4	Executive Distinctive Ringing Off (0). Executive Distinctive Ringing Tone 1. Executive Distinctive Ringing Tone 2. Executive Distinctive Ringing Tone 3. Executive Distinctive Ringing Tone 4.

Table 102: LD 16: Deny or allow Distinctive Ringing and define Network Ring Index.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	RDB	Route Data Block
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.

Prompt	Response	Description
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
TKTP	aaa	Trunk Type.
...		
DRNG	(NO) YES	Deny or allow Distinctive Ringing.
NDRI	(0)-4	Define the Network Distinctive Ringing Index.

Table 103: LD 56: Define Flexible Tones and Cadences.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	FTC	Flexible Tones and Cadences data block.
TABL	0-31	FTC Table number.
USER	(NO) YES	Print users of this table and tone table values (tone table value only).
DFLT	0-31	Default to existing FTC tone table.
RING	(NO) YES	Change the ringing feature definitions.
...		
- NDR1 PBX	0-255	Network Distinctive Ring 1 cadence for analog (500/2500- type) phones.
- NDR1 BCS		Network Distinctive Ring 1 for BCS Meridian 1 digital phones.
- NDR2 PBX	0-255	Network Distinctive Ring 2 cadence for analog (500/2500- type) phones.
- NDR2 BCS		Network Distinctive Ring 2 for BCS Meridian 1 digital phones.
- NDR3 PBX	0-255	Network Distinctive Ring 3 cadence for analog (500/2500- type) phones.
- NDR3 BCS		Network Distinctive Ring 3 for BCS Meridian 1 digital phones.
- NDR4 PBX	0-255	Network Distinctive Ring 4 cadence for analog (500/2500- type) phones.
- NDR4 BCS		Network Distinctive Ring 4 for BCS Meridian 1 digital phones.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 24: Network Individual Do Not Disturb

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

This feature extends several functionalities of the Individual Do Not Disturb feature to operate within a network environment.

A DN in the Do Not Disturb mode is free to make calls, but appears busy to incoming calls. Incoming Direct Inward Dialing (DID) calls to a DN in the Do Not Disturb mode are intercepted to the local attendant, or the network attendant servicing the call. All other calls receive customer-defined intercept treatment defined in LD 15 (i.e., busy treatment, call routed to the attendant, or call routed to recorded announcement).

An attendant dialing a busy DN receives overflow (the DN can be on the same or different node as the attendant). The attendant can then verify whether or not the DN is in Do Not Disturb mode by pressing the IND DND key on the console; if the associated lamp remains steadily lit, it indicates that the DN is in Do Not Disturb mode. The attendant can then temporarily override Do Not Disturb by activating the Break-in feature.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

Call Forward All Calls

Hunting

Call Forward All Calls, and then Hunting, take precedence over DNDI treatment.

Do Not Disturb - Group

An attendant can receive a visual indication of the state of a phone belonging to Group Do Not Disturb mode, whether this phone is located on the local node or any other network node.

Make Set Busy

The DNDI intercept treatment takes precedence over Make Set Busy indication.

Feature packaging

This feature requires the following packages:

- Do Not Disturb Individual (DNDI) package 9
- Attendant Break-in/Trunk Offer (BKI) package 127
- Network Attendant Service (NAS) package 159

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 104: LD 12: Allow the attendant to override DNDI, and configure the attendant console for DNDI. on page 219
2. Table 105: LD 15: Configure intercept treatment for DNDI. on page 219
3. Table 106: LD 16: Define the route number for DNDI RAN intercept treatment (the same route number defined in LD 15). on page 220
4. Table 107: LD 14: Define the trunks associated with the RAN route. on page 220

Table 104: LD 12: Allow the attendant to override DNDI, and configure the attendant console for DNDI.

Prompt	Response	Description
REQ	CHG	Change existing data.
...		
KEY		Attendant Keys.
	xx BKI	The key number on the Attendant Console assigned to Break-in to DNDI.
	xx DDL	The key number on the Attendant Console assigned for DNDI indication.

Table 105: LD 15: Configure intercept treatment for DNDI.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	INT	Intercept treatment.
...		
- DNDT		DNDI intercept treatment.
	(BST) ATT RAN	Busy tone (default). Attendant. Recorded announcement.

Prompt	Response	Description
- - RRT	0-511	Route number for the recorded announcement, prompted only if the DNDI intercept treatment is RAN. For Large Systems.

Table 106: LD 16: Define the route number for DNDI RAN intercept treatment (the same route number defined in LD 15).

Prompt	Response	Description
REQ	CHG	Change existing data.
...		
RRT	0-511	Route number for the recorded announcement, prompted only if the DNDI intercept treatment is RAN. For Large Systems.
TKTP	RAN	The trunks associated with the RAN treatment.

Table 107: LD 14: Define the trunks associated with the RAN route.

Prompt	Response	Description
REQ	CHG	Change existing data.
...		
TKTP	RAN	The trunks associated with the RAN treatment.

Feature operation

See the Do Not Disturb feature description in *Avaya Features and Services, NN43001-506.*

Chapter 25: Network Intercom (Hot Type D and Hot Type I Enhancements)

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Hot Line enables a designated phone to place calls to a predetermined destination that can be internal or external to the system. The call does not require attendant intervention. When the handset is lifted or when a preprogrammed key is activated, the system automatically dials a preprogrammed DN. Hot Lines access a set of Terminal Numbers programmed by direct entry using LD 11, or by list entry such as System Speed Call (SCC) using LD 18. Once a Hot Line call enters the ringing state, it is the same as a normal call.

There were two types of Hot Line keys (DN-based Hot Type D and Speed Call List-based Hot Type L). This enhancement introduces another type of Hot Line key, Hot Type I, while also providing improvements to the existing Hot Type D. These two improvements function in both stand-alone and network environments.

Hot Type I

An option is available with Hot Type I to provide a No Answer Indication, informing the called party that a Hot Line call was made during the called party's absence. If a Hot Line call cannot be completed on the Hot Line key, the calling party is informed through the phone's display, and the call is completed over the network as a normally dialed call that attempts to terminate on the destination Prime DN.

Hot Type D Enhancement

Hot Type D provides the ability for Meridian digital phones to have two-way intercom calls on specially designated keys (not on the DN keys) with other Meridian digital phones connected to PBXs across a Meridian Customer Defined Network (MCDN) Integrated Services Digital Network (ISDN). A Hot Type D call can terminate in three different modes: Voice, Ringing, and Non-ringing. With the Voice mode, speech path is automatically connected after a short ring. With Ringing and Non-ringing modes, the call must be manually answered by the called party. The difference between the two modes is that for Non-ringing no audible tone is given, but the Hot Line key flashes to indicate the call.

Hot Type D allows more than one phone to have the same target DN defined for the Hot Type D key. This enhancement includes Voice, Ringing, and Non-ringing termination modes, as well as the capability to leave a No Answer Indication in some situations (i.e., the Hot Line key winks). A call terminating on an enhanced Hot Type D key operates the same as if it is terminating on a Hot Type I key (if the originating DN is the same as the target DN defined for the key). If it is not the same, but another Hot Line key exists on the phone that has a target DN that matches the originating DN, a No Answer Indication is left on that key.

Note:

When configuring two-way Hot Type D keys in voice mode, the fact that the CLID does not transmit the originator's Hot Type D DN between ISDN locations must be taken into account; it contains the prime DN of the originating phone, and not the originator's Hot Type D DN. Therefore, ringing can occur on the Hot Type D key rather than immediate answer, since a match could not be found for the originator's Hot Type D DN. For this reason also, when the configured mode is either voice, ringing, or non-ringing, a "No Answer Indication" is not left on called phone of a two-way Hotline. It is, therefore, recommended that the Hot Type I be used for a two-way Hotline, since it relies only on the prime DN.

Operating parameters

Hot Type I calls are not allowed on analog (500/2500-type) phones.

A Hot Line key should not be defined on a station without a Prime DN and likewise should not be defined on the primary key. If this is not done, the improved functionality will not work and the call is treated as a non-Hot Line call.

The network DN for Hot Type I and Hot Type D (when the No Answer Indication applies) must be either a Coordinated Dialing Plan or a Universal Dialing Plan number that must terminate on a Prime DN of a Meridian digital phone; otherwise, the call is completed as a non-Hot Line call.

The network-wide application of Hot Type I is only applicable to nodes in a Primary Rate Interface (PRI), ISDN Signaling Link (ISL), Virtual Network Services (VNS), and Basic Rate Interface network.

If the termination mode is voice, the called party is idle, and the handsfree voice call (HVA in LD 15) is active, there is no indication to the software that the called party really answered the call. If any other key is pressed, the No Answer Indication is not left.

Hot Line keys must be defined with the same dialing plan.

Feature interactions

Attendant Blocking of DN

A Hot Type I key cannot be blocked by the attendant because it has no DN.

Pressing a Hot Type D key that is attendant blocked establishes the call on the source side of the attendant.

Auto Hold

If a user who originated a Hot Type I call receives or makes another call on another DN, pressing that DN puts the established call on hold. If a user presses the Hot Type I key while a call is established on it, the call is placed on hold. If the Hot Type I key is pressed while a call is established on another DN, the established call is put on hold. If a station with automatic hold allowed Class of Service receives a Hot Line call, the user of that station can put the active call on hold by pressing the Hot Type I key or by making or answering another call on another key.

Automatic Call Distribution (ACD)

Hot Type I calls cannot terminate on an ACD DN. A call attempting to terminate on an ACD DN receives an overflow tone. Hot Line calls involving ACD phones must use the Hot Type D option.

Busy Forward Status (BFS)

In a Secretarial Filtering scenario, the secretary's BFS lamp also will reflect that the boss's phone is busy if the boss is on a Hot Type I call.

Call Forward

Hot Type I calls respect or override all kinds of Call Forward features (Busy, No Answer, All Calls, Internal, etc.) according to per-set definitions. If Call Forward is respected, the call becomes a normally dialed call, and the originator will receive the appropriate indication on their display.

Call Join

Hot Type I calls can be moved to the Conference key with the Call Join feature.

Call Park

Hot Type I calls cannot be parked.

Call Party Name Display

Hot Type I calls display names the same way as a normal call.

Hot Type I calls that become a normal call indicate on the originating station's display that the call is no longer a Hot Line call.

Call Pickup

Hot Type I calls cannot be picked up. An attempt to pick up a Hot Type I call results in an overflow tone.

Call Transfer

Hot Type I calls can be transferred to another Hot Line key or to a normal DN key; likewise calls on a normal DN key can be transferred to a Hot Line key.

Conference

A Conference call can involve a mixture of intercom and regular DN keys.

Display Key

Hot Type I calls are supported by the Display key feature; pressing the Display key and then the Hot Type I key will show the target DN on the originating station's display.

Do Not Disturb (DND)

Hot Type I calls ignore the Do Not Disturb feature. Hot Line calls are presented to the defined target, even when DND is activated.

Flexible Feature Code (FFC) Boss Secretarial Filtering

Hot Type I calls override this feature (i.e., Hot Type I calls are not filtered by FFC Boss Secretarial filtering). The call terminates on the Boss' phone and is not forwarded to the secretary.

FFC Boss Secretarial Filtering takes precedence over enhanced Hot Type D calls. In this case, if FFC Boss Secretarial Filtering is active, calls terminate on the secretary's phone.

Last Number Redial

A Hot Line key cannot be redialed using the Last Number Redial feature.

Make Set Busy

Hot Type I calls terminating on a station in the Make Set Busy mode override Make Set Busy.

Multiple Appearance Redirection Prime (MARP)

If more than one phone is allocated the same prime DN, the Hot Type I call will terminate on the phone designated as the Multiple Appearance Redirection Prime (MARP). If the MARP DN is not the prime DN on the phone, or if the phone designated as the MARP DN is not a Meridian digital phone, the first Meridian digital phone with the prime DN will be used. If none of these conditions are met, the call will terminate as a non-Hot Line call, and the calling party will be notified on the display.

Hot Type D calls can have voice termination only on a MARP Terminal Number (TN), or if there is no MARP TN, then on the first TN in the TN list. A No Answer Indication for Hot Type D can only be left on the MARP TN, or if there is no MARP TN, then on the first TN in the TN list.

Override

An internal Hot Type I call never returns busy, unless the call became a non-Hot Line call due to the Hot Line key being busy. In this case, the call behaves like a normally dialed call, and Override can be used upon receipt of a busy signal.

Ring Again

Hot Line calls terminating on a busy key become normal calls. Hence, they can use the Ring Again feature under normal circumstances.

Ring Again - No Answer

If Ring Again No Answer is activated for a Hot Type I call, it is activated as though the call had been dialed normally.

Ringing Change Key

The ringing/non-ringing mode of an enhanced Hot Type D or of a Hot Type I key is not changeable by using the Ringing Change Key feature.

Vacant Number Routing

Hot Type I keys and enhanced Hot Type D keys support Vacant Number Routing.

Feature packaging

The following packages are required for Network Intercom (Hot Type D and Hot Type I Enhancements):

The Network Intercom (Hot Type D and Hot Type I Enhancements) feature is included in Enhanced Hot Line (HOT) package 70

For Hot Type I in an ISDN network the following packages are required:

- Integrated Services Digital Network (ISDN) package 145
- Advanced ISDN Network Services (NTWK) package 148
- at least one of Integrated Services Digital Network Signaling Link (ISL) package 147; ISDN Primary Rate Access (PRA) package 146; 2.0 Mbit Primary Rate Interface (PRI2) package 154; Virtual Network Services (VNS) package 183; ISDN BRI Trunk Access (BRIT) package 233

DNPSSS1 connectivity for Hot Type D requires:

- Integrated Digital Access (IDA) package 122
- Digital Private Signaling System 1 (DPNSS) package 123

R2MFC connectivity for Hot Type D requires Multifrequency Compelled Signaling (MFC) package 128.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 108: LD 11: Define Hot Type D and I keys and Classes of Service. on page 227
2. Table 109: LD 95: Configure the Calling Party Name Display. on page 228

Table 108: LD 11: Define Hot Type D and I keys and Classes of Service.

Prompt	Response	Description
REQ	NEW	Add new data.

Prompt	Response	Description
	CHG	Change existing data.
TYPE	a...a	Telephone type. Type **?** for a list of possible responses.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
CLS	FICA (FICD) NAIA (NAID)	Forward Hot Type I allowed. Forward Hot Type I denied. No Answer indication allowed. No Answer indication denied.
...		
KEY	nn HOT D dd target_num hot_dn	Two-way Hot Line type D Key. nn = key number. dd = number of digits dialed. target_number = terminating DN (31 digits maximum). Hot_dn = two-way Hot Line DN.
	R V N (H)	Termination mode: Ringing Voice Non-ringing Hot Line
KEY	nn HOT I dd target_number	Hot Line type I key. nn = key number. dd = number of digits dialed. target_number = terminating DN (31 digits maximum).
	(V) N R	Termination mode: Voice Non-ringing Ringing

Table 109: LD 95: Configure the Calling Party Name Display.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	CPND	Calling Party Name Display.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
- NITC	aaaa (NI)	Non-Hot Line call. Indicates that the Hot Line call terminated as a normal call.

Feature operation

Press the Hot Type I or D key to initiate a Hot Line call to a target DN (the DN can be an external DN in an MCDN ISDN network). The called party answers the call by pressing their Hot Type I or D key if configured. If the called party has no Hot Type I or D key configured, the call will behave as a normal call and is answered accordingly.

If the called party does not answer, and has No Answer Indication Allowed Class of Service, the Hot Type I or Hot Type D key winks as a form of No Answer Indication.

Chapter 26: Network Message Services

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Network Message Services (NMS) uses ISDN signaling capabilities to provide messaging services across an ISDN network. Systems interconnected with PRI or ISL can extend supported message services to all users within that network on a customer basis from a single, central location. Access to NMS and feature activation from the messaging system is transparent to the end user.

A second distinct application, NMS-Meridian Mail (NMS-MM), is introduced to provide end-user and calling party access to centralized Meridian Mail services across the network.

NMS functions common to both applications are described here and details specific to each are described later in this module. Differences between Message Center and Meridian Mail functions are described under their respective headings.

Within NMS operations, there are direct message calls and indirect message calls:

- Direct calls are initiated by the user accessing the Message Center to receive messages. Access is allowed by dialing the message facility directly or using the Message Waiting Key (MWK).
- Indirect calls occur when a redirection feature directs the call to a Message Center so the caller can leave a message.

An NMS call has two components: basic PRI call signaling and transaction signaling. The PRI portion of the call is supported by ISDN PRI or ISL and Network Call Redirection (NCRD)—subject to the requirements for PRI calls and the NCRD feature. NMS always uses non-call-associated, connectionless Transaction Signaling messages to turn on/off the user set Message Waiting Indication (MWI) and to transport call information for certain Meridian Mail features, including Call Sender (that is, the transport of connectionless signaling information across the ISDN network).

There are three types of network nodes supporting NMS:

- Originating node. For direct calls, the originating node is the PBX where the calling party resides. For indirect calls, the originating node is the node where the originally dialed party resides.
- Tandem node. This switch can pass transaction signaling messages on to the next PBX. Stations on a tandem node do not have access to Network Message Services functionality.
- Terminating node. This is the PBX where the Message Center or Meridian Mail server resides, and where the call terminates.

NMS supports Coordinated Dialing Plans (CDPs) and Uniform Dialing Plans (UDPs). All nodes must conform uniformly to the adopted dialing plan. NMS does not support mixed CDP/UDP across a network and limits CDP support to Distant Steering Codes.

Network Message Services - Message Center

Network Message Services-Message Center (NMS-MC) allows a caller transparent access to a centralized message center over an ISDN PRI/ISL network.

These Message Center configurations are supported:

- ACD Message Center
- DN Message Center
- Attendant Message Center

For these types of Message Centers, the Message Indication Key (MIK) on a message taker's phone is used to turn on Message Waiting Indication at a user phone. The Message Cancellation Key (MCK) is used to turn off Message Waiting Indication.

The NMS-MC supports direct and indirect NMS-MC access across ISDN. Direct access is initiated by dialing the Message Center DN or pressing the Message Waiting Key (MWK). Indirect access occurs when a call is presented to the NMS-MC by any of the call redirection features supported by Network Call Redirection (NCRD) including

- Network Call Forward All Calls
- Network Call Forward No Answer
- Network Call Forward Busy
- Network Hunting

See the NCRD module in this document for further details.

Network Message Services - Meridian Mail

NMS-MM provides transparent access to the Meridian Mail system across the network. NMS-MM operates only between system machines supported by a single Meridian Mail server facility. Users on remote nodes configured as part of the NMS-MM server base have access to all the Meridian Mail features available on the local switch.

See the NCRD module when you consider the redirections that apply to your particular environment. Since Message Center support is on a customer-by-customer basis, configure your network accordingly. See *Avaya Hospitality Features Fundamentals, NN43001-553*. In Meridian Mail applications, different network PBXs (nodes) must be configured with the same Meridian Mail server for proper messaging support. See the Meridian Mail suite of technical documents.

Direct calls for NMS-MM are initiated by dialing the message facility directly or pressing MWK on a properly programmed phone. Functionality mimics current operations, including Auto-login with a user's password. See the appropriate technical documentation for a description of call functions.

Indirect calls are presented to the Meridian Mail server from call redirection services. NMS-MM relies on Network Call Redirection (NCRD) to provide the originally dialed and calling party numbers to the Meridian Mail server for message processing. NMS-MM supports Off-net Access through direct dialing.

Table 110: Network Message Services DN (applies to both NMS- MC and NMS- MM) on page 233 summarizes parameters associated with the numbering plan.

Table 110: Network Message Services DN (applies to both NMS- MC and NMS- MM)

Call type	Network Message Services DN (NMS- DN)	Number of digits
Private call using Uniform Dialing Plan (UDP)	ACC + LOC + XXXX	8 to 9
Private call using Coordinated Dialing Plan (CDP)	DSC + X..X	10 maximum
Public numbering plan	ACC + (1) + NPA + NXX + XXXX ACC + (1) + NXX + XXXX	14 maximum

Network Message Services - SIP MWI

By default, MWI is supported over SIP with CS 1000 endpoints using Meridian Mail or Avaya CallPilot. There may be a requirement to use the Notify method for MWI (for example, HMS or MCS) when the voicemail is located on a CS 1000 node. The SIP GW translates the MCDN Facility message to an unsolicited SIP NOTIFY only if the RCAP on DCH configuration has MWI; otherwise, the SIP GW tunnels the MCDN message into a SIP INVITE. RCAP MWI allows the support of SIP Notify method as well as MCDN proprietary signaling. It is recommended that all MCDN D-channels used for NMS have RCAP MWI if SIP trunk routes are controlled by the D-channel.

Operating parameters

The following list describes the NMS operating parameters:

- Password Suppression is not supported across a system network.
- Packet Transport Equipment Meridian Mail (MP) is not supported.
- Multiple Message Center interworking is not supported.
- PRI or ISL is needed for both direct and indirect Message Center calls.
- The NMS DN must be unique and still be able to be reached by means of PRI or ISL from all NMS users in the network, and vice versa.
- NMS supports system to system connections only.
- The local NMS-MM DN defined in each node must also be configured in the Meridian Mail server database, in the VSDN table.
- In-band End-to-End Signaling (EES) is required for NMS-MM at terminating and originating nodes.
- NMS-MM requires the Meridian Hospitality Voice Services package to provide link recovery enhancements for Meridian Link ISDN/AP.
- NMS-MM does not support international dialing.
- Only one Message Center DN can be defined for a phone. Multiple Message Center types are not supported.
- The NMS does not support Trunk Steering Codes (TSCs).

The context sensitive keys on M2317, M3000, and M3900 telephones are updated when Avaya CallPilot or Meridian Mail answers a call. Context sensitive keys on M3900 telephones show the words "play, stop, next, delete", for example, when a call is placed to the voice mail system over PRI TIE trunks and is answered by a Meridian Mail or CallPilot Virtual Agent.

Important:

The NMS feature uses non-call associated ISDN Facility message. Therefore, digit manipulation through DMI or IDC tables can inhibit feature operation. The ORG6 and the DES6 in the FAC message must be directly translatable and the user must be able to dial in both directions: the source and the target PBX.

Feature interactions

Listed here are differences in networking applications, which can impact Network Message Services operations.

Password Suppression

Password Suppression is not supported across a system network.

Network Call Redirection (NCRD)

Indirect access to the NMS-Meridian Mail (NMS-MM) application is based on the NCRD package, which is broken down into the following areas:

- Call Forward All Calls and Call Forward No Answer and Call Forward Busy, Network Call Transfer, and Network Hunting provide the base for NMS indirect access.
- Attendant Extended Call presents the same information to Meridian Mail as Network Call Transfer except that the DN Update message is sent to the NMS-MM when the attendant releases the call. The connected party number is updated only when the attendant is released.
- NMS does not support incoming calls from CO Loop Start trunks. Calls that come into the switch from a CO Loop Start trunk cannot be redirected to another trunk by means of attendant extension or call redirection; these calls are blocked when redirection is activated.

Barge-in Attendant

The attendant can barge-into an NMS-MM call at the terminating PBX. During barge-in, the user cannot use features that require switch effort, such as the Call Sender feature.

Trunks

When a call is presented to the NMS-MM by means of a non-PRI or ISL trunk, the call is treated as an external call even if it is an on-network call. The external greeting is applied and the message is announced as from an external number.

Meridian Hospitality Voice Services

NMS-MM requires the Meridian Hospitality Voice Services (MHVS) package to provide Meridian Link ISDN/AP protocol recovery treatment for link applications. All calls to the ACD Night Call Forward (NCFW) DN are redirected to the Meridian Mail server when the ISDN/AP link fails. Call treatment in NMS-MM is identical to the NCFW treatment.

ISDN requires that the network be equipped with either Coordinated Dialing Plan (CDP) or a Uniform Dialing Plan (UDP) throughout, but it does not support a mixture of both.

Feature packaging

The package requirements for Network Message Services-Message Center are different for each node.

The following packages are required for an NMS-Message Center originating node:

- End-to-End Signaling (EES) package 10
- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution Package A (ACDA) package 45
- Message Center (MWC) package 46
- ISDN Signaling (ISDN) package 145
- ISDN Primary Rate Interface (PRI) package 146 or ISDN Signaling Link (ISL) package 147 or 2.0 Mbit Primary Rate Access (PRI2) package 154
- Advanced Network Services (NTWK) package 148
- Network Message Services (NMS) package 175

The following packages are required for an NMS-Message Center tandem node:

- ISDN Signaling (ISDN) package 145
- ISDN Primary Rate Interface (PRI) package 146 or ISDN Signaling Link (ISL) package 147 or 2.0 Mbit Primary Rate Access (PRI2) package 154
- Network Message Services (NMS) package 175

The following packages are required for an NMS-Message Center terminating node:

- End-to-End Signaling (EES) package 10
- Basic Automatic Call Distribution (BACD) package 40
- Automatic Call Distribution Package A (ACDA) package 45
- Message Center (MWC) package 46

- ISDN Signaling (ISDN) package 145
- ISDN Primary Rate Interface (PRI) package 146 or ISDN Signaling Link (ISL) package 147 or 2.0 Mbit Primary Rate Access (PRI2) package 154
- Advanced Network Services (NTWK) package 148
- Network Message Services (NMS) package 175

Note:

BACD (package 40) and ACDA (package 45) are not necessarily required for your particular Message Center application.

Feature packaging for SIP MWI

- End-to-End Signaling (EES) package 10
- Basic ACD (BACD) package 40
- ACD package A (ACDA) package 45
- Message Center (MWC) package 46
- ISDN Signaling (ISDN) package 145
- ISDN Primary Rate Access (PRI) package 146 or ISDN Signaling Link (ISL) package 147 (for system to system
- ISDN Network Service (NTWK) package 148
- Network Message Service (NMS) package 175
- Message Waiting Indication (MWI) package 219

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 111: LD 17: Define the software release of each switch at the far end of each D-channel in the NMS network. on page 238
2. Table 112: LD 15: Enable Message Services on page 238

3. Table 113: LD 16: Create an ISDN transport signaling database. on page 238 These procedures apply to both NMS-MM and NMS-MC, except for LD 23, which applies to Meridian Mail only.
4. Table 114: LD 23: Define Meridian Mail ACD group in the remote switch (NMS-MM only). on page 239 These procedures apply to both NMS-MM and NMS-MC, except for LD 23, which applies to Meridian Mail only.
5. Table 115: LD 10: Define Network Message Services DN for each analog (500/2500-type) phone. on page 240
6. Table 116: LD 11: Define Network Message Services DN for each digital phone. on page 240

These procedures apply to both NMS-MM and NMS-MC, except for LD 23, which applies to Meridian Mail only.

Table 111: LD 17: Define the software release of each switch at the far end of each D-channel in the NMS network.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	Configuration Record.
ADAN	CHG DCH x	Change D-channel information. x = 0-63 (For Large Systems)
-RLS	xx	Enter the software release of the far end.
-RCAP	MWI	Remote virtual D-Channel capability for MWI support over SIP trunk.

Table 112: LD 15: Enable Message Services

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	IMS	Integrated Messaging Service.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
IMS	YES	Change Integrated Message System.
- IMA	YES	Enable Integrated Message System.

Table 113: LD 16: Create an ISDN transport signaling database.

Prompt	Response	Description
REQ	NEW	Add new data.

Prompt	Response	Description
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
- ISDN	YES	ISDN option.
- - PNI	1-32700	Customer private identifier—unique to a customer. This is the private identifier of the target switch and must be the same number used for PNI in LD15 for remote customer. Matches PNI in LD16 at remote to PNI in LD15 at local site.
- NCRD	YES	Network Call Redirection
- - TRO	YES	Trunk Route Optimization allowed (denied) on the route.
- INAC	(NO) YES	Insert Access Code. INAC = YES is required for ISDN network features. This prompt only appears if the route type is a TIE trunk.

Table 114: LD 23: Define Meridian Mail ACD group in the remote switch (NMS-MM only).

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ACD	Automatic Call Distribution data block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ACDN	x..x	The Meridian Mail DN.
MWC	YES	Message Center services.
MAXP	xxxx	Maximum number of agent positions.
...		
NCFW	x..x	Night Call Forward DN, where x...x is the NMS-DN. If network DN, include AC1/AC2.

Prompt	Response	Description
		Do not define any ACD agents for this ACD group to allow automatic redirection to the ACD Night Call Forward DN (NFCW).

Table 115: LD 10: Define Network Message Services DN for each analog (500/2500-type) phone.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	500	Type of phone.
TN		Terminal number
	l s c u	Format for Large System, Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
DIG	0-253 0-99	Dial Intercom Group number and Member number.
CLS	MWA	Class of Service
FTR	FDN x..x	Flexible Call Forward No Answer NMS-DN, x..x is the NMS-DN. The NMS-DN can be the local or the network DN. If network DN, include AC1/AC2.

Table 116: LD 11: Define Network Message Services DN for each digital phone.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	aaaa	Type of phone.
...		
FDN	x..x	Flexible Call Forward No Answer NMS-DN. The NMS-DN can be the local or the network ACD DN.
CLS	CFTA HTA	Class of Service required to define EFD and EHT.
...		
EFD	x..x	Call Forward by Call Type - External No Answer to NMS-DN.
HUNT	x	Hunt to NMS-DN.
EHT	x x	Call Forward by Call Type - External Hunt to NMS-DN.
...		
KEY	xx MWK x...x	Message Waiting key, where x..x i s the NMS-DN.

Prompt	Response	Description
		The NMS-DN can be the local or the network ACD DN.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 27: Network Ring Again

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Network Ring Again (NRAG) provides ring again capability within an MCDN PRI/ISL network, or across an ECMA-QSIG or DPNSS1 gateway. NRAG allows a caller at one location to activate Ring Again against a terminating station that is busy at another location.

The NRAG feature operates in "free notification" mode. This means the terminating switch determines when the called party becomes idle and notifies the originating switch.

Once the NRAG feature has been activated, the status of the called party is observed until the line is idle and a new call set-up can be attempted, or until NRAG is deactivated by a timeout or manually disconnected by the caller.

NRAG operates as follows: station A makes a call across an MCDN network, ECMA-QSIG, or DPNSS1 gateway to busy station B. Station A can activate NRAG against station B. When station B becomes idle, free notification is sent to phone A. Station A can then press the Ring Again (RGA) key to call station B.

Note:

If station B has activated Call Forward All Calls to station C, and station C is busy, station A can activate NRAG against station C, if station C is located in the same node as station B.

If a Multiple Appearance Redirection Prime (MARP) is configured for station B, the MARP rules for redirection are applied, with the MARP TN being used to check whether Call Forward All Calls is active. If MARP is not configured, but station B has a Multiple Appearance DN, the first TN from the DN block found to have Call Forward All Calls is used.

When more than one caller activates NRAG on a terminating station, the calls are queued on a first-come, first-served basis. When the called station becomes idle, only the first caller in the queue is signaled. The second caller in the queue is signaled only after the Queue Advance Timer (four seconds) expires.

Operating parameters

NRAG cannot be activated on an Automatic Call Distribution (ACD) termination, because ACD users are serviced by the ACD queue.

Only Call Forward All Calls is supported; any other type of redirection is not supported (including Call Forward All Calls in two or more steps).

Call Forward All Calls is only supported to DNs on analog (500/2500-type) phone or digital phones.

If the terminating station presses the RGA key after receiving free notification, and station B has deactivated Call Forward All Calls in the meantime, station B is rung.

NRAG requires a number of timers to control the feature functions on both the originating and terminating switches. Originating Switch Timers and Terminating Switch Timers show the values defined and which timers are used by the system.

Table 117: Originating Switch Timers

Timer code	Description	Duration
T2	Period for unanswered recall notify	30 seconds
T5	Message Response Timer	4 seconds
T6	Duration Timer	30 minutes
TR2	Recall Suspend Option Timer	9 minutes

Note:

TR2 not applicable to the system

Table 118: Terminating Switch Timers

Timer code	Description	Duration
T7	Duration Timer	30 minutes
GT	Guard Timer	6 seconds
QAT	Queue Advance Timer	4 seconds
Note: GT is not applicable to system.		

Feature interactions

Make Set Busy

NRAG can be originated by a station in the Make Set Busy (MSB) Mode. It can also be activated against a station in the MSB Mode, assuming no Call Forward All Calls DN.

Do Not Disturb

Ring Again, originating from a station with Do Not Disturb (DND) active, is supported; however, NRAG cannot be activated against a terminating station which has DND activated.

Call Waiting

Camp-On

If Call Waiting or Camp-On is active on the terminating station, no notification will be sent to the originating party until the terminating station becomes idle.

Call Forward All Calls

If the originating station activates Call Forward All Calls (CFAC) after activating NRAG, NRAG can still be received.

Data calls

NRAG is supported for data calls.

Calling Line Identification

NRAG is supported only if the Calling Line Identification (CLID) uses the prime DN.

Incoming Digit Conversion

If there is any conversion done to the called DN, NRAG is not supported.

ISDN QSIG Basic Call

Network Ring Again signaling is supported within the Meridian Customer Defined Network only. Network Ring Again requests which go through the QSIG interface will not be supported.

CDP and NARS

For networks with CDP and NARS using the same route, turn off INAC and insert a DMI when needed.

Feature packaging

This feature requires the following packages:

- Background Terminal (BGD) package 19
- ISDN signaling (ISDN) package 145
- Network Ring Again (NRAG) is package 148

This feature requires one the following packages:

- ISDN Primary Rate Interface (PRI) package 146 or
- 2.0 Mbit ISDN Primary Rate Interface (PRI) package 154 or
- ISDN Signaling Link (ISL) package 147; which, if ISL is over DTI/DTI2, requires:
    - 1.5 Digital Trunk Interface (PBXI) package 75 or
    - 2.0 Mbit Digital Trunk Interface (DTI2) package 129

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 119: LD 17: Define the software release ID. on page 247
2. Table 120: LD 15: Set up Private Network Identifier (PNI) mapping between call type translator HLOC, LSC, HNPA, or HNXX for proper CLID construction. on page 247
3. Table 121: LD 16: Set up duration timer (NRAG), Private Network Identifier (PNI), insertion of ESN Access Codes (INAC). on page 248

Table 119: LD 17: Define the software release ID.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Configuration Record.
- ADAN	NEW DCH x	Add a primary D-channel x = 0-63 (For Large Systems)
- CTYP	DCHI MSDL	Card type.
- DNUM	0-15	Device number: physical port (odd) for D-channel on DCH, physical card address for MSDL.
- PORT	0-3	Port number on MSDL card.
RLS	xx	Release ID of the switch at the far end of the D-Channel.

Table 120: LD 15: Set up Private Network Identifier (PNI) mapping between call type translator HLOC, LSC, HNPA, or HNXX for proper CLID construction.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	NET	Networking Data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
- OPT	aaa	Options

Prompt	Response	Description
- AC2	aaa	Access Code 2. Enter call types (type of number) that use access code 2. Multiple call types can be entered. Default is to access code 1.
- ISDN	YES	Change ISDN options
- PNI	1-32700	Customer private identifier—unique to a customer. Within one network, use the same value for PNI in both the Customer Data Block (LD15) and the Route Data Block (LD16) in all PBXs.
	100-999	Area code for the system.
	100-999	Prefix for the Central Office.
	100-999	Home Location Code (NARS).
	1-9999	1- to 4-digit Local Steering Code established in the Coordinated Dialing Plan (CDP). The LSC prompt only appears if user has a 5- or 6-digit dialing plan.

Table 121: LD 16: Set up duration timer (NRAG), Private Network Identifier (PNI), insertion of ESN Access Codes (INAC).

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
...		
CNTL	(NO) YES	Changes to controls or timers.
TIMR	NRAG (30)-240	Network Ring Again duration timer (T6 and T7 timers) —time is in minutes. Currently, only a value of 30 minutes is supported. Package 148, Advanced ISDN Features, is required.
...		
INAC	(NO) YES	Insert Access Code. Permit an ESN access code to be automatically added to an incoming ESN call from a private network. If INAC is YES, the digit insertion option (INST) is bypassed. This prompt only appears if the route type is a TIE trunk.
PNI	1-32700	Customer private identifier—unique to a customer. Within one network, use the same value for PNI in both the Customer Data Block (LD15) and the Route Data Block (LD16) in all PBXs.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 28: Network Signaling on Virtual Network Services

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

The Network Signaling on Virtual Network Services (NSIG on VNS) feature enhances the functionality of Virtual Network Services by supporting Network Signaling on the VNS D-Channel (VNS_DCH).

With VNS, the Public Switched Telephone Network (PSTN) trunk serves as a B-Channel. However, NSIG is not allowed over PSTN trunks; therefore, it is necessary to send NSIG over the D-Channel in order to maintain the Network Class of Service (NCOS) information.

NCOS information is transported through Network Signaling over routes, depending on the value of the Signaling arrangement (SIGO) prompt in the Route Data Block. When SIGO = STD, no NCOS information is sent on the Bearer Channel (B-Channel).

The value of the Virtual Signaling (VSIG) prompt in LD 17 determines whether or not NSIG is supported on the VNS D-Channel. When VSIG = NO, NSIG is not sent over the VNS D-Channel. When VSIG = YES, NSIG is sent over the VNS D-Channel, and the standard ESN5 protocol is used.

VSIG = YES and SIGO is set to STD

In this situation, NSIG is configured on the VNS D-Channel. Two nodes are connected by a VNS D-Channel, and the bearers are TIE trunks connected to the Central Office (CO). When Set A initiates a call to Set B, using the VNS D-Channel, the NCOS of Set A travels over the VNS D-Channel using ESN5 protocol and is present at the terminating node for further access restrictions. No Network Signaling is on the bearer in this case.

VSIG = YES and SIGO is not set to STD

In this situation, NSIG is configured on the VNS D-Channel and on the bearer. When Set A initiates a call to Set B, the NCOS of Set A travels over the VNS D-Channel and on the bearer.

VSIG = NO and SIGO is not set to STD

In this situation, NSIG is not configured on the VNS D-Channel. When Set A initiates a call to Set B, no NCOS information travels over the VNS D-Channel, but will travel on the bearer.

Scenarios involving Satellite (SAT) Routes

When Satellite Routes are involved, NSIG on VNS behaves as shown in the following scenarios.

VSIG = NO and SIGO is not set to STD

Referring to A scenario involving two SAT-Routes where VSIG = NO and SIGO is not set to STD, a call from Node 1 to Node 3 passes a Satellite Route. The route between Node 2 and Node 3 is also a Satellite Route; therefore, the call is blocked at Node 2.

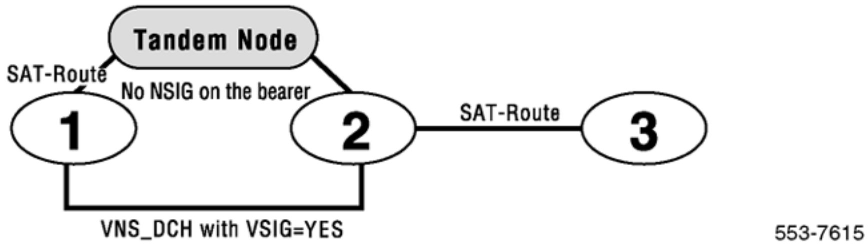

Figure 29: A scenario involving two SAT-Routes where VSIG = NO and SIGO is not set to STD

VSIG = YES and SIGO is not set to STD

Referring to A scenario involving two SAT-Routes where VSIG = YES and SIGO is not set to STD, a call from Node 1 to Node 3 passes a Satellite Route. The route between Node 2 and Node 3 is also a Satellite Route; therefore, the call is blocked at Node 2. The Satellite information is transported over the bearer.

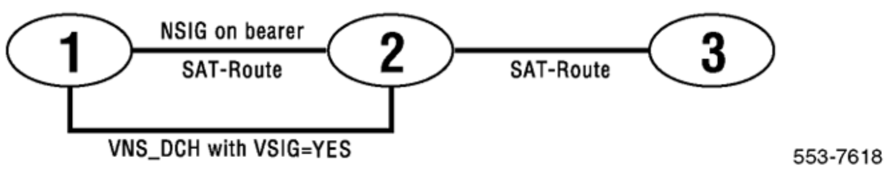

Figure 30: A scenario involving two SAT-Routes where VSIG = YES and SIGO is not set to STD

Referring to A scenario involving two SAT-Routes where VSIG = YES and SIGO is not set to STD, a call from Node 1 to Node 4 passes a Satellite Route. The Satellite Count is updated at Node 2, and the Satellite information is sent to Node 3. The route between Node 3 and Node 4 is also a Satellite Route; therefore, the call is blocked at Node 3.

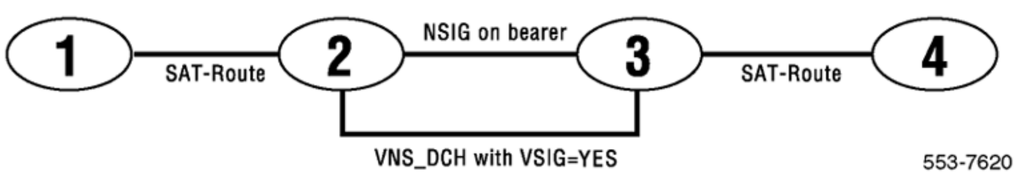

Figure 31: A scenario involving two SAT-Routes where VSIG = YES and SIGO is not set to STD

Referring to A scenario involving two SAT-Routes where VSIG = YES and SIGO is not set to STD, a call from Node 1 to Node 3 is initiated, and the call is blocked at the Tandem Node. In this scenario, the Satellite information is sent from Node 2 to the Tandem Node. The route between the Tandem Node and Node 3 is also a Satellite Route; therefore, the call is blocked on the bearer side of the Tandem Node.

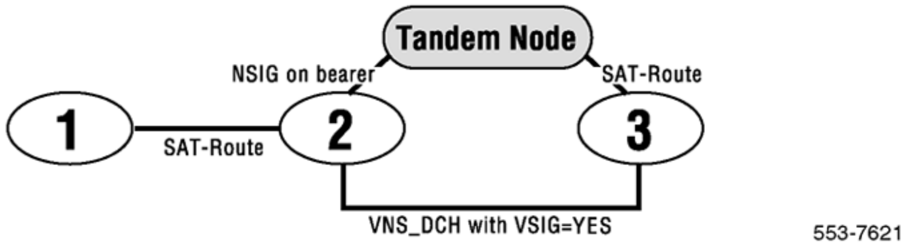

Figure 32: A scenario involving two SAT-Routes where VSIG = YES and SIGO is not set to STD

VSIG = YES and SIGO is set to STD

Referring to A scenario involving two SAT-Routes where VSIG = YES and SIGO is set to STD, a call from Node 1 to Node 4 passes a Satellite Route, and the Satellite Count is updated at Node 2. The Satellite information travels over the VNS D-Channel to Node 3. The route between Node 3 and Node 4 is also a Satellite Route; therefore, the call is blocked at Node 3.

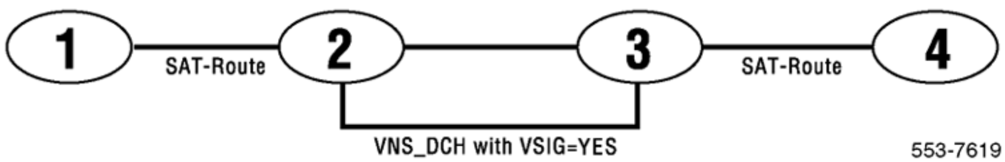

Figure 33: A scenario involving two SAT-Routes where VSIG = YES and SIGO is set to STD

Referring to A scenario involving two SAT-Routes where VSIG = YES and SIGO is set to STD, if NSIG is not configured on the bearer side, the Satellite information is not sent over the bearer. A call from Node 1 to Node 3 passes even if there is a second Satellite Route involved in the call. At Node 3, the only Satellite information received is that which is received over the VNS D-Channel.

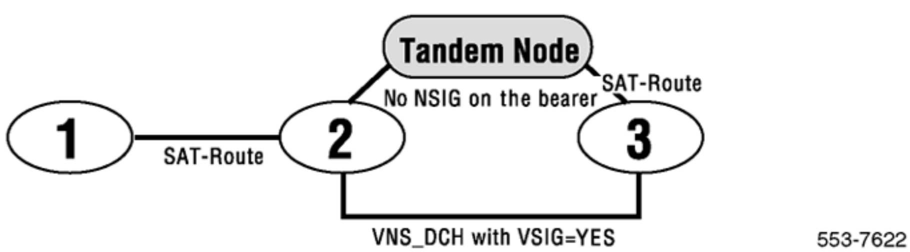

Figure 34: A scenario involving two SAT-Routes where VSIG = YES and SIGO is set to STD

Operating parameters

This feature does not support Call-Back Queuing.

When the NSIG on VNS feature is disabled, the previous functionality exists. In this case, no signaling digits are sent over the VNS D-Channel. However, if configured, NSIG is transported over the bearer.

A non-symmetric configuration is supported for bearer trunks.

The VNS D-Channel only supports the NSIG ESN5-protocol. It does not support EN19 and ETN protocols.

Referring to SAT-count is not updated when NSIG is not configured on the bearer (VSIG = YES and SIGO is set to ST, when NSIG is configured only on the VNS D-Channel, the Satellite Count is not updated if a Satellite Route is passed on the bearer side. A call from Node 1 to Node 3 passes even when there are two Satellite Routes involved in the call. When no NSIG information is sent from the Tandem Node to Node 2, the Satellite information is lost.

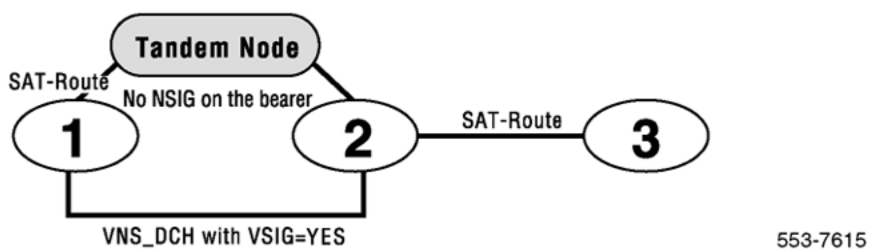

Figure 35: SAT-count is not updated when NSIG is not configured on the bearer (VSIG = YES and SIGO is set to STD)

Referring to A scenario where the call is blocked, as NCOS is insufficient (VSIG = YES and SIGO is not set to STD, in a case where the bearer passes a Tandem Node (Node 2) with NSIG on the route, the call is blocked at Node 2 when the NCOS is insufficient.

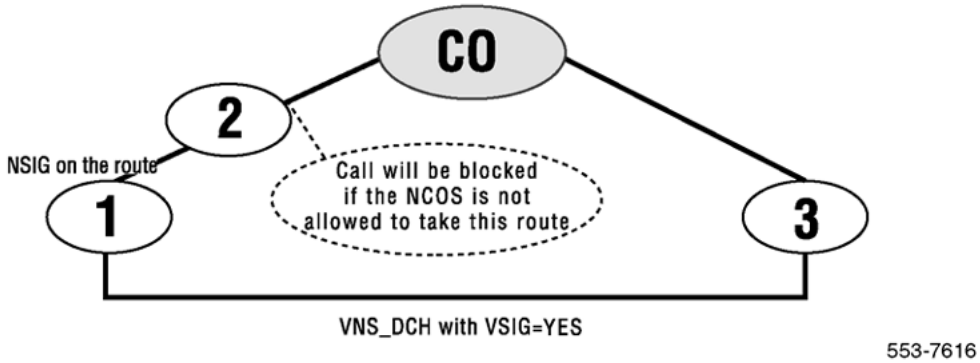

Figure 36: A scenario where the call is blocked, as NCOS is insufficient (VSIG = YES and SIGO is not set to STD)

Feature interactions

NSIG on VNS has no specific interactions with existing features.

Feature packaging

The NSIG on VNS feature requires the following packages:

- Basic Routing (BRTE) package 14
- Network Class of Service (NCOS) package 32
- Network Alternate Route Selection (NARS) package 58
- ISDN Signaling (ISDN) package 145
- ISDN Signaling Link (ISL) package 147
- Advanced Network Services (NTWK) package 148
- Virtual Network Services (VNS) package 183

Feature implementation

Table 122: LD 17: Allow or deny Network Signaling on Virtual Network Services.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Configuration data block
- ADAN	CHG DCH	Change D-Channel information. xx = 0-63 (For Large Systems)
- USR		Type of user.
	VNS SHAV	Virtual Network Services. D-Channel used for VNS or ISLD. Shared Virtual Network Services. D-Channel shared between PRI, VNS, and ISLD.
- - VCRD	YES	Virtual Network Services Network Call Redirection is available over this D-Channel.
- - VTRO	(NO) YES	Trunk Route Optimization before answer is available over this D-Channel for VNS.
- - VSIG	(NO) YES	NSIG on VNS (denied) allowed. When VSIG = YES, the Signaling arrangement is ESN5. When VSIG = NO, the Signaling arrangement is Standard.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 29: Network Tenant Service

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

This feature provides the capability of Network Attendant Service (NAS) on a tenant basis, with network-wide tenant-to-tenant and tenant-to-trunk blocking.

The Multi-location Business Group (MBG) number is the grouping agent used to associate users belonging to a customer group or "sub-group". Network Tenant Service (NTS) uses MBG numbers to define the relationship between the Multi-location Business Group Subgroup (MBGS) number and the tenant number on a particular node. The tenant number related to an outgoing call is translated into the corresponding MBGS number and then transmitted through the network. At the terminating node, the MBGS number is translated back into a meaningful tenant number.

Attendant routing

NTS allows Console Presentation Groups (CPGs) and related attendants to be defined at any node in the Integrated Services Digital Network (ISDN).

Calls can be directed to another node based upon:

- a time of day schedule defined at the CPG level
- overflow conditions
- status of local attendants in the CPG group
- status of trunks to other attendant locations
- status of the NAS key on a customer basis, and
- Night Service indicator of the CPG group

Each Attendant Console group (ACG) can have its own NAS routing table defined. Calls not associated with a particular console group will be presented to ACG 0.

Tenant-to-tenant blocking

It is possible to define tables which allow or deny calls between tenant groups in the same customer group. Normal intercept treatment is given to a station attempting to dial into a denied access tenant.

Tenant to tenant blocking is maintained across the network. Access is allowed or denied according to information defined on the node which currently processes the call.

It is possible with network-wide tenant-to-tenant blocking to define one-way restrictions ("A" cannot call "B", but "B" can call "A"), even though this is not possible in standalone cases. If nodes do not have the same tenant-to-tenant restrictions defined, one-way blocking can result.

Timed Reminder Recalls

Timed Reminder Recalls work in the same way as in NAS, but on a tenant basis. The attendant is chosen based on the tenant number of the target party.

Operating parameters

To ensure correct call routing, all nodes in the ISDN must have the Network Tenant Service feature equipped.

Each ACG can have a NAS routing table, or several ACGs can share the same NAS routing table. However, the NAS key is defined only on a customer basis – it is not a CPG-level parameter. When one Attendant Console activates the NAS key, regardless of ACG, the entire system is in NAS service.

Feature interactions

Intercept Computer Dial from Directory

The Intercept Computer (ICP) Dial from Directory feature only works at the customer level and for a single node. If several tenants are configured in a network situation, they will all be affected by how the ICTD prompt in LD 15 has been configured for the customers on different nodes

Feature packaging

This feature requires the following packages:

- Basic Routing (BRTE) package 14
- Network Class of Service (NCOS) package 32
- Network Alternate Route Selection (NARS) package 58
- Multi-tenant Service (TENS) package 86
- Integrated Services Digital Network (ISDN) package 145
- ISDN Primary Rate Interface (PRI) package 146 or
- 2.0 Mbit Primary Rate Access (PRA) package 154
- Network Attendant Service (NAS) package 159

Note:
Do not equip with Attendant Overflow (AOP) package 56.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 123: LD 15: Define the Multi-Location Business Group value in the Customer Data Block. on page 262

   This value is sent as the Business Group Identifier in the MBG Information Element.

2. Table 124: LD 17: Define a prompt to control whether the MBG parameter is sent on a particular D-channel. on page 263
3. Table 125: LD 86: Define a table number for the NAS routing table. If no table number is entered, table 0 applies the customer. on page 263
4. Table 126: LD 93: Define the relation between a Multi-Location Business Group Subgroup and a tenant number. Assign a NAS routing table with a particular Attendant Console Group. on page 264
5. Table 127: LD 93: Define the relation between a Multi-Location Business Group Subgroup and a tenant number. Assign a NAS routing table with a particular Attendant Console Group. on page 264

Table 123: LD 15: Define the Multi-Location Business Group value in the Customer Data Block.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	NET	Networking data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
…		
- ISDN	(NO) YES	Integrated Services Digital Network (not) allowed for this customer.
- PNI	(0)-32700	Private Network Identifier. Prompted if ISDN = YES.
- MBG	(0)-65535	Multi-Location Business Group. This parameter is used to define the Multi-Location Business Group. 0 = no indication. 1 = reserved for public network. 2-65535 = Business Group Identifiers.
- BSGC	(0)-65535	Business Sub Group Consult-only. 0 = no indication. 1-65535 = Subgroup identifier. This value is sent as the Multi-Location Business Group Subgroup (MBGS) identifier or tenant number when an existing call has more than two different MBGSs. In this case, a consultation connection will be

Prompt	Response	Description
		allowed, but completion of a call modification, such as conference or transfer, will be disallowed.

Note:

If MBGA is set to YES, the MBG will be sent on the D-channel as required. If MBGA is set to NO, the MBG will not be sent on the D-channel. Note that the RLS value in the D-channel data block also prevents the sending of the MBG parameter to versions of the software that do not support MBG.

Table 124: LD 17: Define a prompt to control whether the MBG parameter is sent on a particular D-channel.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN ADAN	Configuration Record. Gate opener.
ISDN	(NO) YES	Integrated Services Digital Network.
…		
- NASA	(NO) YES	Network Attendant Service (disallowed) allowed.
- MBGA	(NO) YES	Multi-Location Business Group messages are allowed to be sent on this D-channel.

Table 125: LD 86: Define a table number for the NAS routing table. If no table number is entered, table 0 applies the customer.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	NAS	Network Attendant Service.
TBL	(0)-63	NAS routing table 0. 0 is the customer routing table. It is associated with ACG 0. Prompted if FEAT = NAS.
ALT	1-7 X1-X7	Alternative number to be defined. Precede with "X" to delete the alternative number.

Table 126: LD 93: Define the relation between a Multi-Location Business Group Subgroup and a tenant number. Assign a NAS routing table with a particular Attendant Console Group.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	TACC	Tenant Access information.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
TEN	1-511	Tenant number.
MBGS	(0)-65535	Multi-Location Business Group Subgroup number associated with this tenant. 0 means no indication.

Table 127: LD 93: Define the relation between a Multi-Location Business Group Subgroup and a tenant number. Assign a NAS routing table with a particular Attendant Console Group.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ACG	Attendant Console Group.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
AGNO	1-63	ACG number.
NTBL	(0)-63	NAS routing table to be used for calls directed to this ACG.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 30: Network Time Synchronization

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Description

The Network Time Synchronization feature is designed to ensure that all time stamps in a network are synchronized from one source. One switch becomes the master for this purpose.

In a private network environment, each switch in the network has an individual system clock. These system clocks can, under certain conditions, lose or gain time, causing inaccurate time stamps for different features.

Also, in a private network, several switches can be located in different time zones. As features become more centralized in a network environment, it is useful to have time stamps based on one time zone.

To provide Time Synchronization on a network-wide basis, Meridian Customer Defined Integrated Services Digital Network (ISDN) nodes can request Time Synchronization from another node, using D-channel messages. Therefore, Slave switches can request the time from the Master switch, while the Master switch can do the same to a Backup node.

A time difference (or delta) is provided for every node, in order to distinguish time zones for time usage by local features (e.g., Automatic Wake-up) and centralized ones (e.g., Centralized Call Detail Recording).

The Time Synchronization request messages are composed of:

- the message identifier
- the requester's ID
- the time
- the date
- the time-adjust factor

IDs are virtual DNs, and are used to route the messages.

On the Slaves, Time Synchronization requests are sent automatically under the background routines (default setup) or with the daily routines (optional setup), every time a time change is performed (to accurately set the seconds), and on every SYSLOAD and initialization.

On the Master, Time Synchronization requests are sent to a Backup node upon initialization and, therefore, after SYSLOAD. The Master will be forbidden to synchronize Slave switches during these backup periods. In the rare event where Master and Backup nodes would start requesting synchronization at the same time, the real time will be considered to be on the Slave node, if it is not initializing. If both nodes are only initializing, the real time would be considered to be carried by the Master switch. If a SYSLOAD occurs at the Master and the Slave is initializing, the real time would be considered to be carried by the Slave switch. A warning message will be printed if both switches SYSLOAD, and all Time Synchronization would be put to a halt until the Master's clock is reset.

If no answer is received on the first time synchronization request (by the end of the request time-out), extra Time Synchronization requests will be sent. If there is still no answer on the third time synchronization request, a warning message will be issued.

Note:

Upon SYSLOAD, the clock starts on time zero, while upon initialization, only the seconds are lost.

Note:

Through service change (LD 2) or through an Attendant Console, the clock can be reset to the correct time if desired. If the Network Time Synchronization feature is on, then the Master will be requested for synchronization upon these service changes (to permit fine synchronization).

Operating parameters

This feature uses D-channel messaging over a Meridian Customer Defined Integrated Services Digital Network (ISDN).

Feature interactions

Time-of-day Adjustment

Every time LD 2 is used to change the system time, a request for synchronization will be made of the Master to accurately set the seconds.

Time and Date (TAD) Attendant key

As done with LD 2, every time the TAD key is used to change the system time, a request for synchronization will be made to the Master to accurately set the seconds.

Call Detail Recording (CDR)

Upon receipt of synchronization messages, Slave switches will issue CDR records (if so equipped) for monitoring the feature. These CDR records will be identical to those issued by a time change performed in LD 2 or by an attendant's TAD key.

Feature packaging

This feature is included with the Integrated Services Digital Network Supplementary Features (ISDNS) package 161.

Feature implementation

The following parameters are used to configure Network Time Synchronization:

- Node Status: Can either be Master, Slave, or standard stand-alone node (MAST, SLAV or STDA).
- Customer Number: Customer that will issue and receive the Network Time Synchronization messages. The default value is "0". For a change (only possible on switches with the multi-customer package) to be accepted, the customer should already exist. Furthermore, the Local DN has to be reentered.
- Local DN: Virtual DN (access code included) dedicated for synchronization services on the Local node; up to 16 digits. A call with these routing digits should terminate on the previously designated customer.
- Master or Backup DN: Virtual DN (access code included) dedicated for synchronization services on the Master or Backup node; up to 16 digits.
- Time Delta: Time difference added to the local time in order to get the Master or Backup time. The entry is prefixed with the digit 1 for positive and 0 for negative.
- Requesting mode: Operating mode used to request the time synchronization messages (i.e., with the background routines (default setup) or with the daily services (BKGD or DSVC)).

Note:

The Node Status, Customer Number, Local DN, and Master or Backup DN parameters must be configured for the Network Time Synchronization feature to be operational.

Task summary list

The following is a summary of the tasks in this section:

LD 2: Define entries for the Network Time Synchronization feature.

The following commands are Network Time Synchronization feature specific:

- **Query Node Status** (Type Time Synchronization Status).

  The command format is:

  INPUTOUTPUT

.TTSS.TTSS (STATUS)

Example:

.TTSS.TTSS MAST

- **Set Node Status** (Set Time Synchronization Status).

The command format is:

.STSS (status)
where status can be:

STDA — stand-alone (default)
MAST — Master
SLAV — Slave

Example:

.STSS SLAV

- **Query Customer in charge** (Type Time Synchronization Customer).

The command format is:

INPUTOUTPUT

.TTSC.TTSC (CUSTOMER NUMBER)

Example:

.TTSC.TTSC 5

- **Set Customer in charge** (Set Time Synchronization Customer).

The command format is:

.STSC (customer number)
where customer can be:

0 - 99 — 0 is default.

Example:

.STSC 5

- **Query Local Virtual DN** (Type Local DN).

The command format is:

INPUTOUTPUT

.TLDN.TLDN (DN)

Example (for 6 = ESN access code, 613 = ESN location code, 5999 = DN):

.TLDN.TLDN 66135999

- *Set Local Virtual DN* (Set Local DN).

  The command format is:

  .SLDN (dn)

  Example:

  .SLDN 66135999

- **Query Master or Backup Time Synchronization Number** (Type Master DN).

  The command format is:

  INPUTOUTPUT

  .TMDN.TMDN (DN)

  Example (for 6 = Outside line, 514 = ESN code, 3999 = DN):

  .TMDN.TMDN 65143999

- **Set Master or Backup Time Synchronization Number** (Set Master DN).

  The command format is:

  .SMDN (dn)

  Example:

  .SMDN 65143999

- **Query Time Delta.**

  The command format is:

  INPUT *OUTPUT*

  .TDEL.TDEL (SIGN) (HR) (MIN)

  Example:

  .TDEL.TDEL 0 01 30

- *Set Time Delta.*

  The command format is:

  .SDEL (sign) (hr) (min)

  - sign – is the time-adjust factor direction indicator which can be: 0 — to indicate the Master switch is behind in time. or 1 — to indicate the Master switch is ahead in time.
  - hr – is the number of hours the time must be adjusted by and can be any number from 0 to 23, and

- min – is the number of minutes the time must be adjusted by and can be any number from 0 to 59.

0 is the default for the SDEL parameters.

Example:

.SDEL 1 23 00

Note:
The hour and minute entries are two digits. The minute entry is defaulted to zero if not entered. "1" identifies a positive delta (Master is ahead in time), "0" identifies a negative delta.

- **Query Requesting Mode** (Type MODe).

  The command format is:

  INPUT *OUTPUT*

  .TMOD.TMOD (MODE)

  Example:

  .TMOD.TMOD BKGD

- *Set Requesting Mode* (Set MODe).

  The command format is:

  .SMOD (mode)

  where mode can be: BKGD — Background (default) or DSVC — Daily Service (midnight)

  Example:

  .SMOD DSVC

LD 22: Print the DN type for the Network Time Synchronization Virtual DN. The DN type is TIME.

Feature operation

Each node of the network that is to be synchronized sets its status (i.e., Master, Slave, or Standard stand-alone (the feature is not used)). The craftsperson also sets the node's customer in charge of synchronizing the switch (that customer will request Time Synchronization and receive the time from the Master or Backup switch). The customer must already exist, prior to referencing it, and then sets the local access codes with the virtual DN, the Master (or Backup) routing digits, the time difference between local and Master nodes, and the requesting mode (for example, performed under the background routines (default) or the daily services. The time delta and the requesting mode are optional entries).

The time synchronization feature is designed to work in a Meridian Customer Defined Integrated Services Digital Network (ISDN) environment, using D-channel messages. The synchronization messages are carried by TCAP facility messages on a Meridian Customer Defined ISDN, and routed according to the configuration defined in LD 2.

Once the configuration is defined in LD 2, the Slaves will automatically start requesting "time-stamps" from the Master periodically, upon initialize, and when the time and date is changed in LD 2. The message to be sent is identified as being a time synchronization request. The stored Master's routing digits (access codes + virtual DN) are used to route the synchronization requests. As part of the request, the requester's access codes + virtual DN is sent to provide the Master with a way back to the requesting node.

Upon receipt at the Master node, the terminating DN is recognized as being a time synchronization virtual DN, and the request is then processed. The processing consists of constructing a message, identified as being a time synchronization response and originating from that virtual DN, which includes:

- time
- date, and
- time-adjust factor (if used).

The message is then routed to the Slave using the access codes and virtual DN provided with the request. The time-adjust factor is sent to all Slaves in order to have the whole network correct any inaccurate clock settings in unison, if any slippage correction is necessary.

Up to three requests will be sent at one minute intervals, to allow the system to overcome possible temporary malfunctions. On receipt of the time message, the requester verifies the originator's ID (its virtual DN), and updates its clock accordingly (i.e., equal to the time sent minus the time delta between the two switches). If equipped with the CDR package, a time change record is provided with every time synchronization occurrence.

Chapter 31: Network-wide Listed Directory Number

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Listed Directory Numbers (LDNs) can be defined as Incoming Call Identification (ICI) keys on an attendant console, making it possible to have different presentations when different DNs are dialed. Without this feature, it was only possible to define four LDNs on a system. This feature makes it possible to define six LDNs on a system.

Without this feature, when an LDN call was routed from one node to another, the call was presented according to trunk type (for example, NDID, NTIE, NCO, NFEX, or NWAT). The call was presented on LDN key zero if none of the trunk route ICIs were configured. With the Network-wide Listed Directory Number feature, if the dialed DN is an LDN and an LDN key exists that corresponds to the dialed LDN, the call is presented on that ICI LDN key.

This feature also enables LDNs to be recognized network-wide when Network Attendant Service (NAS) is used. The same LDNs must be configured in multiple nodes. Network LDN is defined on a customer basis.

Operating parameters

The network part of this feature works in a Meridian Customer Defined Network (MCDN) environment with NAS configured.

The LDNs to be used network-wide cannot be used in conjunction with Distant Steering Codes.

Feature interactions

Call Forward No Answer

With this feature, the LDN ICI has a higher priority than CFNA ICI. When a call is forwarded to an LDN through Flexible DN, the call will be presented on the LDN ICI.

Departmental Listed Directory Number

Departmental LDN is not supported over the network; however, this feature does provide two more LDNs for the DLDN feature.

Console Presentation Group

This feature provides two more LDNs for each Console Presentation Group.

Console Operation/Console Presentation

Console Operation makes it possible for each console to select which ICI call types will be presented to the console. Network -wide LDN does not work with the Console Presentation feature because it is not supported by NAS. Console Operation can, however, be configured with two new LDNs.

Network Message Center

With this feature, the LDN ICI has a higher priority than MWC ICI. When a call is forwarded to an LDN over the network to a Message Center, the call will be presented on the LDN ICI.

Network Attendant Service

The way the network LDN calls are presented in a NAS environment is changed by this feature. The presentation on the NDID, NTIE, NCO, NFEX, or NWAT, and the LDN0 key is changed to the correct LDN key, if it exists. Otherwise, it will be presented as it previously was on the NDID or LDN0 key.

Console Operation/Queue Thermometer

The queue thermometer indicates how many calls are in the queue for a certain ICI key. An ICI key can correspond to more than one ICI type. Even though the ICI type of a call can be different with or without this feature active, it will not interact with queue thermometer operations.

Centralized Attendant Service

Centralized Attendant Service (CAS) is mutually exclusive to the NAS package. As the network wide LDN feature requires NAS for its networking functions, the network part of this feature will not work with CAS, but the two extra LDNs can be used locally.

Feature packaging

Network Wide LDN requires Network Attendant Service routing. The following packages are required for Network-wide LDN:

- Basic Routing (BRTE) package 14
- Network Class of Service (NCOS) package 32
- Network Alternate Route Selection (NARS) package 58
- Network Attendant Service (NAS) package 159
- applicable ISDN options, depending upon customer requirements

To use the attendant queue thermometer, Console Operations (COOP) package 169 must be provisioned.

For Departmental LDN to be configured with six LDNS, Departmental LDN (DLDN) package 76 must be provisioned.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 128: LD 15: Configure LDN data. on page 276
2. Table 129: LD 15: Enable the network recognition of the LDNs. The ICI keys can also be assigned to the new LDN values. on page 277
3. LD 10, LD 11 – The LDN prompt has been changed to accept a value of 0-5 in these overlays.

Table 128: LD 15: Configure LDN data.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	LDN	Departmental Listed Directory Numbers data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
- OPT	aaa	Options.
- DLDN	YES	Departmental Listed Directory Numbers.
…		
- LDN3	…	Listed DN 3.
- LDA4	xx xx… ALL	xx can be in the range of 1-63 or all attendants. Precede an attendant number with X to remove.
- LDN4	x…x	Listed Directory Number. If the DNXP package is equipped, up to seven digits are allowed; otherwise, only four digits are allowed.
- LDA5	xx xx… ALL	xx can be in the range of 1-63 or all attendants. Precede an attendant number with X to remove.
- LDN5	x…x	Listed Directory Number. If the DNXP package is equipped, up to seven digits are allowed; otherwise, only four digits are allowed.

Table 129: LD 15: Enable the network recognition of the LDNs. The ICI keys can also be assigned to the new LDN values.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	LDN	Departmental Listed Directory Number data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
- OPT	NLDN	Network-wide LDN allowed
…		
- ICI	xx LD4	New answer to existing prompt, where xx is the key number.
- ICI	xx LD5	New answer to existing prompt, where xx is the key number.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 32: NI-2 B-channel Service Messaging

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

This feature is only available in North America. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

The NI-2 B-channel Service Messaging feature provides B-channel availability control on the NI-2 interface. With this feature, service messages communicate B-channel status changes to the far-end. This feature does the following:

- increases B-channel availability
- increases throughput on PRI service
- reduces line degradation

- reduces the number of lost calls
- minimizes the number of repeated calls on an out-of-service B-channel

When the status of a system B-channel changes, the system sends a service message to the Central Office (CO). The CO replies with a service acknowledgment and changes the status of the corresponding B-channel. When a CO sends a service message to a system, the system acknowledges the service message and changes the B-channel status on the near-end.NI-2 B-channel Service messaging illustrates B-channel service messaging on the NI-2 interface.

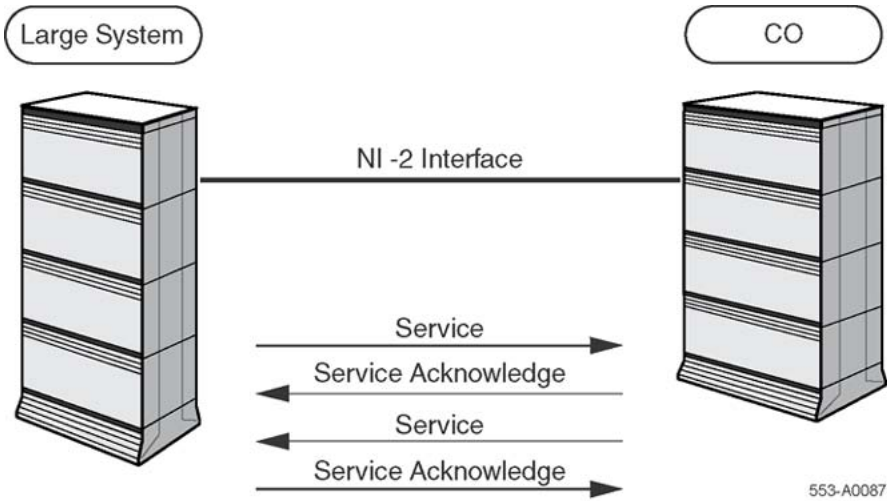

Figure 37: NI-2 B-channel Service messaging

B-channel status categories

The following are the status categories associated with the NI-2 B-channel Service Messaging feature:

- IS - Indicates that the B-channel is in service and available for outgoing and incoming calls.
- OOS-FE - indicates that the far-end B-channel is out-of-service.
- OOS-NE - indicates that the near-end B-channel is out-of-service.

When a B-channel at the near-end goes out-of-service, the system sends a service message with OOS status to the far-end. The near-end B-channel status is OOS-NE. On receipt of this service message, the far-end changes the corresponding B-channel to OOS-FE.

When the near-end B-channel becomes available, the system sends a service message with IS status to the far-end. The near-end B-channel is temporarily placed in OOS-FE. On receipt of this service message, the far-end changes the channel status to IS and returns a service acknowledge message with the IS status to the system. On receipt of this service acknowledge message, the near-end B-channel is placed in service.

The near-end status takes precedence over the far-end status. For example, if a near-end B-channel is in an OOS/NE state and receives an OOS request from the far-end, the final status is OOS/NE.

Near-end status scenarios lists the status scenarios when a message is received.

Table 130: Near-end status scenarios

Current Status (Near-end)	Status Received in Service Message	Final Status/ Status sent in Acknowledgement Message
OOS-NE	IS or OOS	OOS-NE/OOS
OOS-FE	IS	IS/IS
OOS-FE	OOS	OOS-FE/OOS
IS	OOS	OOS-FE/OOS
IS	IS	IS/IS

Message Event Triggers

IS trigger events

IS service messages are triggered when the following occur:

- The administrator enables the B-channel in LD 60 using the ENCH command.
- The status audit is triggered to resolve conflict between the status of the near-end and far-end of the channel. B-channels that are OOS receive either call clearing messages, channel negotiation messages, or requests for B-channel use.
- A new B-channel is provisioned and defaults to OOS-FE. The network side controls the initial service messaging requesting IS status on the user side of the B-channel.
- Alarm clear messages are received from the hardware

OOS trigger events

OOS service messages are triggered when the following occur:

- The administrator disables the channel from LD 60 using the DSCH command.
- The status audit is triggered to resolve conflict between the status of the near-end and far-end of the channel. B-channels that are OOS, receive either call clearing messages, channel negotiation messages or requests for B-channel use.
- An existing B-channel is removed from service.

- The administrator changes the channel ID in LD 14 using the MOV command.
- A PRI restart is sent or received for channels which are OOS.
- A channel is disabled for maintenance and an OOS message is sent.
- Alarm set messages are received from the hardware.
- A loop test is enabled in LD 60 for channels in a fault state.

Service message retransmission

Service messaging retransmits the message when an acknowledgment is not received within 120 seconds of the originating transmission. The number of retransmissions, up to a maximum of four, is configured in LD 17.

Service message collision

A message collision occurs when a service message is received between the time when a service message is sent and its corresponding service acknowledgement is received from the same B-channel. A re-transmission occurs after 120 seconds if an acknowledgment is not received. Service collision outcome lists the possible service message collision outcomes.

Table 131: Service collision outcome

Previous Near-end Status	Status Sent in Service Message	Colliding Status Received	Final Near-end Status
OOS-NE	IS	IS	IS
OOS-FE	IS	IS	IS
OOS-NE	IS	OOS	OOS-FE
OOS-FE	IS	OOS	OOS-FE
OOS-NE	OOS	IS	OOS-NE
OOS-FE	OOS	IS	OOS-NE
OOS-NE	OOS	OOS	OOS-NE
OOS-FE	OOS	OOS	OOS-NE
IS	IS	IS	IS
IS	IS	OOS	OOS-FE
IS	OOS	IS	OOS-NE
IS	OOS	OOS	OOS-NE

Operating parameters

The NI-2 B-channel Service Messaging feature operates on any system configured with a D-channel interface. The following PRI cards do not support the NI-2 B-channel Service Messaging feature:

- QPC757 Primary Rate Interface card
- NTAK93 D-Channel Handler Interface card

For the NI-2 B-channel Service Messaging feature, the far-end must support B-channel service messaging.

On an outgoing call, if the far-end triggers channel negotiation, an alternate channel is assigned. If the alternate B-channel has a near-end status of OOS-FE, the channel negotiation is accepted and the channel is placed in IS status. Otherwise, a Release Complete message is sent or a channel negotiation is triggered again.

When a setup message is received requesting an OOS channel, a Release Complete message is sent or a channel negotiation is performed. However, if the requested B-channel is OOS-FE, the status is changed to IS and the call is accepted.

With no existing call on the channel, B-channel Service messaging activates the B-channel to IS status. When there is a call on the B-channel, B-channel restart messaging is used.

The B-channel is placed in a lockout state when a restart message is sent. The lockout ends on receipt of a restart acknowledgement from the far-end. Calls cannot be placed on B-channels in the lockout state.

The identity of B-channels in the OOS-NE state are included in the PRI restart message.

To disable a PRI loop, corresponding D-channels are disabled. In this state, the B-channel service messaging is not active.

When a backup D-channel becomes active the restart procedure is triggered. Service messages containing B-channel status information are sent to all far-end B-channels in the OOS state.

If a colliding service message is received, the T323 timer stops and the original message does not retransmit.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature requires the following packages:

- ISDN Signaling (ISDN) package 145
- Primary Rate Access (PRA) package 146
- Multi-Serial Data Link (MSDL) package 222
- National Interface (NI-2) package 291

Feature implementation

Table 132: LD 17: Configure NI-2 B-channel Service Messaging.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Configuration Record.
ADAN	NEW DCH xx CHG DCH xx	Add a primary D-channel where: xx = 0-63 Change a primary D-channel where: xx = 0-63
IFC	NI2	NI-2 TR-1268 interface type.
BSRV	YES	NI-2 B-channel Service Messaging enabled. NO = NI-2 B-channel Service Messaging disabled (default).
BSRC	1-(2)-4	NI-2 B-channel Retransmission Counter.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 33: NI-2 Call By Call Service Selection

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

This feature is only available in North America. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

The National ISDN-2 (NI-2) Call By Call (CBC) Service Selection feature provides a standardized version of call by call service over an NI-2 TR-1268 interface, as defined in the Bellcore Technical Reference Specification TR-NWT-001270. It is intended that NI-2 CBC apply to all Class 5 type local exchanges complying with the NI-2 TR1270 standard.

Note:

The NI-2 Call By Call service Selection feature provides all of the NI-2 TR-1268 Basic Call services. Please refer to the National ISDN-2 TR-1268 PRI Interface feature module for a description of the services that are offered.

Prior to the introduction of this feature, proprietary call by call capabilities were offered by the Integrated Services Access feature (ISA) Call By Call Type service for DMS switches (such as the DMS-100), and Lucent's Call By Call Service Selection for 5ESS Local Exchange Carriers. Differences between ISA, CBC, and NI-2 CBC on page 291 provides a summary of the functional differences between the three offerings.

Note:

The ISA Call By Call Type service and the NI-2 Call By Call Service Selection feature can co-exist on the same PBX.

NI-2 Call By Call Service Selection allows multiple service routes to share the same common pool of B-channels, rather than using dedicated routes that require each service route to have its own trunks. The channels are assigned to a service for each call.

Figure 38: Dedicated facilities configuration on page 287 depicts a configuration using dedicated facilities, while NI-2 B-channel Service Messaging on page 279 shows an NI-2 Call By Call Service Selection configuration. NI-2 CBC service route treatment on page 290 provides a graphical representation of the NI-2 CBC master route and service routes.

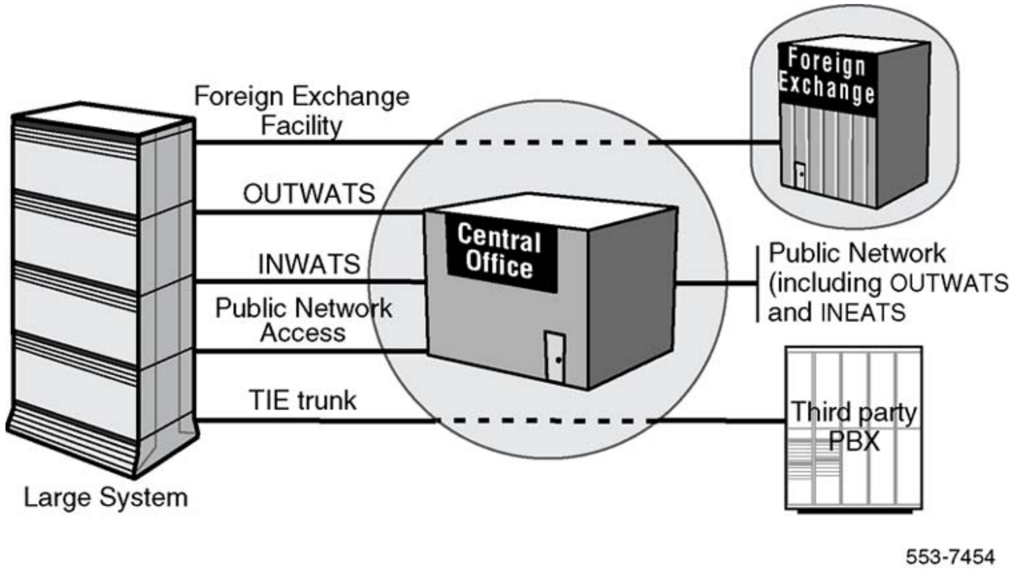

Figure 38: Dedicated facilities configuration

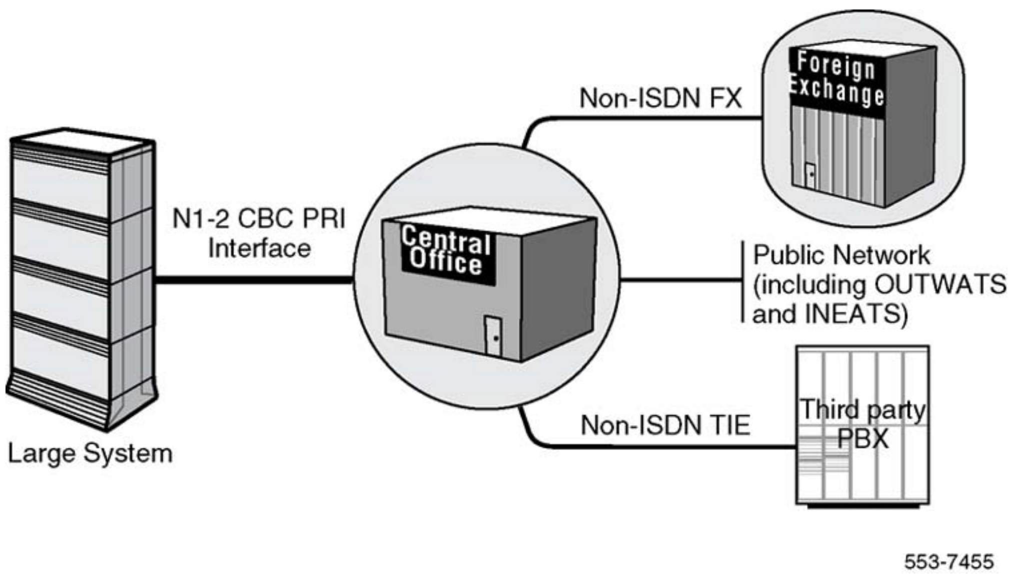

Figure 39: NI-2 Call By Call Service Selection configuration

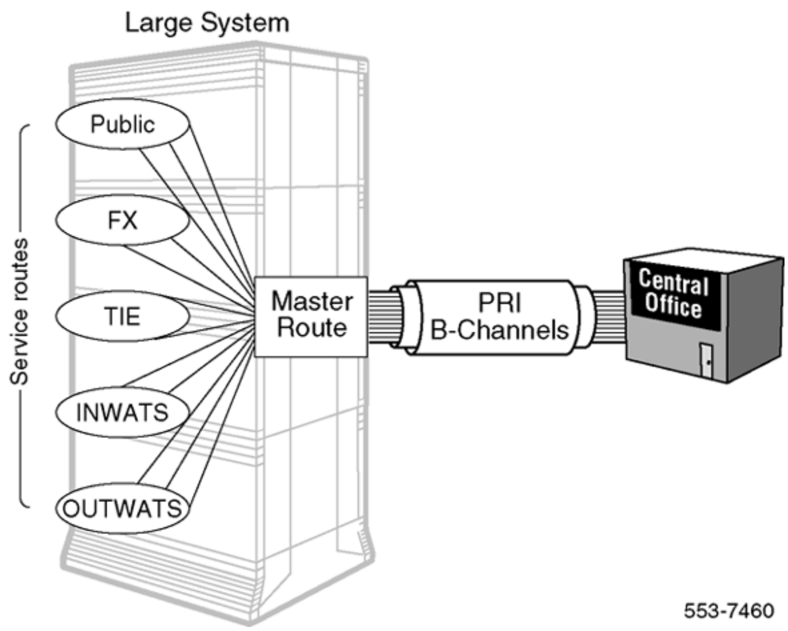

Figure 40: NI-2 CBC master route and service routes on the system

Provisioning a master route and service routes

NI-2 Call By Call Service Selection is provisioned by configuring a trunk route as an NI-2 Call By Call Service Selection master route, and associated service routes. A master route contains a list of B-channels (trunks) to be shared by the different service routes. Service routes do not have dedicated trunks. They are associated with the master route and share trunks for different Call By Call services. Calls from the Central Office to the system are offered over the CBC master route.

The NI-2 CBC master route is defined in LD 16. The associated list of B-channels (trunks) is defined using LD 14. Then, the service routes are configured, also using LD 16. When configuring the service routes, the type of service to be carried over the B-channels for the NI-2 PRI interface is defined as a decimal value, as follows:

0 = Public call service (No Network Specific Facility IE is sent, since COT/DID routes are used)

19 = FX (Foreign Exchange) service

20 = TIE service

17 = Inward Wide Area Telecommunication Service (INWATS) service

18 = Outward Wide Area Telecommunication Service (OUTWATS) service. Information pertaining to the band number and the Inter-Exchange Carrier is stored in the service route.

Three OUTWATS services can be accessed:

1. IntraLATA OUTWATS, provided by a local service provider
2. InterLATA OUTWATS, provided by a carrier other than that of the local service provider and
3. Banded OUTWATS, using bands which each represents a geographical area to which a subscriber can place a call at a special tariff level

Lucent proprietary call by call services are as follows (these values are defined in the facility coding field in the NSF IE in order for the system to recognize the Lucent call by call services):

- 00001 = Access to Virtual Private Network (such as Lucent's Software Defined Network service)
- 00010 = MEGACOM 800
- 00011 = MEGACOM
- 00110 = ACCUNET switched digital service
- 00111 = International long distance service
- 01000 = International 800
- 01011 = Electronic Tandem Network
- 01101 = Private Virtual Network
- 10000 = DIAL IT and Lucent MultiQuest

For each FX and TIE trunk service, a Facility Number is assigned.

The maximum number of trunks limited by each service route is entered when configuring the service routes. The maximum number of channels for each service (a maximum value is required by the Bellcore Technical Reference Specification) is controlled by the Central Office, and assigned at the time of subscription. It is this value that must be entered in LD 16.

There is no minimum limit specified by the Bellcore Technical Reference Specification, therefore no minimum value is assigned by the Central Office, or defined on the system.

Engineering consideration pertaining to service maximums

The maximum value of trunks defined for any service type cannot exceed the network maximum, but the total of all maximums combined can be greater than the network maximum.

For example, in a single 23B+D span, two service routes can be configured, each with a maximum of 15 trunks (B-channels). Even though the combined number of B-channels (30) is greater than the network maximum (23), a minimum of 8 B-channels would be left available for other service routes.

For an incoming call to the system, if the maximum number of trunks defined for a service has been reached, the system will return a "Release Complete" message to the Central Office, with the "Cause" value set to "User Busy". This allows the Central Office to return a busy tone to the caller.

Service routes for public network calls

NI-2 Call By Call Service Selection uses the Network Specific Facility (NSF) Information Element (IE) to indicate the requested service in the call request. If no NSF IE is included, the call is treated as a TR-1268 public network call (CO or DID).

Multiple service routes can be configured on a master route to serve outgoing public network calls, but only one service route can be specified in the master route to serve incoming public network calls (this is done using the IPUB prompt in LD 16). The route type for these service routes can be COT and DID. The result is that a system can be configured to handle public network calls with one incoming route and multiple outgoing routes, or one incoming and outgoing route with multiple outgoing routes.

NI-2 CBC service route treatment

Each service route stores the information, pertaining to a particular subscribed service, required to initiate or terminate a call. The information is transmitted to, or received from, the network by means of an NSF IE contained in the outgoing or incoming SETUP message.

Originating treatment (system to Central Office)

The system can designate the desired service to the Central Office, on a call-by-call basis. This is done by means of an NSF IE in the outgoing SETUP message. The NSF IE is built using the information configured in the service route. The SETUP message is sent by seizing a B-channel from a pool of channels associated to the CBC master route.

Termination treatment (Central Office to the system)

The Central Office, when offering a call to the system over the CBC master route, indicates in the NSF IE the type of service of the incoming call. The NSF IE contains the information required to identify a service route and to handle further call processing. The termination of NI-2 CBC service routes is based on the existing Integrated Services Access feature (ISA) call by call service treatment, and summarized in Table 133: Call termination for NI-2 CBC service route on page 291.

Table 133: Call termination for NI-2 CBC service route

TKTP	AUTO [a] = No				AUTO = Yes	
	DNIS[b] = No		DNIS = Yes		DNIS = No	DNIS = Yes
	IDC[c] = No	IDC = Yes	IDC = No	IDC = Yes		
COT	attendant	N/A[d]	N/A	N/A	AUDN[e]	N/A
FEX	attendant	IDC digit	N/A	IDC digit	AUDN	N/A
WAT	attendant	IDC digit	N/A	IDC digit	AUDN	AUDN[f]
DID	last n CADdigit[g]	IDC digit	N/A	IDC digit	AUDN	AUDN[h]
TIE	CAD	IDC digit	N/A	IDC digit	AUDN	AUDN[i]

a. AUTO = Autoterminate. b. DNIS = Direct Number Identification Service. c. IDC = Incoming Digit Conversion. d. N/A = Not supported. e. AUDN = Autoterminate DN. AUDN in LD 16 has the same significance as ATDN in LD 14. f. Must be an ACD DN. g. Last n CAD digit = the last n digits of the Called Party Number IE, where Ôn' is defined using prompt LDN0 in LD 15. h. Must be an ACD DN. i. Must be an ACD DN.

Differences between ISA, CBC, and NI-2 CBC

Table 134: Differences between Avaya ISA, Lucents CBC, and NI-2 CBC on page 291 summarizes the differences between Avaya ISA, Lucent's Call By Call Service Selection, and NI-2 Call By Call Service Selection.

Table 134: Differences between Avaya ISA, Lucents CBC, and NI-2 CBC

Avaya ISA	Lucent CBC	NI-2 CBC
Proprietary (interface specific to DMS-100 and DMS-250).	Proprietary (interface specific to Lucent 5ESS Local Exchange Carriers).	Bellcore-based standard CBC service (independent of switch type).
Services: — Public — PRIVATE — INWATS — OUTWATS — TIE — FX	Services: — ACCUNET — SDN — MEGACOM — MEGACOM 800 — WATB — WATM — LDS	Standardized Services: — TR-1268 Public (CO or DID) — FX — TIE — OUTWATS (IntraLATA, Bands, and InterLATA) — INWATS

Avaya ISA	Lucent CBC	NI-2 CBC
	— IWAT — I800	Non-standardized Services: — e.g., Lucent proprietary services, as follows: • Access to operator • Access to Exchange Carrier Services (call by call services) • Access to Virtual Private Network • MEGACOM/ MEGACOM 800 • ACCUNET switched digital service • International long distance service • International 800 • Electronic Tandem Network • Private Virtual Network • DIAL IT and Lucent MultiQuest
Avaya ISA	Lucent CBC	NI-2 CBC
CBC calls are routed according to the Service Identifier in Service Parameter of the NSF IE.	CBC calls are routed according to the service specified by the Facility Coding Value in the NSF IE.	CBC calls are routed according to the service specified by the Facility Coding Value and the Service Parameter in the NSF IE.
Up to 512 service routes can be configured on the system (one per Service Identifier value), enabling access to 512 possible services.	Only one service route can be configured per service type on the system, enabling access to only nine possible services. — 1 ACCUNET — 1 SDN — 1 MEGACOM — 1 MEGACOM 800 — 1 WATB — 1 WATM — 1 LDS — 1 IWAT — 1 I800	Up to 512 service routes can be configured on the system, enabling access to a maximum of 512 possible services (see Note 1). — Public (COT or DID) (see Note 2) — 1 INWATS — OUTWATS (98 bands, 1 IntraLATA, 1 InterLATA — Up to 512 FX or TIE (for FX and TIE, a Facility Number can be assigned in LD 16 for each service route)
The operation mode for TIE trunks is send (see Note 1).	N/A	The operation mode for TIE trunks can be send (see Note

Avaya ISA	Lucent CBC	NI-2 CBC
		3) or cut-through (see Note 4).
The minimum and maximum function are defined on a per service route basis.	The minimum and maximum function are defined on a per service route basis.	The maximum value is defined on a per service route basis (a maximum is required by the Bellcore Specification). The maximum value is also defined by the serving Central Office. There is no minimum value allowed by the Bellcore Specification.
One Public service route (no NSF IE) can be configured for multiple incoming and outgoing trunks, with a maximum and a minimum value.	N/A	A system can be configured to handle public network calls with one incoming route and multiple outgoing routes, or one incoming and outgoing route with multiple outgoing routes. The route type for these service routes can be COT and DID.

Note:
The maximum cannot be greater than 512 for all call types.

Note:
Multiple service routes can be configured on a master route to serve outgoing public network calls, but only one service route can be specified in the master route to serve incoming public network calls. The route type for these service routes can be COT and DID. The result is that a system can be configured to handle public network calls with one incoming route and multiple outgoing routes, or one incoming and outgoing route with multiple outgoing routes

Note:
For a TIE trunk operating in send mode, the Central Office collects and screens the called digits before sending the digits to the Class II equipment or PBX at the end of the TIE trunk.

Note:
For a TIE trunk operating in cut-through mode, the Central Office does not collect the called digits. The Class II equipment or the switch at the end of the TIE trunk are allowed to exchange in-band information, such as dial tone and address information.

Operating parameters

NI-2 Call By Call Service Selection does not support the TIE trunk cut-through mode.

The maximum number of NI-2 Call By Call Service Selection routes that can be configured on a system is 512.

The maximum number of trunks for each route is 254 for each master route.

Feature interactions

Calling Party Privacy

The Calling Party Privacy feature allows a user the option of restricting the display of the calling number on the phone of the called party. The INWATS service requires that the CLID always be displayed. Therefore, subscribers to INWATS cannot restrict the display of the calling number, even though they have the Calling Party Privacy feature active.

Feature packaging

The NI-2 Call By Call Service Selection feature requires the NI-2 Call By Call (NI2 CBC) package 334.

The following packages are also required as dependencies:

- Integrated Services Digital Network (ISDN) package 145
- Primary Rate Access (PRA) package 146
- Multi-purpose Serial Data Link (MSDL) package 222
- National ISDN-2 (NI2) package 291

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

Table 135: LD 17: Configure the primary D-channel for the NI-2 Basic Call Service.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	CFN	Configuration Record.
ADAN	NEW DCH xx	Add a primary D-channel where: xx = 0-63
CTYP	MSDL	Supported only on Multi-purpose Serial Data Link (MSDL) or Downloadable D-channel cards.
...		
USR	PRI	D-channel mode.
IFC	NI2	NI-2 TR-1268 interface type.
CO_TYPE		Central Office switch type (prompted only if IFC = NI2).
	(STD) ATT	STD = Totally compatible with Bellcore standard. ATT = Lucent 5ESS.
PRI	lll nn	lll = PRI loop using the same D-channel (0,1,...159) nn = Interface identifier (2-15)

Table 136: LD 16: Configure the NI-2 Call By Call Service master route.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
DMOD	1-127	Default Model number for this route (for Media Gateway 1000B).
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number

Prompt	Response	Description
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
TKTP	CBCT	The trunk type is a Call By Call master route.
...		
ISDN	YES	ISDN route.
- IFC	NI2	Interface type is NI-2.
- IPUB	0-511	Service route to be used for incoming network calls. For Large Systems.
...		
- - PNI	1-32700	Private Network Identifier.
...		
ICOG	IAO ICT OGT	IAO = The trunk is incoming and outgoing. ICT = The trunk is incoming only. OGT = The trunk is outgoing only.

Table 137: LD 14: Define the associated list of trunks (B-channels) that are to be shared by the NI-2 CBC service routes.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	CBCT	Call By Call trunk.
TN		Terminal Number.
	l ch	Loop and channel for digital trunks, where: l = Previously defined loop number (0-159). ch = channel (1-24).
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
RTMB		Route number and Member Number
	0-511 1-4000	Range for Large System, Media Gateway 1000B, and CS 1000E system.

Note:

Up to 512 service routes can be configured using this procedure.

Table 138: LD 16: Configure the NI-2 CBC service routes.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number **Note:** Service route number must be different than the value entered for the master route.
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
TKTP	TIE COT DID WAT FEX	Service trunk type. TIE Central Office Direct Inward Dial Wide Area Telecommunication Service Foreign Exchange
...		
ISDN	YES	ISDN route.
- IFC	NI2	Interface type is NI-2.
- CBCR	YES	Service route indicator.
- - RTN	0-511	Master route number, as previously defined in LD 16.
- - SRVC	(0)-31	Decimal value of the service provisioned for NI-2. Prompted only if IFC = NI2. 0 = Public call service 19 = FX (Foreign Exchange) service 20 = TIE service 17 = Inward Wide Area Telecommunication Service (INWATS) service 18 = Outward Wide Area Telecommunication Service (OUTWATS) service. Lucent proprietary call by call services can also be defined here. Refer to List for a list of these values.
- - FACN	(0)-99999	TIE or FX facility number. Prompted only if IFC = NI2, and SRVC = 19 (FX) or 20 (TIE).
- - BAND	(0)-99	OUTWATS band number. Prompted only if IFC= NI2 and SRVC = 18 (OUTWATS).

Prompt	Response	Description
- - IEC	(0)-xxx (0)-xxxx	Inter-Exchange Carrier providing the service. Prompted if IFC = NI2 and SRVC = 0-16, 18, or 21-31.
- - MAX	xxx	Maximum number of trunks for the service route. This value must be the same as the value assigned by the Central Office at the time of subscription.

Sample configuration

The following provides a sample configuration of the NI-2 CBC feature.

LD 17 provides a sample configuration of a primary D-channel for the NI-2 Basic Call Service.

Table 139: LD 17: Configure a primary D-channel for the NI-2 Basic Call Service.

Prompt	Response	Description
REQ	NEW	Add configuration information.
TYPE	CFN	Configuration Record.
ADAN	NEW DCH 1	Add a primary D-channel for NI-2, where 1 is the primary D-channel number.
CTYP	MSDL	Supported only on Multi-purpose Serial Data Link (MSDL) or Downloadable D-channel cards.
...		
USR	PRI	D-channel mode.
IFC	NI2	NI-2 TR-1268 interface type.
CO_TYPE	STD	Central Office switch type for the NI-2 interface. STD = Totally compatible with Bellcore standard.
PRI	1 2	1 = PRI loop using the same D-channel (0,1,...159) 2 = Interface identifier (2,3,...15)

LD 16 configures a trunk route as an NI-2 Call By Call Service Selection master route.

Table 140: LD 16: Configure a trunk route as an NI-2 Call By Call Service Selection master route.

Prompt	Response	Description
REQ	CHG	Change existing data.

Prompt	Response	Description
TYPE	RDB	Route Data Block.
DMOD	1-127	Default Model number for this route (for Media Gateway 1000B).
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT	0	Master route number
TKTP	CBCT	The trunk type is a Call By Call master route.
DTRK	YES	Trunk route is digital.
DGTP	PRI	Trunk type is digital.
ISDN	YES	ISDN is used.
...		
- IFC	NI2	Interface type is NI-2.
- IPUB	1	Service route for incoming public network calls.
...		
- - PNI	1	Customer's Private Network Identifier.
...		
ICOG	IAO	The trunk is incoming and outgoing.

LD 14 defines the associated list of trunks (B-channels) that are to be shared by the NI-2 CBC service routes.

Table 141: LD 14: Define the associated list of trunks (B-channels) to be shared by NI-2 CBC service routes.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CBCT	Call By Call trunk.
TN		Terminal Number
	0 1	Loop and channel for digital trunks, where: 0 = Previously defined loop number (0-159). 1 = channel (1-24).
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
RTMB	0 1	CBC master route and member number.

LD 16 defines the NI-2 CBC service routes. Up to 512 service routes can be configured using this procedure.

Table 142: LD 16: Define the NI-2 CBC service routes.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT	1	Service Route number
...		
TKTP	TIE	Service trunk type.
...		
ISDN	YES	ISDN route.
- IFC	NI2	Interface type is NI-2.
- CBCR	YES	Service route indicator.
- - RTN	0	Master route number, as previously defined in LD 16, with which the service routes are associated.
- - SRVC	20	Decimal value of for TIE service.
- - FACN	20	TIE Facility Number.
- - MAX	1	Maximum number of trunks for the service route. This value must be the same as the value assigned by the Central Office at the time of subscription.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 34: NI-2 Name Display Supplementary Service

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

This feature applies only to North America. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

The NI-2 Name Display Supplementary Service extends the system capability to support name display on National ISDN-2 (NI-2) interfaces. This feature provides the following:

- calling name information on outgoing and incoming calls
- Connected/Alerting name information to incoming calls and from outgoing calls

The NDS feature retains the existing user interface for Meridian Customer Defined Network (MCDN) name display capabilities.

To enable this feature, configure each D-channel's remote capability as NDS. The calling name is sent in the SETUP message. The Connect/Alerting name is sent in the CONNECT/ALERT message.

The display of the name information at the far-end is controlled by the programming at the originating switch and the terminating switch. The status of the Presence Indicator (PI) depends on how the Name Display Allowed/Name Display Denied (NAMA/NAMD) Class of Service is configured on the phone at the near-end.

The presentation status from the near-end is overridden using the Calling Party Privacy (CPP) or Calling Party Privacy Override (CPPO) features.

The display on the far-end is determined by the Call Party Name Display Allowed (CNDA) or Call Party Name Display Denied (CNDD) Class of Service configured on the far-end phone.

Presentation status of the originating node without Calling Party Privacy (CPP) describes the presentation status of the originating node (the near-end) if Calling Party Privacy is not implemented.

Table 143: Presentation status of the originating node without Calling Party Privacy (CPP)

Class of Service	Presentation Indicator
NAMA	Presentation Allowed
NAMD	Presentation Denied

Presentation status of the originating node with CPP for each line blocking Class of Service describes the presentation status of the originating node (the near-end) with CPP for each line blocking Class of Service implemented.

Table 144: Presentation status of the originating node with CPP for each line blocking Class of Service

Class of Service	Presentation Indicator
NAMA + Calling Party Number and Name Per-Line Blocking De-activated (CLBD)	Presentation Allowed
NAMA + Calling Party Number and Name Per-Line Blocking Activated (CLBA)	Presentation Denied
NAMD + CLBD	Presentation Denied
NAMD + CLBA	Presentation Denied

Presentation status of the originating node with CPP for each line blocking Class of Service and FFC describes the presentation status of the originating node (the near-end) with CPP for each line blocking Class of Service and the dialed CPP Flexible Feature Code (FFC).

Table 145: Presentation status of the originating node with CPP for each line blocking Class of Service and FFC dialed

Class of Service	Presentation Indicator
NAMA + CLBA + CPPO FFC dialed	Presentation Allowed
NAMA + CLBD + CPPO FFC dialed	Presentation Allowed
NAMA + CLBD + CPP FFC dialed	Presentation Denied
NAMD + CLBA + CPPO FFC dialed	Presentation Allowed
NAMD + CLBA + CPP FFC dialed	Presentation Denied
NAMD + CLBD + CPPO FFC dialed	Presentation Allowed
NAMD + CLBD + CPP FFC dialed	Presentation Denied

Operating parameters

The NI-2 Name Display Supplementary Service complies with the GR-1367 Bellcore specifications for name delivery on PRI trunks.

The Name Display is not displayed on the far-end if this feature is not supported by the CO or PBX to which the far-end is connected.

With this feature, display names can be up to 15 characters long. Display names longer than 15 characters are truncated on the receiving phone.

Calls with the Calling Party Privacy (CPP) Flexible Feature Code (FFC) override NDS.

Feature interactions

Avaya CallPilot

An interaction occurs with TRO BA feature if a customer using LOC codes and a caller exists on the same CallPilot node. The LOC header will be stripped from the message header if the call is redirected to the customer on the CallPilot node as a result of CFNA or CFAC. Under this circumstance if the customer requires the LOC in the message header it is recommended to use TAT to perform trunk optimization.

Call Forward (all types)

In a stand-alone environment, Phone A calls Phone B. The call is forwarded to Phone C. Phone C displays Phone B's name information. See Call Forward (all types) in a stand-alone environment.

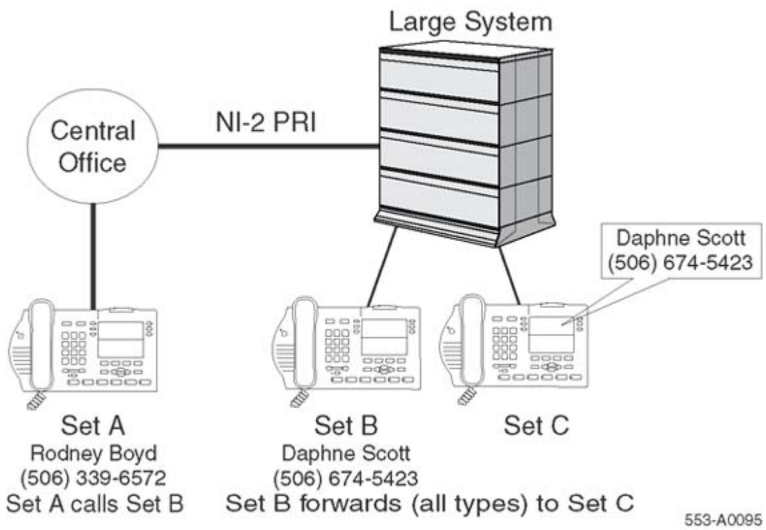

Figure 41: Call Forward (all types) in a stand-alone environment

In a network environment, Phone C displays Phone A's information. See Call Forward (all types) in a networking environment.

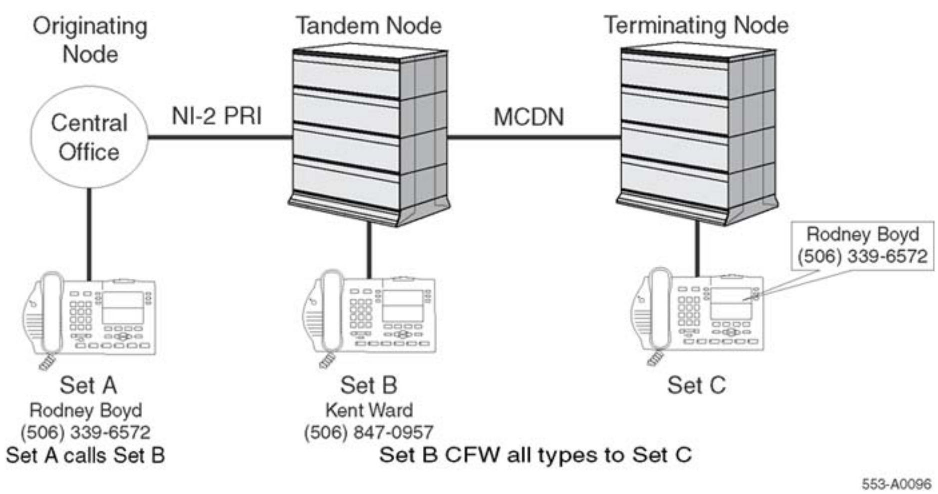

Figure 42: Call Forward (all types) in a networking environment

Call Hold

When an incoming call with Name Display Allowed is put on hold, the receiving phone clears the name information from the display screen. When the call is re-established, the name information is re-displayed.

Call Pickup

Call Pickup Network Wide

In a stand-alone environment, Phone A calls Phone B. Phone C picks up the call for Phone B. Phone C displays Phone B's name information. See Call Pickup in a stand-alone environment.

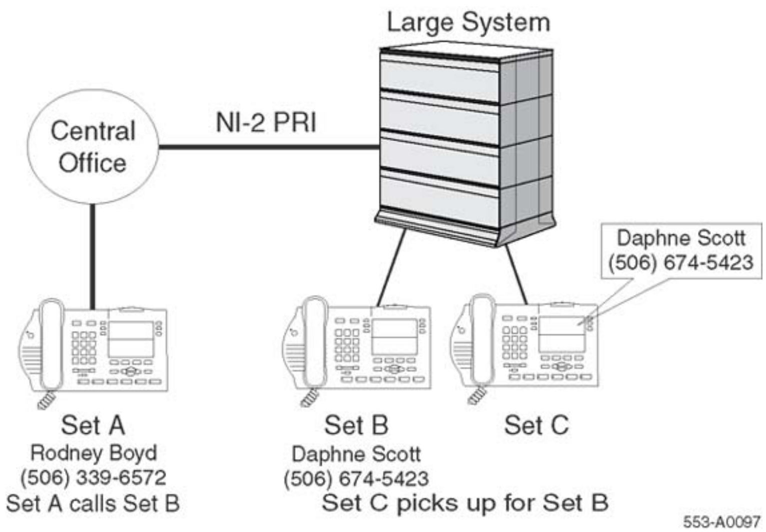

Figure 43: Call Pickup in a stand-alone environment

In a networking environment, Phone C displays Phone A's name information. See Call Pickup Network Wide.

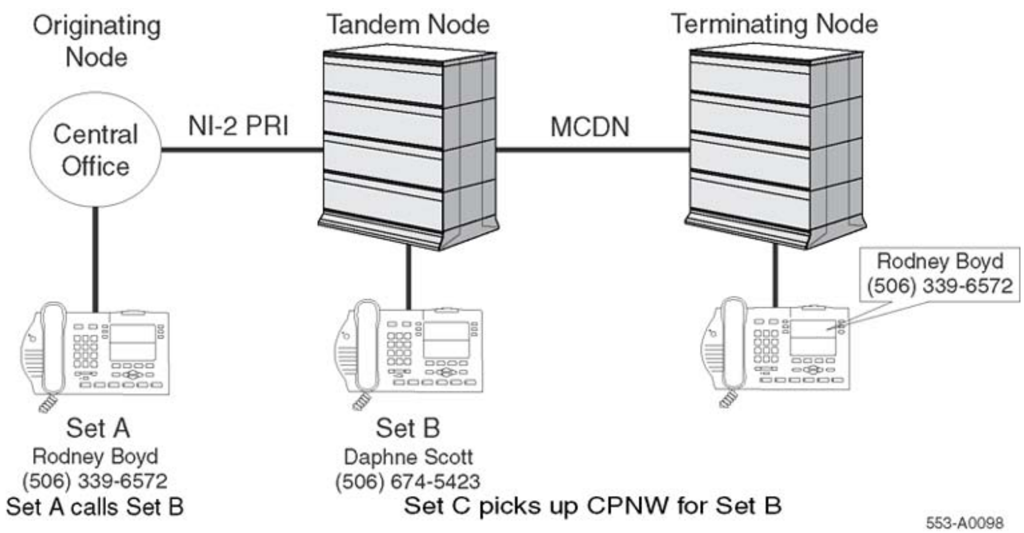

Figure 44: Call Pickup Network Wide

Call Transfer

Phone A calls Phone B. Phone B transfers the call to Phone C. Phone C displays Phone A's name information. This applies to both stand-alone and networking environments.

Calling Party Privacy

The Calling Party Privacy (CPP) feature overrides NDS.

Conference

Phone A calls Phone B. Phone B conferences Phone C. Phone B and Phone C clear the name information from the display screen. If Phone B leaves the conference, Phone A's name information displays on Phone C. See Conference call.

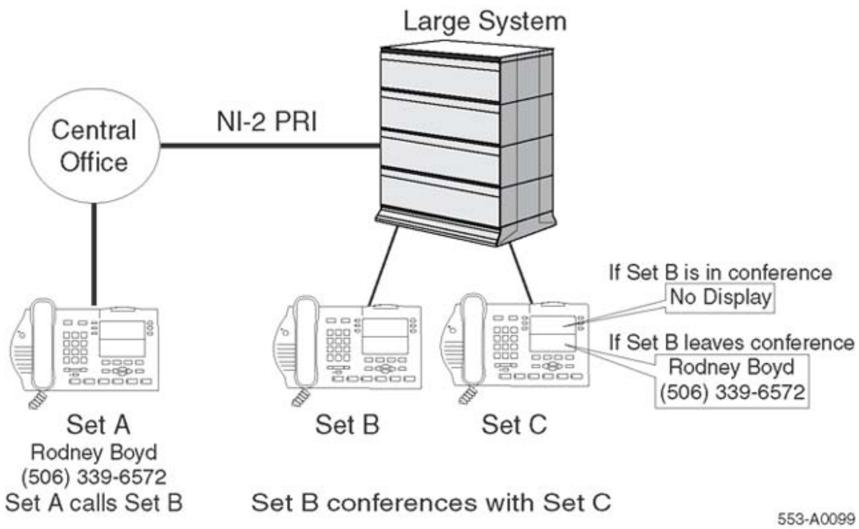

Figure 45: Conference call

Hunt

In a stand-alone environment, Phone A calls Phone B. The call is hunted to Phone C. Phone C displays Phone B's name information.

In a networking environment, Phone C displays Phone A's name information.

Name Display for Dialed Number Identification Services

If DNAM = YES for incoming IDC routes, the DNIS number and name for Incoming Digit Conversion (IDC) DNIS NI-2 incoming calls is displayed instead of the calling name.

Feature packaging

This feature requires the following packages:

- Call Party Name Display (CPND) package 95
- Integrated Services Digital Network (ISDN) package 145
- 1.5 Mbit/s Primary Rate Access (PRS) package 146
- Multi-purpose Serial Data Link (MSDL) package 222
- NI-2 TR-1268 Interface Basic Call Feature (NI-2) package 291

- Calling Party Privacy (CPP) package 301
- NI-2 Name Display Service (NDS) package 385

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

Table 146: LD 17: Configure the remote capability on the NI-2 PRI D-channel as Name Display Service (NDS).

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	Action Device and Number.
ADAN	CHG DCH xx	Change D-channel where: xx = 0-63
....	....	
IFC	NI2	NI-2 TR-1268 Interface type.
Prompt	Response	Description
RCAP	NDS XNDS	Remote Capabilities. Implement NI-2 Name Display Service. Remove NDS.

Table 147: LD 95: Create a new Call Party Name Display (CPND) name string, if not already configured.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	NAME	Create a new name string.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
DN	xxxx	Directory Number.
NAME	aaaa	Calling Party Name Display (CPND) name (maximum 15 characters).

Table 148: LD 10: Allow NDS on analog (500/2500-type) phones.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	500/2500	Type of phone.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...	...	
FTR	CPND	Allow CPND name assignment on this phone (not required if CPND is enabled in LD 95).
CLS	(CNDD) CNDA	Called Party Name Display denied. Called Party Name Display allowed (applies only to portable, personal phones). Allowed if WRLS=Yes.
CLS	(NAMD) NAMA	Name Display Denied on the far-end. Name Display Allowed on the far-end.

Table 149: LD 11: Allow NDS on digital proprietary phones.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	a...a	Telephone type. Type **?** for a list of possible responses.
CUST		Customer number

Prompt	Response	Description
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
CLS	(CNDD) CNDA	Call Party Name Display denied on this phone. Call Party Name Display allowed on this phone.
CLS	(NAMD) NAMA	Name Display denied on the far-end. Name Display allowed on the far-end.

Table 150: LD 12: Allow NDS on Attendant Console.

Prompt	Response	Description
REQ	NEW	Add new data.
TYPE	2250	Attendant Console type.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
....	....	
CPND	(CNDD) CNDA	Call Party Name Display denied. Call Party Name Display allowed.

Table 151: LD 57: Define the Calling Party Privacy (CPP) Flexible Feature Code (FFC) for analog (500/2500-type) and digital proprietary phones.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	FFC	Flexible Feature Code.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...	...	
CPP	xxxx	Calling Party Privacy FFC (typically *67). CPP is only prompted if the CPP package is equipped.
CPPO	xxxx	Calling Party Privacy Override. CPPO is only prompted if the CPP package is equipped.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 35: NI-2/QSIG Compliance Update

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The NI-2/QSIG Compliance Update feature makes the NI-2 and QSIG interfaces compliant with the latest standards documents. This feature applies to both Basic Rate Interface and Primary Rate Interface connections.

Note:
ISDN BRI trunking is not available in North America.

Compliancy with the standards has evolved as follows:

- ETSI QSIG basic call functionality now complies with the ETS 300-172, fourth edition (1997) standards document. Initially, support for the ISDN ETSI QSIG interface and the basic call capability was introduced. This version of the interface was based on the ETS 300-172, first edition (1990) document.
- ISO QSIG basic call functionality now complies with the North American standards document, ISO/IEC 115172 second edition. Initially, support for the ISDN ISO QSIG

interface and the basic call capability was introduced. This version of the interface was based on the ISO/IEC 115172 first edition document.

- National ISDN-2 (NI-2) basic call functionality now complies with the latest North American standards document, Bellcore TR-NWT-001268.

The NI-2/QSIG Compliance Update feature changes the way the system handles a recoverable error. Instead of sending incorrect call state information, the system now sends a correct call state in the STATUS message.

The mandatory parts of the STATUS message are: CAUSE (indicates type of error) and CALL STATE. Whenever the system encounters a recoverable error it sends a STATUS message. Recoverable errors can be cases such as:

- the IE received is non-mandatory and unrecognized
- the IE is non-mandatory and has invalid contents

In cases such as these, the basic call can still be processed, without affecting basic services, if the call state sent does not hinder this process. All the protocol must do is report the errors.

Before the protocol compliancy was updated, the system sent the call state information as it existed before receiving the incoming call message with the recoverable error. This was not appropriate for other-vendor switches which dropped the call when the incorrect call state information was received. Now, the system sends the call state information, adjusted after the incoming call message was received. The adjusted call state information allows the other vendor switch to proceed with the basic call.

Operating parameters

Fatal errors and errors in non-call-associated messages (such as maintenance messages) are not affected by this feature. These errors continue to use the existing error reporting mechanism.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

The following packages are required for the ISDN PRI QSIG interface:

- ISDN Signaling (ISDN) package 145
- 2 Mbit PRI (PRI2) package 154
- International PRA (IPRA) package 202
- Multi-Purpose Serial Data Link (MSDL) package 222
- QSIG Interface (QSIG) package 263

The following packages are required for the ISL QSIG interface:

- ISDN Signaling (ISDN) package 145
- ISDN Signaling Link (ISL) package 147
- 2 Mbit PRI (PRI2) package 154
- Multi-Purpose Serial Data Link (MSDL) package 222 (for ISL on PRI only)
- QSIG Interface (QSIG) package 263

The following packages are required for the ISDN BRIT QSIG interface:

- ISDN Signaling (ISDN) package 145
- ISDN Basic Rate Interface (BRI) package 216
- Multi-Purpose Serial Data Link (MSDL) package 222
- ISDN BRI Trunk Access (BRIT) package 233
- QSIG Interface (QSIG) package 263

The following packages are required for the PRI NI-2 interface:

- ISDN Signaling (ISDN) package 145
- Primary Rate Interface (PRA) package 146
- Multi-Purpose Serial Data Link (MSDL) package 222
- National ISDN-2 Interface (NI-2) package 291

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 152: LD 17: Assign the configuration record. on page 316
2. Table 153: LD 16: Use this overlay to define a route data block. on page 316

Table 152: LD 17: Assign the configuration record.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ADAN	Action Device And Number
...		
IFC	ISIGESIG	Interface ID for ISO QSIG. Interface ID for ETSI QSIG.
TIMR	(NO) YES	NO = skip timer prompt. YES = change timer value.
T310	10-(30)-60	10-60 seconds (one-second increments). 30 seconds is the default value.

Table 153: LD 16: Use this overlay to define a route data block.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route data block.
...		
DGTP	PRI PRI2 BRI	Digital route type.
IFC	ISIG ESIG	New DCH interface ID.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 36: NPI and TON in CDR

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Numbering Plan Identification (NPI) and Type Of Number (TON) in Call Detail Recording (CDR) feature allows NPI and TON information to be optionally displayed on the third line of CDRs. NPI and TON are associated with Calling Line Identification (CLID) information, and are useful for billing incoming calls to the originating party.

The NPI and TON are only displayed for calls on an incoming ISDN trunk. Also, the New Format CDR (FCDR) prompt must be set to NEW and the Calling Line Identification (CLID) prompt must be set to YES in LD 17. Third line format for CDR ticket illustrates the format of the third line of a CDR ticket.

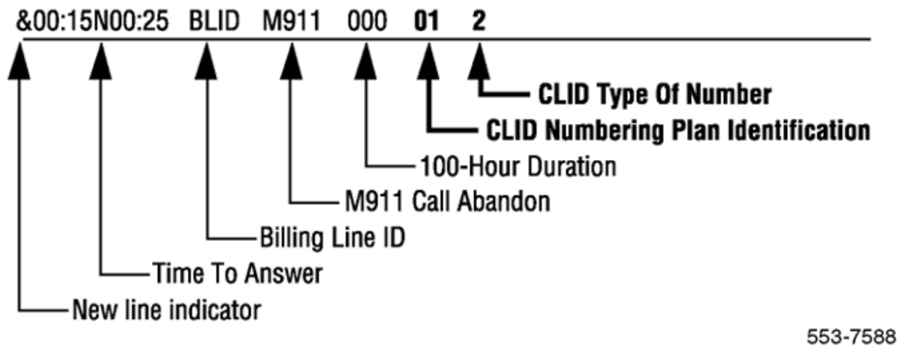

Figure 46: Third line format for CDR ticket

Third line contents of CDRs describes the contents of the third line of CDRs.

Table 154: Third line contents of CDRs

Line	Position	Field	Field Definition
3	1	blank	
3	2	&	New line indicator
3	3-7	TTA	Time To Answer (Total ringing time)
3	8	REDIR/B	Time To Answer (Redirection Indicator)/Busy Tone Identifier
3	9-13	TWT	Time To Answer (Total Waiting Time)
3	14	blank	
3	15-30	BLID...xxx	Billing Line ID
3	31	blank	
3	32-38	ABANDON	M911 Call Abandon Tag
3	39	blank	
3	40-42	000	100-Hour Duration
3	43	blank	
3	44-45	NPI	CLID Numbering Plan Identification
3	46	blank	
3	47	TON	CLID Type Of Number
3	48	blank	

Scenario involving a call over a Meridian Customer Defined Network illustrates a scenario in which DN 4000 (on Node 1) places a call to DN 4100 (on Node 2) over a Meridian Customer Defined Network (MCDN), using a Coordinated Dialing Plan (CDP) Distant Steering Code

(DSC). The call arrives at Node 2 on Route 201 Member 4. A CDR N ticket is produced when the call is disconnected.

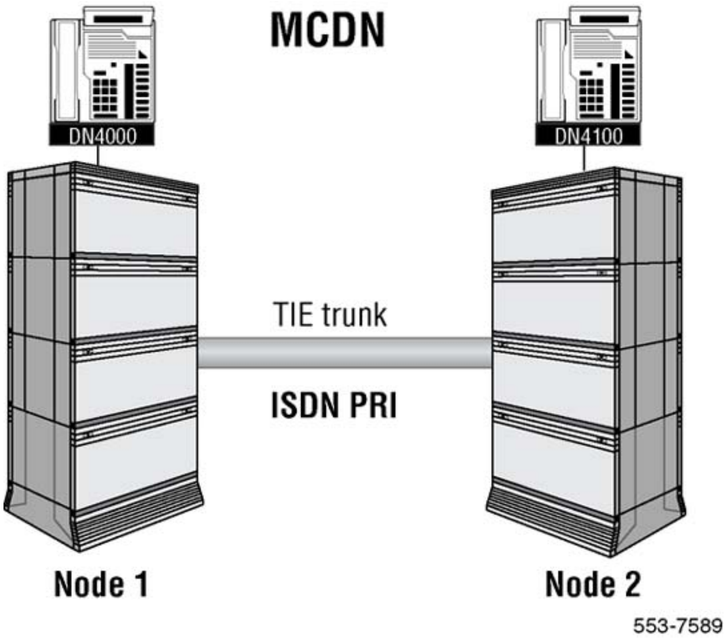

Figure 47: Scenario involving a call over a Meridian Customer Defined Network

The CDR N ticket produced in the described scenario has the following format:

```
N 001 02 T201004 DN4100 02/10 18:07:15:00:02:24.0 & 4000XXXXXXXXXXX
&00:15N00:25 BLIDXXXXXXXXXXXX        000 09 6
```

On line 3 of the ticket, the NPI value of "09" represents a private numbering plan. The TON value of "6" represents an Electronic Switched Network (ESN) Customer Dialing Plan (CDP). Please refer to Table 155: NPI information printed in the CDR ticket for an MCDN incoming trunk on page 322 and Table 156: TON information printed in the CDR ticket for an MCDN incoming trunk on page 322 for the NPI and TON information for an MCDN incoming trunk.

When an incoming call arrives on the system, NPI and TON are sent in the calling party Information Element (IE) and are mapped into internal values. The correspondence between the system values and the values given in the specifications are described inTable 155: NPI information printed in the CDR ticket for an MCDN incoming trunk on page 322 to Table 164: TON information printed in the CDR ticket for an NI-2 incoming trunk on page 325.

Table 155: NPI information printed in the CDR ticket for an MCDN incoming trunk on page 322 to Table 164: TON information printed in the CDR ticket for an NI-2 incoming trunk on page 325 show the information printed in the CDR ticket, depending on the incoming trunk protocol. As shown in these tables, not all combinations of NPI and TON exist.

In the TON tables, only ISDN/Telephony numbering plan (Rec. E.164/E.163) and private numbering plans are detailed. For all other supported NPI values, TON has the value of "unknown number".

Referring to the scenario in Figure 47: Scenario involving a call over a Meridian Customer Defined Network on page 321, Table 155: NPI information printed in the CDR ticket for an MCDN incoming trunk on page 322 andTable 156: TON information printed in the CDR ticket for an MCDN incoming trunk on page 322 show the NPI and TON information for an MCDN incoming trunk.

Table 155: NPI information printed in the CDR ticket for an MCDN incoming trunk

NPI code in CDR	Corresponding value of NPI in specification
00	000 - unknown numbering plan
01	0001 - ISDN/Telephony numbering plan (Rec. E.164)
02	not used
03	not used
04	not used
08	not used
09	1001 - private numbering plan

Table 156: TON information printed in the CDR ticket for an MCDN incoming trunk

TON code in CDR	Corresponding value of TON in specification	
	NPI = ISDN/Telephony numbering plan (Rec. E.164)	NPI = private numbering plan
0	0000 - unknown number	0000 - unknown number
1	0001 - international number	not used
2	0010 - national number	not used
3	not used	0011 - ESN SPN
4	0100 - local number	not used
5	not used	0101 - ESN LOC
6	not used	0110 - ESN CDP

NPI information printed in the CDR ticket for a EuroISDN incoming trunk and TON information printed in the CDR ticket for a EuroISDN incoming trunk show the NPI and TON information for a EuroISDN incoming trunk.

Table 157: NPI information printed in the CDR ticket for a EuroISDN incoming trunk

NPI code in CDR	Corresponding value of NPI in specification
00	0000 - unknown
01	0001 - ISDN/Telephony numbering plan (Rec.E.164/E.163)
02	not used

NPI code in CDR	Corresponding value of NPI in specification
03	0011 - data numbering plan (Rec.X.121)
04	0100 - telex numbering plan (Rec.F.69)
08	1000 - national standard numbering plan
09	1001 - private numbering plan

Table 158: TON information printed in the CDR ticket for a EuroISDN incoming trunk

TON code in CDR	Corresponding value of TON in specification	
	NPI = ISDN/Telephony numbering plan (Rec. E.164)	NPI = private numbering plan
0	000 - unknown or 110 - abbreviated number	000 - unknown or 110 - abbreviated number or 001 - level 2 regional number
1	001 - international number	cannot be mapped
2	010 - national number	010 - level 1 regional number
3	011 - network specific number	011 - network specific number
4	100 - subscriber number	100 - subscriber number
5	not used	not used
6	cannot be mapped	cannot be mapped

NPI information printed in the CDR ticket for a QSIG incoming trunk and TON information printed in the CDR ticket for a QSIG incoming trunk show the NPI and TON information for a QSIG incoming trunk.

Table 159: NPI information printed in the CDR ticket for a QSIG incoming trunk

NPI code in CDR	Corresponding value of NPI in specification
00	0000 - unknown
01	0001 - ISDN/Telephony numbering plan (Rec.E.164/E.163)
02	not used
03	0011 - data numbering plan (Rec.X.121)
04	0100 - telex numbering plan (Rec. F.69)
08	1000 - national standard numbering plan
09	1001 - private numbering plan

Note:

QSIG refers to ISO QSIG and ETSI QSIG.

Table 160: TON information printed in the CDR ticket for a QSIG incoming trunk

TON code in CDR	Corresponding value of TON in specification	
	NPI = ISDN/Telephony numbering plan (Rec. E.164)	NPI = private numbering plan
0	000 - unknown or 110 - abbreviated number	000 - unknown or 110 - abbreviated number or 001 - level 2 regional number or 101 - level 3 regional number
1	001 - international number	cannot be mapped
2	010 - national number	010 - level 1 regional number
3	011 - network specific number	011 - PTN specific number
4	100 - subscriber number	100 - local number
5	not used	cannot be mapped
6	cannot be mapped	cannot be mapped

Note:
QSIG refers to ISO QSIG and ETSI QSIG.

NPI information printed in the CDR ticket for a non-UIPE and non-MCDN incoming trunk and TON information printed in the CDR ticket for a non-UIPE and non-MCDN incoming trunk show the NPI and TON information for a non-UIPE and non-MCDN incoming trunk.

Table 161: NPI information printed in the CDR ticket for a non-UIPE and non-MCDN incoming trunk

NPI code in CDR	Corresponding value of NPI in specification
00	0000 - unknown numbering plan
01	0001 - Rec. E.164
02	0010 - Rec. E.163
03	0011 - Rec. X.121
04	0100 - Telex numbering plan
08	1000 - national numbering plan
09	1001 - private numbering plan

Note:
Non-UIPE refers to the 1TR6, AXE-10 for Australia and Sweden, Swissnet 2, Numeris VN4, SYS-12, and D70 connectivities.

Table 162: TON information printed in the CDR ticket for a non-UIPE and non-MCDN incoming trunk

TON code in CDR	Corresponding value of TON in specification	
	NPI = ISDN/Telephony numbering plan (Rec. E.164)	NPI = private numbering plan
0	0000 - unknown number[1]	0000 - unknown number[1]
1	0001 - international number[2]	not used
2	0010 - national number[2]	not used
3	not used	0011 - network specific number[2]
4	0100 - subscriber number[2]	not used
5	not used	not used
6	not used	0110 - abbreviated number[2]
1. For SYS-12, AXE-10 for Australia and Sweden, Swissnet, Numeris VN4, and D70 interfaces, all received values are mapped into unknown code. 2. For all interfaces not mentioned in 1.		

NPI information printed in the CDR ticket for an NI-2 incoming trunk and TON information printed in the CDR ticket for an NI-2 incoming trunk show the NPI and TON information for an NI-2 incoming trunk.

Table 163: NPI information printed in the CDR ticket for an NI-2 incoming trunk

NPI code in CDR	Corresponding value of NPI in specification
00	0000 - unknown numbering plan
01	0001 - ISDN/Telephony numbering plan (Rec. E.164)
02	unused
03	unused
04	unused
08	unused
09	1001 - private numbering plan

Table 164: TON information printed in the CDR ticket for an NI-2 incoming trunk

TON code in CDR	Corresponding value of TON in specification	
	NPI = ISDN/Telephony numbering plan (Rec. E.164)	NPI = private numbering plan
0	not used	not used

TON code in CDR	Corresponding value of TON in specification	
	NPI = ISDN/Telephony numbering plan (Rec. E.164)	NPI = private numbering plan
1	001 - international number	not used
2	010 - national number	not used
3	not used	not used
4	100 - local number	100 - subscriber number
5	not used	not used
6	not used	not used

Operating parameters

The NPI and TON in CDR feature applies only for incoming ISDN trunk calls. NPI and TON information depends on the incoming trunk protocol.

The NPI and TON fields are left blank for internal calls, outgoing trunks, incoming non-ISDN trunks, or if the CLID prompt is set to NO.

When the FCDR prompt is set to OLD, the NPI and TON fields do not exist, regardless of how the CLID prompt is defined.

NPI and TON information is available with the following incoming interfaces: EuroISDN, QSIG (ISO and ETSI), MCDN, non-UIPE and non-MCDN, and NI2.

NPI and TON information is included in all types of CDR records that contain CLID information.

NPI and TON information is lost when system initialization occurs and the call is then reconstructed. In this case, if the call involves an incoming ISDN trunk and if the NPI and TON in CDR feature is configured, the NPI field contains two zeros (00) and the TON field contains one zero (0), regardless of the NPI and TON sent at call setup.

Feature interactions

The NPI and TON in CDR feature does not have any specific interactions with other features.

Feature packaging

The NPI and TON in CDR feature requires the following packages:

- Call Detail Recording (CDR) package 4
- Call Detail Recording on Teletype Machine (CTY) package 5
- Calling Line Identification in Call Detail Recording (CCDR) package 118
- New Format Call Detail Recording (FCDR) package 234

Feature implementation

Table 165: LD 17: Configure the NPI and TON fields.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	PARM	System parameters.
...		
FCDR	NEW	New Format CDR. OLD = Old CDR format (default).
...		
CLID	YES	TON and NPI fields, in addition to CLID, are included.

Note:

For the NPI and TON in CDR feature, existing CDR implementation procedures must be performed.

Note:

CLID must be configured for the NPI and TON in CDR feature. Refer to the "Calling Line Identification" and "ISDN Calling Line Identification Enhancements" feature modules in this document.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 37: Overlap Signaling on ISDN Networks

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

On ISDN, dialed digits are sent out and received in the following modes:

- Enbloc
- Overlap

Enbloc Signaling

In Enbloc mode, the switch waits for all the dialed digits from the user and then sends all the digits in the SETUP message.

Overlap Signaling

In Overlap mode, the digits are sent out as they are dialed from the user, instead of waiting for an interdigit timer to timeout. This improves the call setup time. The Overlap Signaling method is useful when a system cannot determine the completion of all the digits unless the originator terminates dialing with an octothorpe "#". Examples of this are when a caller dials:

- international numbers
- private numbers where all the sub-DN digits are not known across the network

Overlap Sending and Overlap Receiving are optional on each D-channel interface for ISDN Trunks.

Overlap Sending

Overlap Sending is applicable to the outgoing leg of the ISDN interface and if enabled on a ISDN interface, it is assumed that the far end supports Overlap Signaling and Overlap Receiving.

Overlap Receiving

Overlap Receiving is applicable to the incoming leg of the ISDN interface. If the ISDN interface does not support Overlap Receiving, then INFO messages received from the originating switch are ignored and the system operates only on the digits received in the SETUP message as if the originating switch used ENBLOC dialing.

ISDN Overlap support lists the ISDN interfaces on the system and whether they support or do not support Overlap Sending and Overlap Receiving.

Table 166: ISDN Overlap support

ISDN interface	Overlap Sending	Overlap Receiving	Notes
Australia ETSI	Y	N	
AXE-10 (Sweden and Australia)	Y	N	Overlap Receiving is possible only if the AXE-10 conforms to the guidelines contained in CCITT's preliminary Q.931 section 5.0
Swiss Net (Switzerland)	Y	N	

ISDN interface	Overlap Sending	Overlap Receiving	Notes
NEAX-61 (New Zealand) (non-Asia Pacific ISDN Connectivity)	Y	N	
SYS-12 (Norway)	Y	N	
Numeris VN3 (France)	Y	N	
1TR6 (Germany)	Y	N	
Japan D70 (non-Asia Pacific ISDN Connectivity)	N	N	
Euro ISDN ETS 300-102 basic protocol	Y	Y	
Austria	Y	Y	
Denmark	Y	N	
Finland	Y	Y	
Germany	Y	Y	
Italy	Y	Y	
Norway	Y	N	
Portugal	Y	N	
Sweden	Y	N	
Ireland	Y	Y	
Holland	Y	Y	
Switzerland	Y	Y	
Belgium	Y	Y	
Spain	Y	Y	
United Kingdom	Y	Y	
France	Y	Y	
Commonwealth of Independent States (Russia and the Ukraine).	Y	Y	
Asia Pacific			
Australia	Y	N	
China	Y	Y	
Hong Kong	Y	N	
India	Y	Y	

ISDN interface	Overlap Sending	Overlap Receiving	Notes
Indonesia	Y	Y	
Japan	N	N	
Malaysia	Y	Y	
Philippines	N	N	
Singapore	Y	N	
Taiwan	Y	N	
New Zealand	Y	N	
Thailand	Y	Y	
QSIG	Y	Y	
JTTC (Japan QSIG)	N	N	
BRI	Y	Y	
MCDN (only SL-1)	Y	Y	
National ISDN NI-1, NI-2, NI-3(North America CO interface)	N	N	
ISL	Y	Y	
VNS	N	N	Call establishment over the VNS D-channel does not use Overlap Sending/Overlap Receiving even if it is configured. Enbloc sending is always used on the VNS D-channel. Overlap sending/receiving is supported on the Bearer trunks, if that capability already exists.

Operating parameters

Overlap Signaling is configured in LD 17 at the Overlap Receiving (OVLR), Overlap Timer (OVLT), Direct Inward Dialing Delete (DIDD) and Overlap Sending (OVLS) prompts and in LD 86 at the Overlap Length (OVLL) prompt.

The OVLT prompt is provided only when OVLS = YES. The response to OVLT indicates the time the MSL-1 system waits to accumulate digits to send in a INFORMATION message. If response to OVLT is zero, then during Overlap Sending state, each dialed digit generates an INFORMATION message.

The DIDD prompt indicates the number of leading digits to delete when receiving digits from a DID trunk.

OVLL is defined on a Route List Block basis. If this value is less than Flexible Length (FLEN), it is the minimum number of digits the user must dial before a SETUP is sent on an ISDN interface, or before outpulsing begins on a non-ISDN trunk. If the response to OVLL is zero, then FLEN must be used to determine how many digits to dial before sending out any Called Party information. If FLEN is also zero, no Overlap Sending is attempted; ENBLOC dialing is used instead.

Feature interactions

Call Back Queuing and Off-hook Queuing

This feature does not support Overlap Signaling.

Flexible Hotline

This feature does not support Overlap Signaling.

VNS

Calls established over the VNS D-channel do not use Overlap Sending/Overlap Receiving, even if configured. The VNS D-channel always uses Enbloc Sending. The Bearer trunks support Overlap Sending and Overlap Receiving, if the capability already exists.

Feature packaging

This feature requires the following packages:

- Basic Routing (BRTE) package 14
- Basic Queuing (BQUE) package 28
- Network Class of Service (NCOS) package 32

- Basic Alternate Route Selection (BARS) package 57
- Network Alternate Route Selection (NARS) package 58 and/or Coordinated Dialing Plan (CDP) package 59
- Flexible Numbering Plan (FNP) package 160
- Overlap Signaling (OVLP) package 184

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 167: LD 17: Configure Overlap Receiving, Direct Inward Dialing Delete, Overlay Sending, and Overlap Timer on page 335

   Note:
   If the interfacing switch supports Overlap Receiving, set the value for the OVLR prompt as YES.
2. Table 167: LD 17: Configure Overlap Receiving, Direct Inward Dialing Delete, Overlay Sending, and Overlap Timer on page 335

   Note:
   The recommended value for the DIDD prompt is 0. But incase, some digits need to be deleted, then this value has to be agreed upon with the interfacing switch.
3. Table 167: LD 17: Configure Overlap Receiving, Direct Inward Dialing Delete, Overlay Sending, and Overlap Timer on page 335

   Note:
   If the interfacing switch supports Overlap Sending, set the value for the OVLS prompt as YES.
4. Table 167: LD 17: Configure Overlap Receiving, Direct Inward Dialing Delete, Overlay Sending, and Overlap Timer on page 335

   Note:
   A recommended value for OVLT is 1. This means that the digits dialed by the user will be collected for 1 second before being sent in INFORMATION messages. If a user dials at a rate of 1 digit every.5 seconds, there will be two digits for each INFO message. If the messaging traffic on the D-Channel is of major concern, a higher value of OVLT can be used. The greater the value of

OVLT, the lower the volume of messages generated by the particular call. OVLT must always be less than the values of T302 and T304 for the given interface.

5. Table 168: LD 86: Configure the Overlap Digit Length on page 335

Note:

OVLL is flexible. The smaller the value, the fewer the number of digits that will be included in the SETUP message. For non-ISDN routes, the smaller the value, the faster a non-ISDN route will begin outpulsing. It is recommended that OVLL be at least the average number of digits in the ESN or CDP steering code that will be using the particular Route List Block. If the average number of digits in an ESN or CDP steering code is three then a recommended value for OVLL would be 5. It is also recommended that OVLL be less than FLEN.

6. Table 169: LD 90: Configure the Flexible Digits on page 336

Note:

LD 90 - prompt FLEN: It is recommended that FLEN be the maximum number of digits that can be used for this ESN or CDP steering code. It is also recommended that FLEN be greater than OVLL.

Table 167: LD 17: Configure Overlap Receiving, Direct Inward Dialing Delete, Overlay Sending, and Overlap Timer

Prompt	Response	Description
REQ	NEW CHG	Add new data or change existing data
TYPE	CFN	Configuration Record
- OVLR	YES	Allow Overlap Receiving.
- - DIDD	(0)-15	Number of leading digits to delete from DID trunks.
- OVLS	(NO) YES	(Do not) allow Overlap Sending.
- - OVLT	(0)-8	Overlap Timer in seconds. This timer controls the interval between the sending of INFORMATION messages. "0", the default, means send immediately.

Table 168: LD 86: Configure the Overlap Digit Length

Prompt	Response	Description
REQ	NEW CHG	Add new data or change existing data
TYPE	CFN	Configuration Record
- OVLL	(0)-24	Enter the minimum Overlap Length, pertaining to Overlap Sending. If 0 (the default) is entered, then the Flexible Digit Number Length (FLEN) determines whether Overlap Sending takes place.

Table 169: LD 90: Configure the Flexible Digits

Prompt	Response	Description
REQ	NEW CHG	Add new data or change existing data
TYPE	CFN	Configuration Record
- FLEN	(0)-24	Enter the number of Flexible Digits (the number of digits that the system expects to receive before accessing a trunk, and outpulsing the digits).

Feature operation

No specific operating procedures are required to use this feature.

Chapter 38: Private to Public CLID Conversion

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

The Private to Public Calling Line Identification (CLID) Conversion feature permits the correct CLID to be sent to the CO when a call hops off the private network to the public network (the PSTN) at a tandem node.

On ISDN trunks, Calling Line Identification (CLID) information is sent in the Calling Party Information Element (IE) of the setup message. This information is used to display the originating party's number on the terminating phone. A Call Type indicator is also present, to indicate to the switch at the other end what type of call it is receiving (International, National, Subscriber, UDP, CDP, SPN). This in turn affects how that switch handles the call using the INAC prompt.

Originating nodes configure the format of the CLID using the following components:

- the dialing plan used to make the call
- the type of trunk used for the call
- the Customer Data Block option and Class of Service of the phone related to sending the Prime DN (PDN) or Listed Directory Number (LDN) of the phone

For example, a call dialed with a Location Code (private Uniform Dialing Plan), that is sent out on a private network trunk (TIE trunk) has a CLID in the private network format (LOC+DN). However, a Location Code call that is sent out on a public network trunk (a COT trunk, for example) has a CLID in the public network format [National (NPA+NXX+DN)]. The public network number can be the LDN of the customer group for non-DID phones or the NPA+NXX +DN for DID users.

If the default method for constructing Call Types is not suitable, the administrator can program Digit Manipulation Indexes to apply to calls as they leave the switch to change the Call Type indicator that travels with each call.

Prior to this feature introduction, a tandem node that received CLIDs from another node on an ISDN TIE trunk passed the CLIDs along without changing them. A system acting as a tandem node did not convert a private format CLID to a public format CLID when routing a call on a PSTN trunk. The private format CLID of the originating phone was sent to the Central Office (CO). However, there are COs in North America that modify the CLID (adding an NPA and NXX) when less than ten digits are received. If the system sends seven digits in the CLID to the PSTN, the CO automatically inserts the NPA of the serving area. Therefore, the CLID ends up as: NPA+LOC+DN. Therefore, the terminating phone displayed a CLID that was sometimes a valid phone number in the area around the tandem node, but it was not the correct CLID of the originating user.

The scenario described above is illustrated inFigure 48: Private network to Public network hop off, prior functionality for UDP dialing on page 339 on Private network to Public network hop off, prior functionality for UDP dialing.

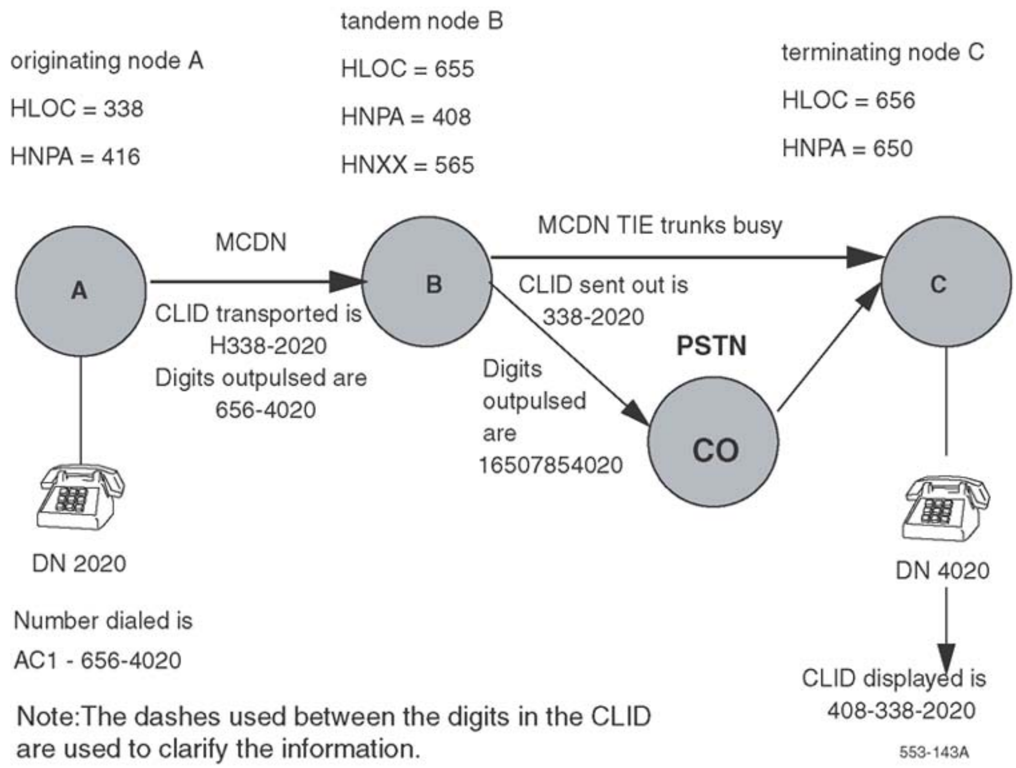

Figure 48: Private network to Public network hop off, prior functionality for UDP dialing

In the example in Private network to Public network hop off, prior functionality for UDP dialing, the calling party dialed a private number in the UDP format: LOC+DN (656-4020). The originator's DN is 2020 and the LOC is 338. If the call is routed all the way through the private network, the user on DN 4020 sees H3382020 on the display. (The terminating node inserts the letter H in front of the CLID digits to indicate that the call originated from the private network.)

If the call encounters "all trunks busy" on the TIE trunks to switch C at the tandem node, switch B is programmed to alternately route the call out to the CO. The calling number digits (3382020) are sent to the CO. The CO sees seven digits and, if ten digits is a requirement, inserts the NPA of the serving area around the tandem node, (408 in this example). When the call reaches the destination, the display reads 4083382020. This CLID is not the correct number for the originator. However, it is possible that the number is valid for a subscriber in the 408 area code. When the terminating party attempts to use the CLID for callback purposes, it can result in a call to someone in the 408 area code who did not originate the earlier call.

The Private to Public Calling Line Identification (CLID) Conversion feature is applicable to Electronic Switched Networks (ESNs) that use the following private network numbering plans and codes:

- Uniform Dialing Plan (UDP) and Location Codes (LOCs)
- Coordinated Dialing Plan (CDP) and Distant Steering Codes (DSCs)

A private format CLID can be in either of the following formats:

- LOC+DN
- DSC+X..X

The Private to Public CLID Conversion feature provides two different options to send a public format CLID to the PSTN. The options are:

- CLID contains the NPA and NXX of the originating node. For outgoing calls from the tandem node you translate location codes (LOC) and/or Distant Steering Codes (DSC). For incoming calls from those switches and CLID conversion purposes, you program the NPA and NXX of each originating node to associate with its LOC or DSC at the tandem node. The tandem node uses this NPA and NXX to build a public format CLID for the originator when calls from that switch hop off to the public network from the tandem node.
- CLID contains the LDN of the tandem node. You can use the LDN of the tandem node for the public format CLID.

This feature introduces a prompt (CPUB) in the Route Data Block (LD 16). This prompt controls what option applies when the tandem node builds the public format CLID. Program the CPUB option on the outgoing PSTN routes. The CPUB options are:

- ON
- OFF
- LDN

ON means the feature is enabled. The system uses the NPA and NXX programmed for the LOC or DSC of the caller to build the CLID.

OFF means the feature is disabled. The CLID is built as it was prior to the introduction of this feature.

LDN The tandem node sends its LDN0 (from LD 15) to the CO as the CLID. The CLID is constructed by coupling the HNPA and HNXX in CLID entry 0 in the Customer Data Block (LD 15) with the LDN0 from LD 15 at the tandem node.

Uniform Dialing Plan (UDP)

In LD 90 you program an NPA and NXX (to be used for CLIDs) for each LOC you translate.

Figure 49: Private network to Public network hopoff, NPA and NXX conversion functionality for UDP dialing on page 342 on Private network to Public network hopoff, NPA and NXX conversion functionality for UDP dialing illustrates the effect of the conversion capability when a user dials a private network call in the UDP format and the tandem node is programmed to send the CLID of the originator.

Figure 50: Private network to Public network hopoff, LDN conversion functionality for UDP dialing on page 343 on Private network to Public network hopoff, LDN conversion functionality for UDP dialing illustrates the effect of the conversion capability when a user dials a private network call in the UDP format and the tandem node is programmed to send its LDN as the CLID.

Before sending the call to the CO, the system software checks the Route Data Block for the PSTN route. It checks the CPUB option and one of the following results can occur:

- if it is "OFF", no manipulation of the digits occurs. The Private CLID is sent to the CO. Figure 48: Private network to Public network hop off, prior functionality for UDP dialing on page 339 on Private network to Public network hop off, prior functionality for UDP dialing illustrates what happens when CPUB is OFF.
- if it is "ON" the software checks the CLID within the Calling Party IE of the outgoing setup message. UseFigure 49: Private network to Public network hopoff, NPA and NXX conversion functionality for UDP dialing on page 342 on Private network to Public network hopoff, NPA and NXX conversion functionality for UDP dialing as an example. The software detects the leading digits (338) and checks LD 90 for translation of LOC 338. If it is in the translation tables, the software checks for NPA and NXX entries for that location code. If these entries are there, the LOC 338 is replaced by the NPA and NXX. The changed CLID number is sent to the CO. In this example, 3382020 is replaced by 4162532020. This is a number which the terminating user can dial to reach the originator.
- if it is "LDN", the listed directory number of the tandem system is sent. The LDN0 of the tandem node is paired with the HNPA and HNXX associated with CLID entry 0 in LD 15 to build the CLID that is sent to the CO. Refer to Figure 50: Private network to Public network hopoff, LDN conversion functionality for UDP dialing on page 343 on Private network to Public network hopoff, LDN conversion functionality for UDP dialing.

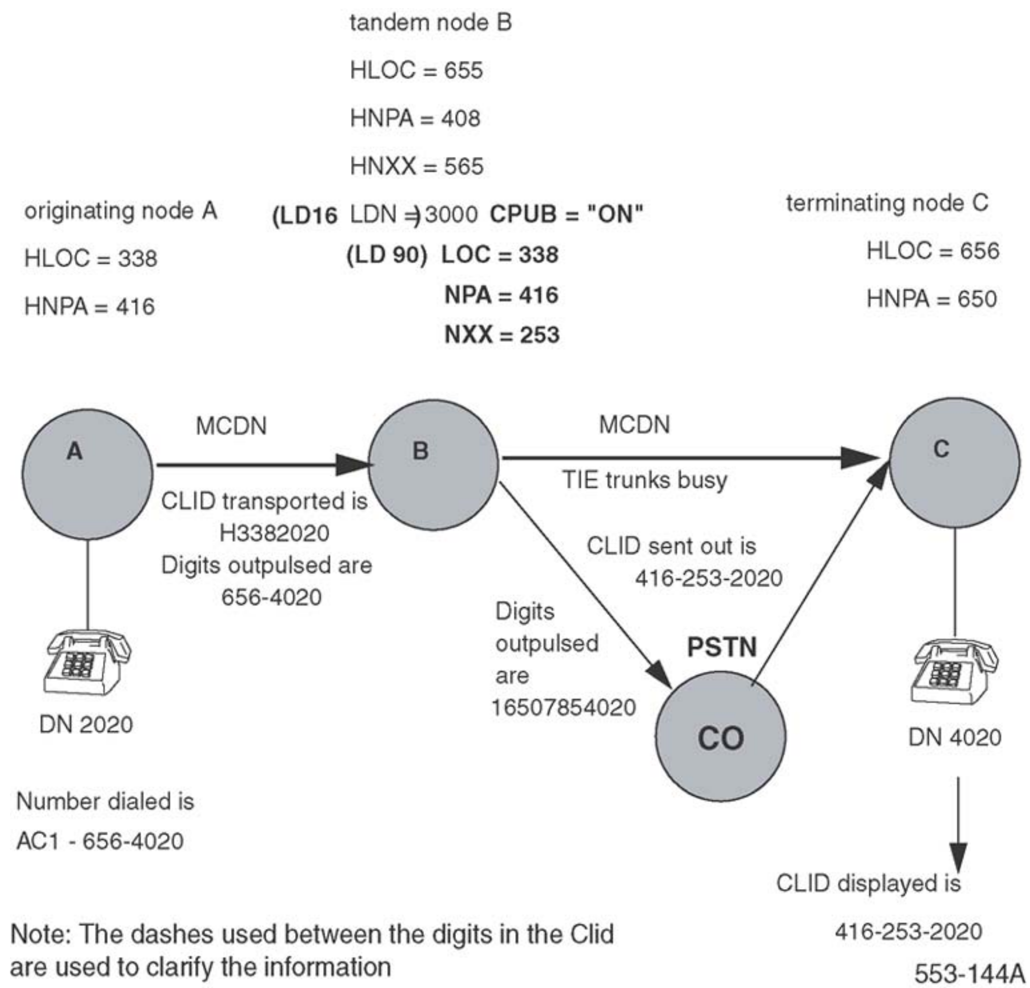

Figure 49: Private network to Public network hopoff, NPA and NXX conversion functionality for UDP dialing

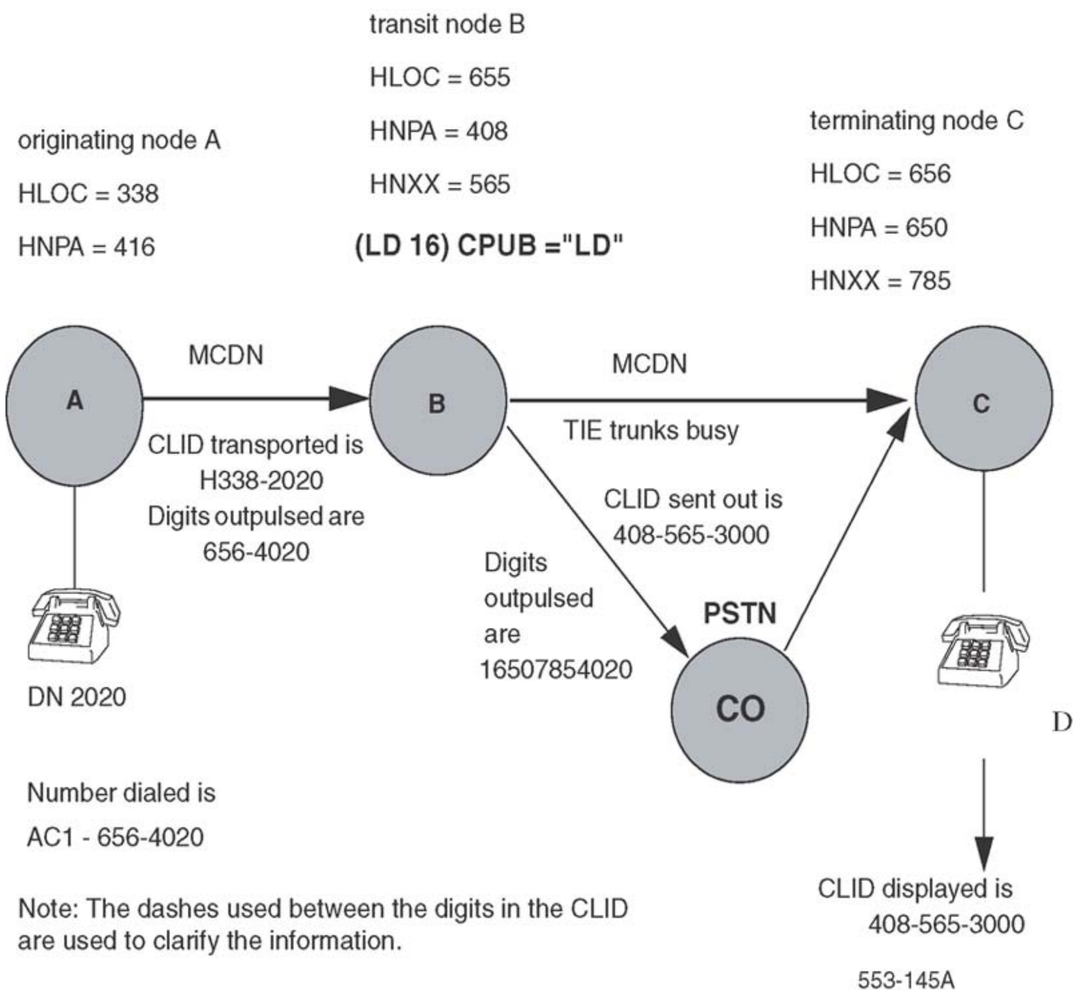

Figure 50: Private network to Public network hopoff, LDN conversion functionality for UDP dialing

Coordinated Dialing Plan

In LD 87, at a tandem node, program an NPA and NXX for each Distant Steering Code (DSC) you translate. The system uses this information to build public format CLIDs.

In the examples that follow, the calling party (DN 2020) dials a private network number (4020). The tandem node translates this number as a DSC (4) followed by the digits 020.

If the switches can use the private network for the call, the user on DN 4020 sees CLID H2020 on the display.

If the TIE trunks at the tandem node to the destination node are all busy, the tandem node can send the call out to the CO. With the conversion feature turned off, the CLID sent to the CO is 2020.

In the figures that follow, the tandem node is in area code (NPA) 408 and has an exchange code (NXX) of 565. If the CO requires ten-digit CLIDs, it inserts 408 and 565 as leading digits in the CLID. When the call reaches the destination, the display reads 4085652020. It is possible that this number is a valid number for a subscriber in area code 408. The user at the terminating phone cannot use this number to place a call to the originator of the call.

Private network to Public network hopoff, prior functionality for CDP dialing on Private network to Public network hopoff, prior functionality for CDP dialing shows you how a tandem node and a CO build a CLID when a system with CDP does not have the Private to Public CLID Conversion feature.

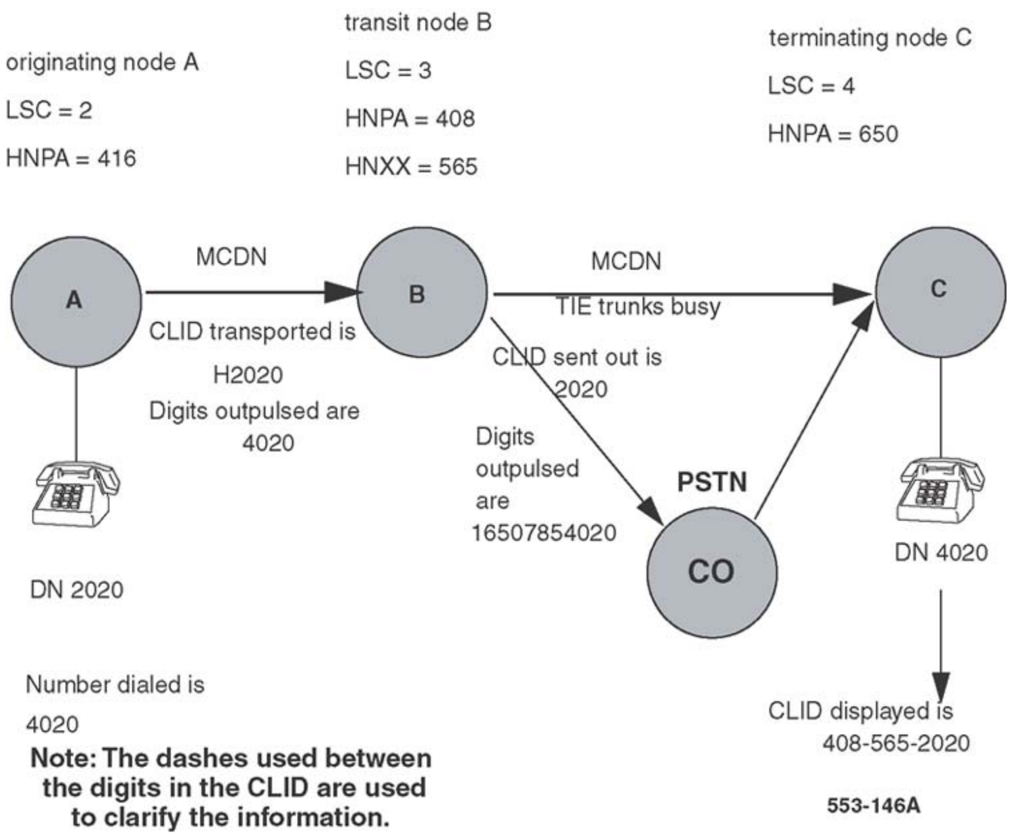

Figure 51: Private network to Public network hopoff, prior functionality for CDP dialing

Figure 52: Private network to Public network hopoff, NPA and NXX conversion functionality for CDP dialing on page 346 on Private network to Public network hopoff, NPA and NXX conversion functionality for CDP dialing illustrates the effect of the conversion capability when a user dials a private network call in the CDP format and the tandem node is programmed to send the CLID of the originator.

Figure 53: Private network to Public network hopoff, LDN conversion functionality for CDP dialing on page 347 on Figure 53: Private network to Public network hopoff, LDN conversion functionality for CDP dialing on page 347 illustrates the effect of the conversion capability when a user dials a private network call in the CDP format and the tandem node is programmed to send its LDN as the CLID.

Before sending the call to the CO, the system software checks the Route Data Block for the PSTN route. It checks the CPUB option and one of the following results can occur:

- If it is "OFF", no manipulation of the CLID digits occurs. The tandem node sends the Private CLID to the CO.Figure 51: Private network to Public network hopoff, prior functionality for CDP dialing on page 344 shows you the CLID format when the CPUB option is OFF.
- If it is "ON" the software checks the CLID within the Calling Party IE of the outgoing setup message. Use Figure 52: Private network to Public network hopoff, NPA and NXX conversion functionality for CDP dialing on page 346 on Figure 52: Private network to Public network hopoff, NPA and NXX conversion functionality for CDP dialing on page 346 as an example. The software detects the leading digits (2020). The system checks for a DSC translation entry in LD 87 equal to 2, 20, 202, or 2020. (It uses the left-wise unique rule.) If there is an entry for the DSC, the software checks for NPA and NXX entries for that Steering Code. The node adds the NPA and NXX as leading digits in the CLID. The software automatically deletes the DSC from the CLID. You must include the removed DSC at the end of the NXX field to maintain the accuracy of the CLID. The node sends the changed CLID to the CO. In this example, 4162532020 replaces 2020. The terminating user can dial this number to reach the originator.
- If it is "LDN", the node sends its listed directory number as a CLID to the CO. The node attaches the HNTN and HLCL from CLID entry 0 in LD 15 to the LDN0 in LD 15. It sends this CLID to the CO.

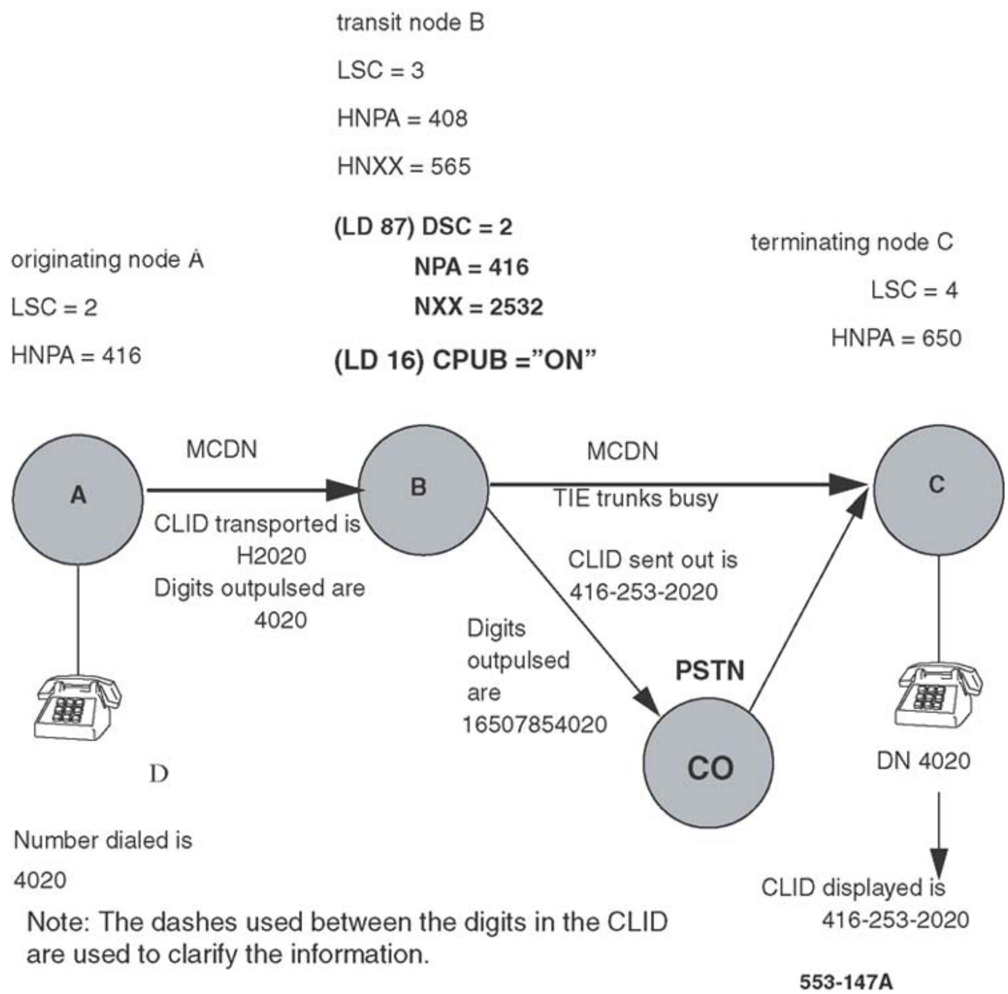

Figure 52: Private network to Public network hopoff, NPA and NXX conversion functionality for CDP dialing

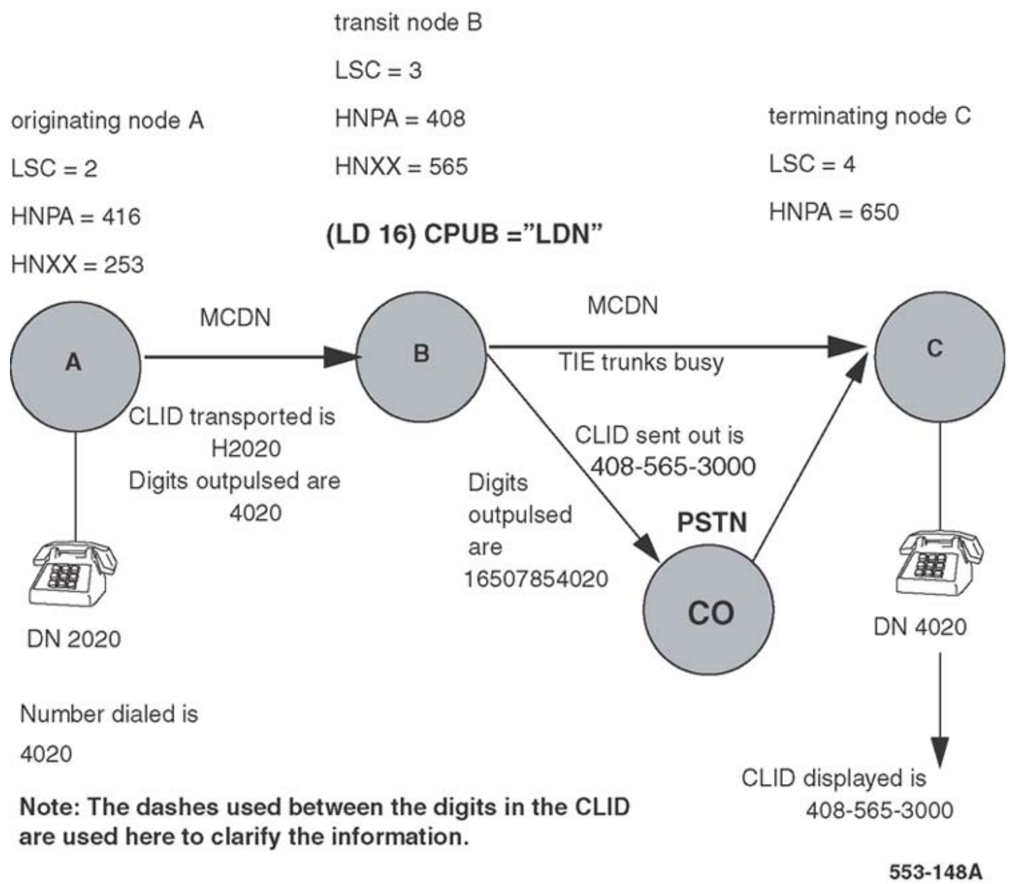

Figure 53: Private network to Public network hopoff, LDN conversion functionality for CDP dialing

Operating parameters

You can use these features with the following types of ISDN interfaces at the tandem node:

- DMS 100
- DMS 250
- #4 ESS
- #5 ESS
- SL-100
- NI-2 TR-1268

The conversion of the CLID also occurs when features such as Call Forward All Calls, Forward No Answer, and Hunting divert calls to the public network.

Some COs use the CLID to perform billing. When a system tandem node interfaces with one of these COs, set the CPUB option to "LDN" to allow correct billing. Or else, with the CPUB option on, the CO uses the originator's CLID for billing purposes. The call used the private network part of the way; the bill for the call is not correct when it is based on this CLID. If you use the Incoming Trunk Programmable Calling Line ID feature, it takes priority over the Private to Public CLID conversion feature (refer to Feature interactions).

The software does not validate the NPA and NXX you input for each LOC and DSC. When you test the operation of this feature, check the CLID shown on the display of the terminating phone. Make sure it is the call originator's CLID.

When used with CDP, the software automatically deletes the DSC from the CLID. You must include the removed DSC at the end of the NXX field to maintain the accuracy of the CLID. For example, if the DSC is 32 and the NXX is 658, program the NXX as 65832 in order to construct the correct CLID.

To activate the feature you must enable it in LD 16 on the outgoing PSTN route. You must also program an NPA and NXX for each LOC in LD 90 or each DSC in LD 87. If you do not program an NPA and NXX in LD 90 or LD 87, the system cannot build the public format CLID.

The feature does not work if CPUB = LDN but there is no LDN0 or CLID entry 0 in LD 15.

The tandem node must receive the CLID in the LOC+DN or DSC+X..X format for the feature to operate.

This feature addresses only private to public CLID conversion and not public to private CLID conversion.

The Private to Public CLID Conversion feature provides one NPA and one NXX for each LOC or DSC. To support networks with switches that have more than one NPA or NXX, assign one LOC or DSC for each NPA or NXX.

The feature does not operate if the originating CLID contains a DSC or LOC that the tandem node cannot translate. (One reason not to translate an LOC or DSC is to block outgoing calls to that destination from the tandem node.) Solution: Add the codes to the translation tables at the tandem node so it can convert incoming CLIDs to the correct public network format. Block outgoing calls from the tandem node to the destination with other forms of restriction. [For example, you can use Supplemental Digit Restriction (in LD 90) or Facility Restriction Levels (in LD 86)].

This feature only operates on the CLID and not on other information elements such as the redirecting number, the connected name, or the connected number.

The tandem node has limitations when it handles calls from an originating switch that has both DID and non-DID DNs. The tandem node converts all CLIDs from a switch with one LOC the same way. You can program the tandem node to send its LDN for non-DID DNs at the originating switch, if these DNs are associated with a different LOC than the DID DNs.

Feature interactions

Automatic Call Distribution (ACD)

When a private call is presented to an ACD DN, and the call flows to the PSTN due to the ACD Night Call Forward or the Interflow or the Overflow feature, the Private to Public CLID Conversion feature operates.

Call Redirection (External Calls)/Hunting

Call Redirection includes the following redirections at the tandem node:

- Call Forward All Calls
- Call Forward Busy
- Call Forward by Call Type
- Call Forward External Deny
- Call Forward No Answer/Flexible Call Forward No Answer
- Call Forward No Answer, Second Level
- Call Redirection by Time of Day
- Call Redirection by Day

When a call forwards to an external phone, and if the call is sent out on a PSTN route, then the Private to Public Conversion feature configures a public format CLID, if the option is configured at the node that is redirecting the call. The same applies to Hunting, if the Hunt DN is an external number.

Alternate Routing

The Private to Public CLID Conversion feature applies to calls which are alternately routed by one of the following features: Network Alternate Routing (NARS), QSIG Alternate Routing, and MCDN Alternate Routing.

Call Transfer

The Private to Public Conversion feature has no interaction with Call Transfer. The prior functionality continues.

Calling Party Privacy (CPP) and Calling Party Privacy Override (CPPO)

A call marked as a CPP or CPPO call can hopoff the private network to the public network. Even though the Private to Public Conversion feature modifies the private CLID to a public format CLID, the presentation indicators indicating whether this is CPP/CPPO call are not modified. After hopoff occurs, the call continues to be identified as a CPP or CPPO call.

Call Detail Recording (CDR)

This feature has no interaction with CDR. After the CLID is converted, the information in the call record is the same as it was with no conversion.

Incoming Trunk Programmable Calling Line ID

The Incoming Trunk Programmable Calling Line ID feature allows you to program a CLID (or billing number) on an incoming route. This feature takes precedence over the Private to Public CLID Conversion feature when they are both programmed at the tandem node.

Meridian Mail

In a case where a call terminates on Meridian Mail with a converted CLID, the private greeting is not given. Either an unknown origin or public greeting is given.

Call Sender feature

This feature has no interaction with the Call Sender feature of Meridian Mail. If a public format, converted CLID is received and the Call Sender feature is configured in Meridian Mail, the user can use Call Sender to callback the caller.

Remote Virtual Queuing

Remote Virtual Queuing continues to work normally. During a call reinitiation (when a public network trunk becomes available), if a hopoff to the public network takes place, this feature converts the originating CLID to a public format.

Network feature interactions

CLID Enhancements

The CLID Enhancements feature provides flexibility in the way the CLID at the originating node is built. The Private to Public Conversion feature works at the tandem node, and does not have any interaction with the CLID Enhancements feature. If the tandem node is configured to send the LDN of as the CLID, CLID entry Ô0" from LD 15 is used to build the tandem node LDN CLID.

Network ACD

When Network ACD routes a call over a PSTN route, the Private to Public CLID Conversion feature builds a public format CLID, if this option is configured at the node that diverted the call.

Network Ring Again

The Network Ring Again feature continues to work normally. During a call reinitiation, if a hopoff to the public network takes place, this feature converts the originating CLID to a public format.

Internet Telephony Gateway (ITG)

ITG 2.0 implements ITG with ISDN as ITG ISL. When an ITG ISL trunk call hops off to the public network, the system builds a public network format CLID, if this feature is configured.

Feature packaging

This feature requires the following packages:

- Network Alternate Route Selection (NARS) package 58 (and Basic Automatic Route Selection (BARS) package 57 - optional) and/or Coordinated Dialing Plan (CDP) package 59
- Integrated Services Digital Network (ISDN) package 145
- Primary Rate Access (PRA) package 146 or 2.0 Mbit Primary Rate Interface (PRI2) package 154

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

Table 170: LD 16: Configure the PSTN route for Private to Public CLID Conversion.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...	...	
ROUT		Route number

Prompt	Response	Description
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...	...	
ISDN	YES	Integrated Services Digital Network.
- IFC	a..a	Interface type for route. IFC must be one of the following for the CPUB prompt to appear: S100, D100, D250, ESS4, ESS5, NI2.
...	...	
CPFXS	(YES) NO	Customer-defined prefixes.
CPUB		Conversion to public number feature.
	(OFF) ON	No conversion; CLID remains in private number format. Send the NPA and NXX associated with LOC (in LD 90) or DSC (in LD 87).
	LDN	Send the LDN of this node.

Table 171: LD 87: Configure the NPA and NXX associated with each DSC.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	CDP	Coordinated Dialing Plan.
TYPE	DSC	Distant Steering Code.
DSC	x..x	Distant Steering Code digits.
- RLI	xxx	Route List Index (used for outgoing calls).
...	...	
-- NPA	x..x	NPA to be inserted in the outgoing public format CLID when this DSC is received in the CLID of an incoming call (maximum seven digits).
-- NXX	x..x	NXX to be inserted in the outgoing public format CLID when this DSC is received in the CLID of an incoming call (maximum seven digits).

Table 172: LD 90: Configure the NPA and NXX associated with each LOC.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	NET	Network Translation.
TRAN	AC1 AC2	Access code 1 translation table. Access code 2 translation table.
TYPE	LOC	Location code.
LOC	x..x	Location code digits (maximum seven digits).
- RLI	xxx	Route List Index (used for outgoing calls).
-- NPA	x..x	NPA to be inserted in the outgoing public format CLID when this LOC is received in the CLID of an incoming call (maximum seven digits).
-- NXX	x..x	NXX to be inserted in the outgoing public format CLID when this LOC is received in the CLID of an incoming call (maximum seven digits).

Feature operation

No specific operating procedures are required to use this feature.

Chapter 39: QSIG Message Waiting Indication Supplementary Service

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The QSIG Message Waiting Indication Supplementary Service (QSIG MWI SS) feature allows the transport of an MWI message between system networks and multi-vendor networks, using the industry standard QSIG protocol.

With this feature, the Served User (the person receiving the message) receives an MWI appropriate for their system when they have at least one new VoiceMail message. For the system user, the red LED is lit, the Message Waiting key lamp flashes or a stutter tone is heard to indicate a new VoiceMail message. When the system user retrieves the message, the MWI is deactivated.

The MWI is transported in the following manner:

1. A Meridian Message Center (for example, Avaya CallPilot) sends an MWI message to the Meridian Message Center Private Integrated Services Network Exchange (PINX) that an unheard VoiceMail message exists for a user. The user is located in

a different multi-vendor Private Integrated Services Network (PISN). See Figure 54: MWI message transport between a system network and a multi-vendor network on page 356.

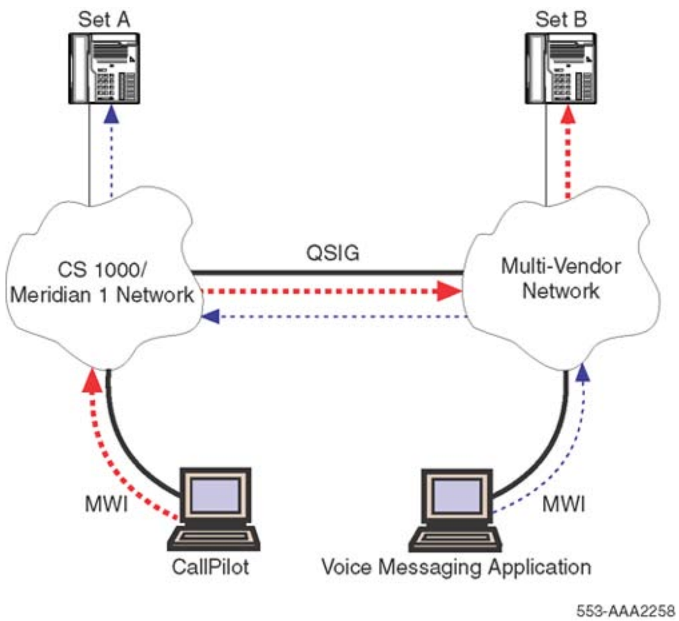

Figure 54: MWI message transport between a system network and a multi-vendor network

2. The Message Center PINX phones up a connection to the multi-vendor Message Center PINX, possibly through one or more transit PINXs.
3. At the MCDN-QSIG gateway of the system network, the MWI message is translated to a QSIG MWI GF Facility message and transported over QSIG to the multi-vendor PINX. See Figure 55: MWI message transport over QSIG in a PISN on page 357 on Figure 55: MWI message transport over QSIG in a PISN on page 357.

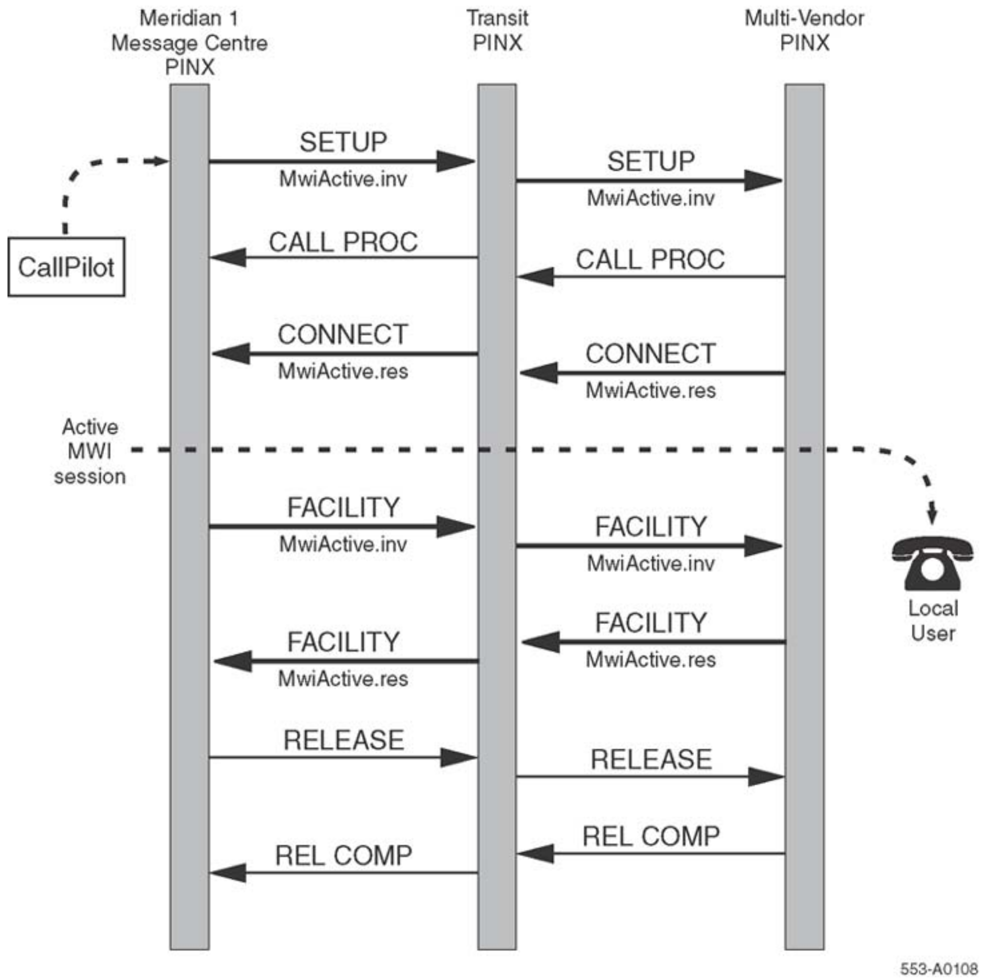

Figure 55: MWI message transport over QSIG in a PISN

4. The multi-vendor's PINX notifies its Message Center that there is an MWI message for a local user.
5. That Message Center activates the local user's VoiceMail message MWI. When the VoiceMail message has been heard, the MWI is de-activated.

For example, if the system network CallPilot receives an MWI message from Phone A for a user in a multi-vendor network (Phone B), the MCDN-QSIG gateway software sends a MWI GF Facility message telling Phone B that there is a new VoiceMail message in their VoiceMail box.

If the foreign network's voice messaging application sends an MWI message from Phone B to Phone A, the MCDN-QSIG gateway software receives the MWI GF Facility message. The system software interprets the message and performs the same actions as if the MWI message had been received from the local CallPilot. The system software activates Phone A's Message Waiting Indication key LED.

When an MWI message is received for a DN assigned to multiple phones, the Message Waiting Indication is activated on each of the phones. When all new messages are heard, the system cancels the MWI on all phones.

QSIG-MCDN Gateways

QSIG MWI Facility messages at QSIG-MCDN Gateway nodes are translated to MCDN MWI Facility messages. MCDN MWI Facility messages at QSIG-MCDN Gateway nodes are translated to QSIG MWI Facility messages.

Operating parameters

The QSIG Message Waiting Indication Supplementary Service feature supports all Meridian phones that support Message Waiting Indication.

QSIG MWI SS requires a Coordinated Dialing Plan (CDP) or a Uniform Dialing Plan (UDP) between the networks using QSIG MWI SS.

ESIG and ISIG networks do not support QSIG MWI SS.

QSIG MWI SS does not support the Remote Call Sender feature.

The QSIG MWI SS feature does not support the QSIG-DPNSS Gateway.

The QSIG-MCDN interface does not support the transport of the MWI Interrogate facility message; however, it tandems MWI Interrogate facility messages to other multi-vendor switches that do support it.

On any system, either the Server User node or the Message Center node must have the QSIG Supplementary Services (QSIG-SS) package 316 equipped in order to use the MWI service.

The QMWI feature is only supported with CallPilot and Meridian Mail as the local message centers hosted off a system running Succession 3.0 software or later. It is not supported with CallPilot MINI or any other systems (for example, Octel VM) that do not use a link for integration. QMWI cannot be used with phone integration or MIK MCK keys.

Feature interactions

Meridian End-to-End Transparency

The system sends the proprietary QSIG MWI message between system switches over a QSIG interface, using Meridian End-to-End Transparency (MEET). MEET requires a Remote Capability (RCAP) of MCDN QSIG Conversion as a Remote Capability (MQC) on the D-channel.

The QSIG MWI SS sends the QSIG MWI message between system switches and multi-vendor switches, using the industry-standard QSIG protocol. QSIG MWI SS requires a RCAP of QSIG Message Waiting Indication using Integer Value (QMWI) or QSIG Message Waiting Indication using Object Identifier (QMWO).

Remove RCAP MQC, if implemented on a D-channel, before implementing RCAP QMWI/QMWO.

Feature packaging

QSIG Message Waiting Indication Supplementary Service (QSIG MWI SS) is included in QSIG Supplementary Services (QSIG-SS) package 316.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 173: LD 15: Configure a PINX DN for the customer. on page 359
2. Table 174: LD 16: Configure QSIG MWI for QSIG BRI trunks. on page 360
3. Table 175: LD 17: Configure QSIG MWI for PRI trunks. on page 360

Table 173: LD 15: Configure a PINX DN for the customer.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	NET	Networking data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
PINX_ DN	xx....x	Private Integrated Services Network Exchange DN Node DN (up to seven digits).

Table 174: LD 16: Configure QSIG MWI for QSIG BRI trunks.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
...	...	
DTRK	YES	Digital Trunk Route.
DGTP	BRI	Basic Rate Interface (BRI) Digital Trunk Type.
...	...	
IFC		Interface type for this route.
	ESGF ISGF EGF4	ESIG interface with GF platform. ISIG interface with GF platform. Q Reference Signaling Point interface.
...	...	
RCAP		Remote Capabilities.
	QMWI	Add Message Waiting Indication as a remote capability. The encoding method uses Integer Value.
	QMWO	Add Message Waiting Indication as a remote capability. The encoding method uses Object Identifier. Do not configure QMWI and QMWO on the same link at the same time. XQMW = Remove Message Waiting Indication as a remote capability.

Table 175: LD 17: Configure QSIG MWI for PRI trunks.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	Action Device and Number.
ADAN	NEW DCH xx CHG DCH xx	New D-channel number. Change D-channel number where: xx = 0 – 63.
...	...	
IFC		Interface type for this route.
	ESGF ISGF EGF4	ESIG interface with GF platform. ISIG interface with GF platform. Q Reference Signaling Point interface.
RCAP		Remote Capabilities.

Prompt	Response	Description
	QMWI	Add Message Waiting Indication as a remote capability. The encoding method uses Integer Value.
	QMWO	Add Message Waiting Indication as a remote capability. The encoding method uses Object Identifier. Do not configure QMWI and QMWO on the same link at the same time.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 40: Recall with Priority during Night Service Network Wide

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

This feature adds the Recall with Priority during Night Service (RPNS) functionality to a network-wide application. For this network application, RPNS is activated on a customer basis from an Attendant Console, according to the NITE service specifications defined in the Network Attendant Service feature description.

If NAS is not active, then conventional attendant service and Night Service are in effect.

Service is provided as follows when NAS is activated:

- If Night Service is not active (the NITE key is dark), calls are routed to a Local or Remote attendant.
- If Night Service is active at a local node (the NITE key is lit), the call is directed to a Remote attendant, queued to a route, or presented to a Night Station. If the NAS schedule does not define an alternative attendant location for this period:
    - If the call is local, night service is given or

- If the call is from a Remote node, it is routed to its originating node if Drop Back is allowed. If Drop Back is not allowed, Night Service is given at the node receiving the call.

Operating parameters

This feature applies only to incoming external calls.

Feature interactions

Night Service Improvement or Enhanced Night Service feature

If Recall with Priority during Night Service is equipped along with either the Night Service Improvement or Enhanced Night Service feature, calls are processed according to priority.

Feature packaging

International Supplementary Services (SUPP) package 131 is required for Recall with Priority during Night Service.

Since Network-wide LDN requires Network Attendant Service routing, the following software packages must also be provisioned:

- Basic Routing (BRTE) package 14
- Network Class of Service (NCOS) package 32
- Network Alternate Route Selection (NARS) package 58
- Network Attendant Service (NAS) package 159
- Applicable ISDN options depending upon customer requirements

Feature implementation

Table 176: LD 15: Enable the network capability of Recall with Priority during Night Service in the Customer Data Block.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	NIT	Night Service data
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
RPNS	(NO) YES	Recall with Priority during Night Service.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 41: Recorded Announcement for Calls Diverted to External Trunks

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Recorded Announcement for Calls Diverted to External Trunks (RANX) provides an optional recorded announcement when the call is being forwarded to the external Public Exchange through DTI, DTI2, PRI2, PRI, analog, and BRI trunks connected to AXE-10 or EuroISDN routes. The announcement notifies the calling party that call forwarding is taking place and the call set-up can require more time than usual. The delay depends upon the signaling that is required to reach the destination party.

Note:

ISDN BRI trunking is not available in North America.

The message is given if the outgoing route is supported by the RANX feature. The calling party receives RAN treatment until either the message is finished or until an answer is received from the external Public Exchange trunk.

This feature operates on a route basis and is controlled by a the RANX prompt in LD 16, for calls diverted to external trunks.

Operating parameters

The RANX feature is supported only for external CO routes. The corresponding RANX prompt in LD 16 appears when the trunk type is:

- A Central Office Trunk (COT) and is not configured as a Radio Paging (RPA) trunk. The trunk has to be configured as an outgoing or outgoing/incoming trunk. The feature is not applicable for trunks configured solely for data traffic.
- A Direct Inward Dialing (DID) trunk configured as an outgoing or outgoing/incoming trunk. The feature is not applicable for trunks configured solely for data traffic.

The RANX feature requires a Recorded Announcement (RAN) machine in the same node as the outgoing route.

If the RAN trunk is configured with supervision, the calling party who is connected to the RAN trunk will be charged from the time the answer signal is sent.

This feature is supported network wide in a Meridian Customer Defined Network (MCDN) environment; no other private network protocols are supported.

Since Digital Private Network Signaling System (DPNSS1) does not support any information concerning redirection, this feature is not supported in a DPNSS1 network.

If a phone is forwarded to a trunk configured with the RANX feature and the party that calls the extension is supposed to dial additional digits, this is not always possible. If the calling party dials digits when being provided with RAN, those digits will be lost since they are not buffered.

If the outgoing trunk, or the phone from which the call originated, times out during the RAN, it is not possible to dial additional digits after the RAN is terminated.

If a DISA call is forwarded to a route with the RANX feature configured, and the RAN message that is provided to the calling party is longer than the duration of the EOD timer, the RAN will be interrupted when the EOD timer expires. When the EOD timer expires, the call is considered as established.

Feature interactions

Call Forward All Calls/Busy/No Answer/Hunt

RANX is activated if the call is forwarded to an outgoing external CO trunk with the RANX feature active.

Network Call Forward

The RANX feature supports call forward to an outgoing external CO route if the route has RANX configured and is located in a node with a RAN trunk. The originating party and the forwarded phone can be in different nodes in the MCDN network.

Internal Call Forward

The RANX feature supports call forward to an outgoing external CO trunk if the route has RANX configured and is located in a node with a RAN trunk.

Phantom TN

If a Phantom TN is forwarded to an external outgoing CO route and the RANX feature is configured for this route, the calling party that is forwarded due to the Phantom TN feature will be provided with a recorded announcement.

Expensive Route Warning Tone

If the calling party is being forwarded to a route with the RANX feature and the Expensive Route Warning Tone feature configured, the Expensive Route Warning Tone will be heard prior to the recorded announcement.

Feature packaging

This feature requires the following packages:

- Recorded Announcement (RAN) package 7
- Intercept Treatment (INTR) package 11

Note:
The use of this feature is not recommended if the outgoing external Central Office (CO) route is not configured with answer supervision.

Feature implementation

Table 177: LD 16: Configure Recorded Announcement for Calls Diverted to External Trunks in the Route Data Block.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
DLDN	YES	YES if no CPG configured.
...		
FORM	aaa	Signaling format.
ICOG	IAO	Incoming and/or outgoing trunk.
RANX	(NO) YES	(RAN not requested when a call is forwarded to this route), RAN is requested when a call is forwarded to this route.
RANR		RAN route number for "Authcode Last" prompt (NAUT)
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 42: Redirecting Name Display Enhancement for QSIG Call Rerouting

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Dialed Name Display Allowed and Dialed Name Display Denied (DNDA/DNDD) functionality is now supported for Call Rerouting when both the originating and the diverted-to user are on the same node.

Call Diversion notification provides, for QSIG generic functional protocol (GF) interfaces, the capability of displaying the diverted-to user's calling line identification (CLID) on the calling user's phone when the diverted-to user's phone is rung during QSIG call diversion.

When both the originating and the diverted-to user are on the same system node and call diversion is performed by the Rerouting method, the originating user's subscription options have no impact on the diverted-to user's notification. If the diverted-to user has Class of Service DNDA, then the diverted-to phone displays the redirecting name.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

The Redirecting Name Display Enhancement for QSIG Call Rerouting feature does not introduce any new packages.

This feature requires the following packages:

- Call Party Name Display (CPND) package 95
- Integrated Services Digital Network (ISDN) package 145
- 2 Mbit/s Primary Rate Interface (PRI2) package 154
- International Primary Rate Access (IPRA) package 202
- Basic Rate Interface (BRI) package 216
- Multi-purpose Serial Data Link (MSDL) package 222
- ISDN BRI Trunk Access (BRIT) package 233
- BRI Line Application (BRIL) package 235
- Q Reference Signalling Point Interface (QSIG) package 263
- QSIG Generic Functional protocol (QsigGF) package 305
- QSIG Supplementary Service (QSIG-SS) package 316

Feature implementation

There are no specific implementation procedures for this feature.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 43: Reference Clock Switching

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

Reference Clock Switching allows a Clock Controller reference to automatically switch to another tracking reference if the reference goes into a non-acceptable state (the Clock

Controller can track on its primary reference, secondary reference, or be in free run). Non-acceptable states are the following:

- The reference loop is disabled
- For PRI2, one of the following group 2 errors is detected on the reference loop:
    - Far end is in out-of-service state
    - Far end has lost Multiframe Alignment Signal
    - Alarm Indication Signal is sent
    - Loss of Frame Alignment
    - Loss of Multiframe Alignment
- For DTI2, if the reference loop is in out-of-service grade of service, or if the reference loop is in No New Call state (if the OOS is inhibited)

Clock Tracking Recovery

If a repeating device loses the signal, it immediately begins sending an unframed all 1's signal to the far-end to indicate an alarm condition. This condition is called a Blue Alarm, or an Alarm Indication Signal (AIS). On Meridian 1 PBX 11C Chassis and Meridian 1 PBX 11C Cabinet systems an Alarm Indication Signal (AIS) on PRI loops puts the reference loop in an unacceptable state. Reference Clock Switching in such a case is implemented using the CTRR (Clock Tracking Recovery) prompt in the Digital Data Block (DDB) in LD 73. The response to the CTRR prompt can be YES or NO. (The default is NO.)

The CTRR option is prompted only for Meridian 1 PBX 11C Chassis and Meridian 1 PBX 11C Cabinet systems and only if at least one of CC0, CC2, CC3, or CC4 is configured.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature requires the following packages:

International Supplementary Features (SUPP) package 131 and one or both of:

- 2.0 Mbit Digital Trunk Interface (DTI2) package 129
- 2.0 Mbit Primary Rate Interface (PRI2) package 154

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 178: LD 73: Define the Grade of Service timers for the DTI card. on page 377
2. Table 179: LD 73: Enable Clock Tracking Recovery on page 378

LD 60: Enable automatic switch over of system clock sources on the Clock Controller by using the EREF command.

Table 178: LD 73: Define the Grade of Service timers for the DTI card.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	DTI2	2.0 Mbit Digital Trunk Interface.
	PRI2	2.0 Mbit Primary Rate Interface.
	JDMI	Japan Digital Multiplex data block.
FEAT	SYTI	System Timers.
...		
CCGD	0-(15)-1440	Clock Controller free run Guard time.
CCAR	0-(15)	Clock Controller Audit Rate.
EFCS	YES	Enable Fast Clock Switching.

Table 179: LD 73: Enable Clock Tracking Recovery

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	DDB	Digital Data Block.
...		
SREF		
CTRR	(NO) YES	Clock tracking recovery in case of Blue Alarm on reference loops.
TRSH		
....		

Feature operation

No specific operating procedures are required to use this feature.

Chapter 44: Remote Virtual Queuing

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Remote Virtual Queuing (RVQ) allows a system to perform queuing- type functions on a busy trunk route (B-Channel) in an ISDN network. This feature is similar to the ESN features Coordinated Call Back Queuing (CCBQ) and Call Back Queuing to a Conventional Main (CBQCM). Prior to operating RVQ, you must have a working knowledge of the ESN features.

Remote Virtual Queuing (RVQ) is supported on a private ISDN PRI/ISL network only.

When an outgoing network path is unavailable, Remote Virtual Queuing (RVQ) provides call back queuing. RVQ repeatedly scans ahead on the ISDN trunk to be sure that the entire path, from origination to termination, is available. When a path becomes idle, you are notified and can ring the path again to terminate the call.

Operating parameters

In addition to the function offered by CCBQ and CBQCM, RVQ provides the following:

- There is no limit to the number of nodes in the ISDN network that RVQ searches.
- The originating node has control of the call.
- Data terminals are supported.
- Attendants cannot activate RVQ.
- RVQ is activated only by phones with Ring Again allowed.
- AUTHCODE is supported on the first tandem node only.
- Trunk Access Codes are not supported.
- ACD DNs are supported as a terminating DN.
- Attendants are supported as terminating stations.

RVQ is supported in a private ISDN PRI/ISL network only. Any trunk other than an ISDN PRI or ISL trunk is considered a Non-RVQ Compatible (NRC) trunk. NRC trunks include analog trunks, T1 trunks, or public trunks. NRC also includes trunks connecting to a non-system, or non-ISDN.

Meridian Modular, analog (500/2500-type) and Meridian digital phones can activate and receive RVQ calls.

The RVQ retry timer is set for each NCOS. Setting a specific NCOS with a low retry timer searches for more connections more often. The lower the timer, the greater the chance to connect the call.

The maximum total amount of time RVQ searches for available paths is 30 minutes. The countdown begins as soon as the originator activates the Ring Again key.

Only one RVQ Ring Again attempt for each phone is allowed at one time. If Ring Again is pressed again, after activating it for RVQ, the most recent number dialed is the one attempted.

RVQ does not check the terminating phone's status. The dialed DN can be invalid or busy. Once the path is available, the RVQ call can reach the dialed DN. It is possible that the dialed phone is busy, and Network Ring Again can be used if enabled. The tone indicating that the trunks are busy is a fast busy tone. A busy DN is indicated by a standard busy tone.

RVQ searches throughout system networks only. Off-net trunk paths cannot be checked beyond the first NRC trunk.

RVQ is a virtual queuing feature. Each RVQ call is independent of another. It does not operate by first in first out policy. The first caller to initiate RVQ is not necessarily the first person connected.

It can take up to 30 seconds for notification to reach the originator. The network path is reserved while RVQ notifies the caller. In a private network, the path is reserved from the originating node to the terminating node. Otherwise the path is reserved up to the first NRC trunk.

RVQ supports Uniform Dialing Plan (UDP) and Coordinated Dialing Plan (CDP). For NRC trunks, the E.164 public numbering plan is supported.

RVQ supports the following trunk types:

Private network ISDN trunks

- TIE
- COT
- Direct Outgoing Dial (DOD)
- WATS
- ISA
- FEX

RVQ supports only system machines in a private ISDN PRI/ISL network. A non-system machine functioning in tandem with a system machine is treated as a Non-RVQ Compatible (NRC) trunk.

NRC trunks

- COT
- Direct Outgoing Dial (DOD)
- WATS
- FEX
- ISA
- TIE

RVQ is cancelled if the originating node system initializes.

If the originating node performs a cold start, RVQ is cancelled.

RVQ from a Conventional Main (RVQCM) requires a special configuration. See the "Feature administration" section in this module.

With RVQ, callers cannot activate Ring Again to refuse expensive routes after the Expensive Route Warning Tone (ERWT) is given.

When using RVQ from a Conventional Main (RVQCM), the originating node seizes the same TIE trunk group that was used to initiate RVQCM for the callback. Thus, these trunk groups must be two-way (incoming/outgoing) and configured for far end disconnect.

Conventional mains must provide answer supervision on TIE trunks connected to the originating node. The system must also permit transmission or repetition of phone dial pulses for RVQCM operation. This feature cannot be used with systems that operate in senderized mode. Operation can require adjustment of the interdigit timeout on systems that employ simulated cut-through operation.

Multiple callback queues are allowed for each trunk group for the Conventional main by dialing any digits (up to 7) based on the availability of system call registers.

When utilizing RVQCM, do not call forward the calling phone when awaiting callback. If the phone is forwarded, it is possible that the TIE trunk will not be released at the end of the call.

Feature interactions

Drop Back Busy

Drop Back Busy (DBB) and Remote Virtual Queuing (RVQ) are both packaged under the Originating Routing Control/Remote Virtual Queuing (ORC-RVQ) package 192. If RVQ and DBB are both configured, DBB will take precedence over RVQ. If the user wishes to activate RVQ, DBB must be disabled for a route entry in response to the IDBB prompt. If the user wishes to activate DBB, it must be enabled by entering DBI or DBA. Refer to the "Feature administration" section for more information.

Coordinated Call Back Queuing

CCBQ and RVQ can both be enabled on a single machine.

Call Back Queuing to a Conventional Main

CBQCM and RVQ can both be enabled on a single machine.

Call Page Network Wide

RVQ is supported for an incoming call to a Paging trunk when all the trunk members of the dialed Paging route are busy.

Direct Inward System Access

DISA DNs are not supported by RVQ.

ISDN QSIG Basic Call

Remote Virtual Queuing (RVQ) does not operate on the QSIG interface. The existing RVQ operation on unsupported interface applies on the QSIG interface.

Make Set Busy

RVQ can be originated by, and terminated on, an ACD DN in Make Set Busy Mode.

Network ACD

If a target agent is available on a Remote node, RVQ cannot be activated if the busy trunk is found on its way to the target node.

Network Call Redirection

RVQ does not guarantee connection if the terminating phone call forwards to a phone on another node. When a terminating phone call forwards to another node, that node is a redirected node. RVQ cannot search between terminating and redirected nodes.

Network Ring Again

Network Ring Again (NRAG) is activated only when the terminating phone or console is busy. If both the network path and the terminating phone are busy, RVQ is activated first. When the path is available, but the phone is busy, NRAG can be activated.

Off -Hook Queuing

RVQ and Off- Hook Queuing (OHQ) are compatible in a system. If OHQ is configured, it is implemented by leaving the handset off -hook. RVQ is implemented by pressing the Ring Again key. Choosing one or the other method activates the specified feature.

Feature packaging

This feature requires the following packages:

- Main Network Queuing package 38
- Flexible Call Back Queuing package 61
- Digital Trunk Interface package 75
- ISDN signaling package 145
- ISDN PRI package 146 or ISL package 147 or 2.0 Mbit Primary Rate Access (PRI2) package 154
- Advanced Network Services package 148 (for NRAG capability)
- ISDN Supplementary (ISDNS) package 161
- Originating Routing Control/Remote Virtual Queuing (ORC-RVQ) package 192

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

Table 180: LD 86: Configure the originating node for Remote Virtual Queuing.

Prompt	Response	Description
REQ	CHG	Change existing data.
CUST		Customer number

Prompt	Response	Description
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	RLB	Route List Data Block.
RLI	nn	Route List Index.
ENTR	nn	Route List entry number.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...	...	...
IDBB	(DBD)	Enter DBD (Drop Back Busy Disabled). This will disable Drop Back Busy, and enable Remote Virtual Queuing for the customer.
	DBI DBA	Drop Back if Initial set is busy. Drop Back if all routes are busy.

Table 181: LD 87: Configure the originating nodes for CBQ.

Prompt	Response	Description
REQ	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	NCTL	Network Control.
...		
SCBQ	YES	Allow system Call Back Queuing for the customer.
NCOS	nn	Network Class of Service number. The originating set must have the same value.
...		
CBQ	(NO) YES	Call Back Queuing is allowed for this NCOS.
RETT	2-(10)-30	Remote Virtual Queuing Retry Timer (Time between searches, in seconds).
RETC	4-(5)-16	Remote Virtual Queuing Retry Counter (Number of times RVQ searches the Initial set before moving on to the Extended set).

Table 182: LD 86: Configure the outgoing routes of the originating nodes for CBQ at least one entry of the Initial set of the outgoing route must allow CBQ.

Prompt	Response	Description
REQ	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
FEAT	RLB	Route List Data Block.
RLI	nn	Route List Index.
ENTR	nn	Route List entry number.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
CBQ	YES	Allow CBQ.
...		
ENTR	<CR>	
ISET	nn	Size of the Initial set.

Table 183: LD 16: Allow CBQ for the incoming non-ISDN routes on the originating nodes (for RVQ at a conventional Main operation).

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System, Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System, Media Gateway 1000B, and CS 1000E system.
...		
CBQ	YES	Allow Call Back Queuing.
...		

Feature operation

RVQ supports private ISDN PRI/ISL networks, non-RVQ compatible (NRC) blocked trunks, and conventional mains (RVQCM). RVQ supports system machines only. A non-system machine working in tandem with a system is treated as a Non-RVQ Compatible (NRC) trunk.

RVQ on a private network

RVQ follows this checklist before starting.

- The first tandem node must be a system node.
- The originating node's Network Class of Service (NCOS) must allow Call Back Queuing (CBQ).
- At least one route in the Initial set of the route list must allow CBQ.
- The system has CBQ allowed at the Network Control Block.

When the checks are complete, activate RVQ by pressing the Ring Again key. As soon as the key is pressed, the retry timer begins. When the retry timer expires, RVQ checks the path again. When a blocked path occurs, RVQ searches the network to ensure that the entire path will be clear once the blockage disappears. The total amount of time RVQ will spend on a search is 30 minutes.

The retry counter controls the number of times the Initial set is checked before RVQ searches the extended set. The extended set search includes all of the trunks in both the Initial and Extended sets.

Tandem nodes must recognize the RVQ messages and pass them on to another tandem or terminating node.

RVQ with NRC trunks

RVQ searches the path until it reaches the firstNon-RVQ Compatible (NRC) trunk. RVQ notifies the originator when that trunk is available, but cannot search beyond it. It is possible that the path can be blocked beyond the NRC trunk, and the call cannot go through.

Any trunk other than an ISDN PRI or ISL trunk is considered an NRC trunk. NRC trunks include analog, T1, or public trunks, as well as trunks connecting to a non-system, or non-ISDN node.

When an NRC trunk is busy, RVQ follows this checklist before implementing RVQ.

- First tandem node must be a system node.
- Originating node's NCOS must allow Call Back Queuing (CBQ).
- At least one route in the initial set of the route list must allow CBQ.
- The system has CBQ allowed at the Network Control Block.

When the checks are complete, activate RVQ by pressing the Ring Again key. As soon as the key is pressed, the retry timer begins. When the retry timer expires, RVQ checks the path again. The total amount of time RVQ will spend on a search is 30 minutes.

The retry counter controls the number of times the Initial set is checked before RVQ searches the Extended set. The extended set search includes all the trunks in both the Initial and Extended sets. Only the first NRC trunk is checked. RVQ cannot search beyond that trunk, even if the subsequent trunks are ISDN PRI/ISL.

RVQ on a conventional main (RVQCM)

A conventional main call is one that comes from a third-party system into the private network through a TIE trunk to a system node.

When the conventional main call enters the network, the default NCOS is assigned to the TIE trunk to determine RVQCM eligibility. Use Authcode last to upgrade the NCOS if necessary.

When a conventional main call is blocked, RVQ checks the following at the first system node to ensure RVQCM can be activated. The system node is considered the Originating node, and controls the call.

- The tandem and terminating nodes must be system nodes.
- The originating node's Network Class of Service (NCOS) must allow Call Back Queuing (CBQ).
- At least one route in the Initial set of the route list must allow CBQ.
- The system has CBQ allowed at the Network Control Block.
- The incoming TIE trunk allows CBQ.

RVQCM is offered to the conventional main caller with a special offer tone (3 beeps). To accept RVQ, enter the calling number. After the same special confirmation tone (3 beeps) is heard, hang up. The originating node begins the retry timer and search process. When the retry timer expires, RVQ checks the path again. The maximum total amount of time RVQ will spend on a search is 30 minutes. When the path is free, the originating node calls the caller back (at the number entered). The phone rings, the same special callback tone (3 beeps) is heard, and the call is connected. RVQCM cannot be cancelled from the conventional main once started.

If the calling phone is busy, or does not answer the callback, the RVQ callback is placed in a 5 minute suspense state. After 5 minutes have passed, RVQ attempts the callback again. If the calling phone is still busy, or does not answer, RVQ is cancelled.

The retry counter controls the number of times the Initial set is checked before RVQ searches the Extended set. The Extended set search includes all the trunks in both the Initial and Extended sets.

Note:

The calling number is accepted only if the database has been configured to accept the given number of digits. If not, or if the caller does not hang up, an overflow tone is given, and the call is disconnected. RVQCM does not verify that the dialed DN is valid or free.

Once started, RVQ cannot be cancelled from the convention main. Operating parameters relating to Call Back Queuing for Conventional Mains (CBQCM) also apply to RVQCM as follows.

Users at Conventional Mains cannot activate Ring Again to refuse expensive routes after the Expensive Route Warning Tone (ERWT) is given.

The node seizes the same TIE trunk group that was used to initiate RVQCM for the callback. These trunk groups must be two way (incoming/outgoing).

Conventional Mains must provide answer supervision on TIE trunks connected to the node. These switches must also permit transmission, or repetition of phone dial pulses, for RVQCM operation. This feature cannot be used with systems that operate in senderized mode. Operation can require adjustment of the interdigit timeout on systems that employ simulated cut-through operation.

Multiple callback queues are allowed for each trunk group for the Conventional Main by dialing up to 7 digits (any digits are allowed) based on the availability of system call registers.

Important:

Conventional Mains must not allow RVQCM callback calls to be modified by call transfer or call forward to an outside line. These Call modifications can result in the TIE trunk not being released at the end of the call.

Chapter 45: Ring Again on No Answer

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

This feature extends the capabilities of Network Ring Again for ISDN applications.

When the called station goes off-hook and then on-hook, the activating station is rung back in the same way that traditional Ring Again on Busy operates. Ring Again on Busy gives a caller the opportunity, after encountering a busy Directory Number (DN), to ring the DN again when it becomes free. If a dialed DN is busy, or if all the trunks are busy, pressing the Ring Again key asks the system to monitor the dialed DN or trunk. When it becomes available, the system notifies the caller. The call is automatically dialed again when the caller presses the Ring Again key a second time.

Ring Again on No Answer is applied to the originally dialed DN only.

Operating parameters

Ring Again on No Answer cannot be applied:

- if the dialed DN is a Pilot DN
- to Attendant Consoles
- to a station which has been intercepted to the attendant
- to a station which is queued for an attendant
- to a station which has been recalled to an attendant due to misoperation
- to Automatic Call Distribution (ACD) stations
- to a station with Radio Paging active
- to trunks

Meridian digital telephones must be equipped with a Ring Again (RGA) key/lamp combination.

Ring Again on No Answer is applied to the originally dialed DN only.

Feature interactions

Call Forward (All Calls)

Call Forward No Answer

Automatic Call Forward

If an unanswered call is forwarded to another station by any of these features, RANA is applied to the originally dialed station.

Hunt

If RANA has been applied to a station going through a Hunt sequence, Ring Again is applied to that station and not the ringing station.

ISDN QSIG/EuroISDN Call Completion

Analog (500/2500 type) phones can have only one Call Completion to Busy Subscriber request at a given time. Meridian 1 Proprietary Phones can make Ring Again requests based on the number of Ring Again keys programmed on a phone.

Feature packaging

This feature requires the following package:

Advanced ISDN Network Services (NTWK) package 148.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 184: LD 15: Allow or deny Ring Again on No Answer operation. on page 393
2. Table 185: LD 11: Define RGA keys against M2317 phones. on page 394

Table 184: LD 15: Allow or deny Ring Again on No Answer operation.

Prompt	Response	Description
REQ	CHG	Change
TYPE	FTR	Features and options data.
CUST		Customer number
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.

Prompt	Response	Description
...		
OPT	(RND) RNA	Ring Again No Answer (Denied) Allowed.

Table 185: LD 11: Define RGA keys against M2317 phones.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	aaaa	Type of phone.
TN		Terminal number
	l s c u	Format for Large System , Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
...		
KEY	xx RGA	Key number, Ring Again Must be key 10 on LOGIVOX phones. RANA can be activated if OPT = RNA in LD 15. When OPT = RND in LD 15, all phones with the RGA key will only be able to activate Ring Again Busy.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 46: SDID Number as CLID for EuroISDN Trunks

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

The following is a description of the SDID number as CLID for EuroISDN Trunks feature. SDID capability is available for EuroISDN calls that have CLID OPT1 enabled. For BRIE interfaces, the OPT1 option is configured at the CLID prompt in LD 16. For PRI2 interfaces, the OPT1 option is configured at the CLID prompt in LD 17.

The Send DID Number (SDID) feature sends the Direct Inward Dial (DID) number of a specific DN as Calling Line Identification (CLID) on an outgoing trunk call. SDID replaces the internal

DN of the phone with the DID (external DN) of the phone. The DID number is obtained from the Incoming Digit Conversion (IDC) table.

The IDC table converts the following:

- the internal DN of the phone to the external DN of the phone
- the external DN of the phone to the internal DN of the phone

Table 186: Example of an IDC table

Incoming Digits (IDGT)	Converted Digits (CDGT)
4322 (external DN)	726 (internal DN)
8741 (external DN)	12 (internal DN)

Phone A with an internal DN of 726 calls Phone B. The IDC table converts Phone A's internal DN 726 to its external DN 4322. The CLID of Phone A is sent to Phone B as 4322. If the internal DN is not entered in the IDC table, the internal DN is sent as the CLID.

Phone C calls Phone D by dialing Phone D's external DN 8741. The IDC table converts Phone D's external DN 8741 (external DN) to its internal DN 12. Phone D's external DN is sent to Phone C as the Connected Number (CONN).

Type Of Number of Calling Party Number

The SDID feature allows the Type of Number (TON) of the calling party number to be changed in the Route Data Block (RDB). The TON is changed when the calling party number has an ISDN numbering plan.

Connected Number Identification

The SDID DN (the external DN) is sent to the CO as the Connected Number for an incoming call.

Operating parameters

This feature is only available on EuroISDN routes.

The EuroISDN route must have an IDC table associated with it when SDID is enabled.

This feature replaces the internal DN with the DID DN for the following:

- analog (500/250- type) phones
- Meridian Digital phones

- Basic Rate Interface (BRI) Line phones
- Attendant Consoles

This feature does not apply to trunks as the originator.

Feature interactions

Automatic Call Distribution

The SDID number as CLID for EuroISDN trunks feature is not applicable to Automatic Call Distribution (ACD), as calls cannot originate from an ACD key.

If the ACD phone is equipped with an active Single Call Ringing (SCR) key, the DN is obtained from the active key. If the DN has been entered in the IDC table, the external DID number is used. See "ISDN Calling Line Identification Enhancement".

Business Network Express

Even though the CLID is changed to the SDID DN, the private CLID or name is not changed.

Call Detail Recording

Call Detail Recording (CDR) is not affected by the SDID feature. The record's Originating ID (ORIGID) and Terminating ID (TERID) remain as the internal DN.

Call Forward

If a forwarding DN on a EuroISDN trunk is used as CLID and is found in the IDC table, the SDID DN is sent as the CLID.

Calling Party Privacy

The Calling Party Privacy (CPP) feature is not affected by SDID.

Direct Inward System Access

Direct Inward System Access (DISA) numbers are not affected by the SDID feature.

EuroISDN Trunk: Network Side

The SDID number as CLID feature is supported on the network side of the EuroISDN trunk.

Feature packaging

This feature requires the following packages:

- Incoming Digit Conversion (IDC) package 113
- International Supplementary Features (SUPP) package 131
- Integrated Services Digital Network (ISDN) package 145

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 187: LD 49: Define the IDC table. on page 398
2. Table 188: LD 16: Define the Route Data Block (RDB) for ISDN trunks. on page 399

Table 187: LD 49: Define the IDC table.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	IDC	Incoming Digit Conversion.
CUST		Customer number

Prompt	Response	Description
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
DCNO	0 – 254	Day IDC tree number.
FDID		Flexible DID.
	(NO) YES	
SDID		Send DID number instead of internal DN.
	(NO) YES	
IDGT	xxxx xxxx	Incoming Digit or range of digits where: xxxx = 0 – 9999.
xxxx	yyyy	Converted Digits (CDGT).
IDGT	xxxx xxxx	Incoming Digit or range of Digits where: xxxx = 0 – 9999.
xxxx	yyyy	Converted digits (CDGT).

Table 188: LD 16: Define the Route Data Block (RDB) for ISDN trunks.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Type of data block = RDB (route data block).
ROUT		Route number
	0-511	Range for Large System , Media Gateway 1000B, and CS 1000E system.
....	....	
ISDN	(NO) YES	Integrated Services Digital Network option.
....	....	
- SDID	YES	Send DID number instead of internal DN. (NO) = default.
-- CTON	(NCHG) UKWN INTL NATL LOCL	Call Type of Number. Call Type is not changed. Unknown Call Type. International Call Type. National Call Type. Subscriber Call Type.
....	....	
IDC	YES	Incoming DID Digit Conversion on this route.
- DCNO	xx	Day IDC tree number where: xx = (0) – 254.
- NDNO	xx	Night IDC tree number where: xx = 0 – 254.

Feature operation

No specific operating procedures are required to use this procedure.

Chapter 47: Singapore ISDN Restart Message Enhancement

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Singapore ISDN Restart Message Enhancement allows systems with Asia Pacific-Singapore ISDN connectivity to recognize and process Restart Acknowledge messages sent from an Alternate Carrier's Nokia Central Office (CO) switch.

Note:

The Alternate Carrier's Nokia CO must be located in Singapore.

With the Singapore ISDN Restart Message Enhancement, the system accepts an Indicated Channels Restart Acknowledge message from the CO. The acknowledge message from the CO is in response to the Single Interface Restart Message.

Restart messaging sequence for the Singapore ISDN Restart Message Enhancement shows the Restart messaging sequence between a system and a Nokia CO switch over the Asia-Pacific Singapore ISDN interface.

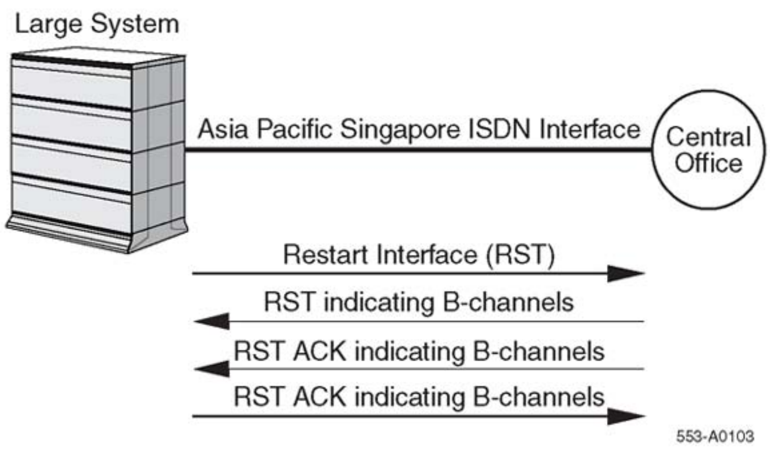

Figure 56: Restart messaging sequence for the Singapore ISDN Restart Message Enhancement

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

There are no new packages associated with this feature.

Feature implementation

There are no specific implementation procedures associated with this feature.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 48: Software Defined Network Access

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Applicable regions

The information presented in this section does not pertain to all regions. Contact your system supplier or your Avaya representative to verify support of this product in your area.

Feature description

AT&T's Software Defined Network (SDN) provides the equivalent of a private network. The network is controlled by customized call-processing specifications stored in the AT&T network, rather than at customer sites. To access SDN, the customer uses access lines from their location to the AT&T network.

SDN can transmit voice, data, or graphics. Analog transmission to 9600 bit/s and 56 Kbit/s or 64 Kbit/s clear end-to-end digital data transmission are supported.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature is included in base System Software.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 189: LD 17: Configure the AT and T interface type. on page 406
2. Table 190: LD 16: Configure a TIE route. Routes defined for access to AT and T services, such as SDN, must be TIE trunk routes. on page 407

Table 189: LD 17: Configure the AT and T interface type.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	CFN	Configuration Record
ADAN	NEW DCH xx	Add a primary D-channel
CTYP	DCHI MSDL	Card type

Prompt	Response	Description
DNUM	xx	Device number: physical port (odd) for D-channel on DCH, physical card address for MSDL or DDCH.
- PORT	xx	Port number on MSDL or card
USR	PRI ISLD SHA	D-channel mode
PRI	xxx yy	Additional PRI loops using the same D-channel, and interface ID
IFC	ESS4 ESS5	AT&T 4ESS or 5ESS

Table 190: LD 16: Configure a TIE route. Routes defined for access to AT and T services, such as SDN, must be TIE trunk routes.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route data block
CUST		Customer number
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System , Media Gateway 1000B, and CS 1000E system.
TKTP	TIE	TIE trunk route
ISDN	YES	Integrated Services Digital Network
- IFC	ESS4 ESS5	AT&T 4ESS or 5ESS
- SRVC	SDN	Software Defined Network

Feature operation

No specific operating procedures are required to use this feature.

Chapter 49: Software Release ID

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Software Release ID uses the D-channel connection of your switch to identify the software release of an adjoining switch. This feature identifies the software release of the NRAG, NACD, NMS, and NCRD features. The software release ID can be requested for all direct connections to the system. However, the Software Release ID cannot be obtained for switches in a tandem configuration. The information provided by the Software Release ID depends on the interfacing switches. That is, a system switch provides a release number and a DMS-100 switch provides a BCS number.

Note:

If the interface is changed, the release ID is also changed. The release ID must then be reconfigured.

This feature prevents software incompatibility between two switches. Different applications are supported by different releases, and for most of the ISDN applications, operations are invoked by sending messages back and forth. To prevent software incompatibility, the following occurs. The release ID of the connecting D-channel is checked before data is sent through the ISDN interface. If the connecting switch does not have the software to handle the feature requested, an application message is not sent. Instead, an error message is printed.

Note:
The release ID information is required and supported for connection to Avaya equipment only.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature is included in base System Software.

Feature implementation

Table 191: LD 17: Configure the Software Release ID feature.

Prompt	Response	Description
REQ	CHG	Change
TYPE	CFN	Configuration Record
ADAN	NEW DCH xx	Add a primary D-channel
CTYP	DCHI MSDL	Card type
DNUM	xx	Device number: physical port (odd) for D-channel on DCH, physical card address for MSDL or DDCH.
- PORT	xx	Port number on MSDL or card
RLS	xx	Release ID of the switch at the far end of the D-channel.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 50: Trunk Route Optimization

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Trunk Anti-Tromboning (TAT), Trunk Route Optimization-Before Answer (TRO-BA), and Trunk Route Optimization-Call Modification (TRO-CM) features work together in a Meridian Customer Defined Network (MCDN) to optimize trunk connections.

For maximum benefit, configure TAT, TRO-BA, and TRO-CM on all nodes in the MCDN.

These features apply to the following:

- IP Peer Virtual Trunks
- IP trunks
- Virtual Network Services (VNS) trunks
- ISDN Signaling Link (ISL) trunks
- Basic Rate Interface (BRI) and Primary Rate Interface (PRI) trunks

TAT, TRO-BA, and TRO-CM provide the following benefits:

- Optimize trunk resources to reduce operating costs for customers in Time Division Multiplexing (TDM) and hybrid networks (IP Trunk and IP Peer Networks).
- Reduce the number of physical Central Office trunks, TIE trunks, IP trunk resources, Virtual Trunks, and Voice Gateway channels.
- Eliminate most of the voice quality degradation associated with multiple tandem IP telephony voice paths, which results from network call transfers in hybrid networks.
- Eliminate redundant tandem Virtual Trunk resources and Voice Gateway resources in an IP Peer network.
- Minimize service interruptions by eliminating unnecessary points of failure in the tandem nodes of established calls.

Configuring TRO-BA, TRO-CM, and TAT

Configure TRO-BA and TRO-CM by setting TRO = YES in the Route Data Block. Configure TAT by setting RCAP = TAT in the D-Channel data block.

Automatic call redirections and user-initiated call modifications in an MCDN require the correct configuration and operation of the TRO and TAT features at all Call Server nodes in order to optimize the route between the connected callers. TRO-BA and TRO-CM depend on the correct implementation of UPD and CDP at all CS 1000nodes and NRS-collaborated servers.

TAT interoperability with IP Trunk 3.01 requires CSE remote node capability. Otherwise, TAT depends on the called number of the first leg of the call matching the calling number of the second leg of the call; this restriction severely inhibits TAT.

TAT interoperability with BCM 3.5 is subject to called/calling number matching on the first and second legs of tromboning. The upcoming BCM release will remove this restriction.

See Feature implementation on page 474.

Trunk Route Optimization-Before Answer

TRO-BA enhances routing on PRI and ISL routes for redirected calls (for example, calls redirected by Call Forward All Calls, Call Forward Busy, Call Forward No Answer, and Hunt). TRO-BA occurs when a direct call is made from the originating station to the redirected station, on Meridian 1 or CS 1000Msystems.

Note:

TRO-BA does not optimize trunks for calls that have undergone a call modification (for example, calls that have been transferred or conferenced).

TRO-BA requires Network Call Redirection to be configured on the system.

TRO-BA applies to the following call redirections:

- Network Call Forward All Calls (NCFAC)
- Network Call Forward No Answer (NCFNA)
- Network Hunt (NHNT)

Example of TRO-BA when NCRD is enabled on each node shows an example of TRO-BA when the NCRD feature is enabled on each node.

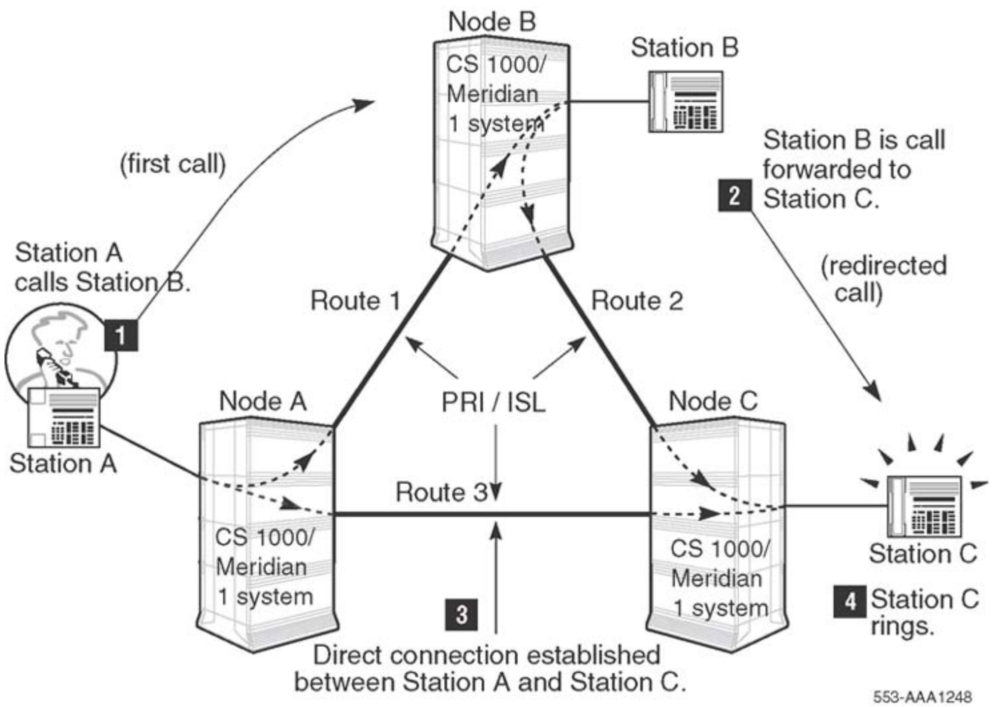

Figure 57: Example of TRO-BA when NCRD is enabled on each node

Figure 57: Example of TRO-BA when NCRD is enabled on each node on page 415 illustrates the following:

- Station A calls remote Station B over PRI/ISL Route 1.
- Due to NCFAC, NCFNA, or NHNT, the call is forwarded to Station C over Route 2.
- When TRO-BA is enabled at Node B, facility messages are sent from the redirecting Node B to the originating Node A with the following redirection information:
    - redirection number
    - reason
    - counter
- The system returns a facility message accepting TRO-BA, if the following conditions are met:
    - Node A has TRO-BA enabled.

- Node A has a first choice RLB entry route member available.

- The redirection counter does not exceed the limit.

If the originating node does not support TRO, the node sends a message rejecting TRO-BA, and the call proceeds on the current route. The redirecting node then cancels TRO-BA routing.

- The redirecting node sends a message to release the connection.
- The originating node sends a message confirming that the original connection (1) is dropped.
- The originating node sets up a direct connection to Station C over Route 3.
- Routes 1 and 2 are available for new calls.

Example 2 of TRO-BA when NCRD is enabled on each node shows another example of TRO-BA when the NCRD feature is enabled on each node.

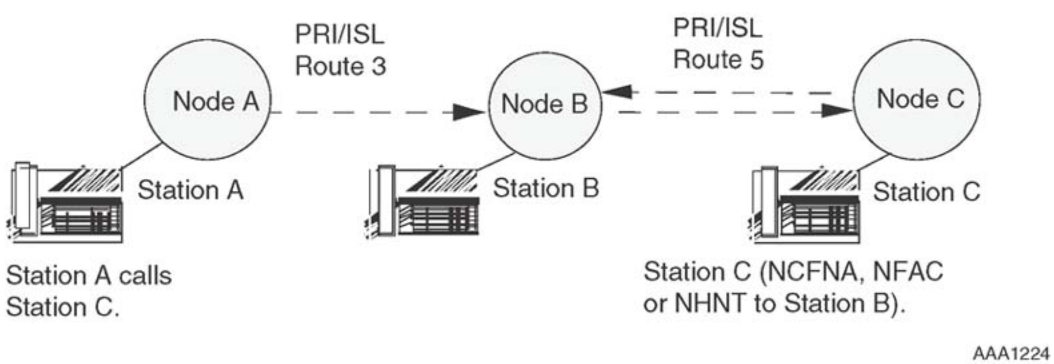

Figure 58: Example 2 of TRO-BA when NCRD is enabled on each node

Figure 58: Example 2 of TRO-BA when NCRD is enabled on each node on page 416 illustrates the following:

- The originating Station A calls remote Station C over PRI/ISL routes 3 and 5.
- Due to NCFAC, NCFNA, or NHNT, the call forwards to Station B over PRI/ISL route 5.
- When Node A accepts the TRO-BA request, Node A establishes a direct connection to Node B over route 3.
- TRO-BA clears both connections over route 5. Route 5 trunks are now available for other calls.

Trunk Anti-Tromboning

TAT optimizes tromboned trunks for calls that are redirected or modified after answer. Tromboning occurs when a call goes to another node and is transferred back on a second trunk, tying up two trunks (for example, call forward or call transfer).

TAT optimizes tromboned trunks under the following conditions:

- The trunks are associated with the same primary channel.
- Both trunks belong to the same customer.

Note:
TAT also applies to calls entering a system network over a Central Office (CO) trunk. TAT eliminates the tromboning of private network trunks that can occur if the call is redirected or modified.

Example of a trunk anti-tromboning operation

The following example is a demonstration of TAT working in a simple system-to-system interworking. Refer to Anti-Tromboning scenarios for other interworking scenarios.

Figure 59: Prior to Trunk Anti-Tromboning operation on page 418 illustrates the following:

- Station B, (at the terminating node), receives an incoming call over a PRI trunk from Station A, (at the originating node), or an incoming CO call is tandemed from the originating node to the terminating node.
- Station B answers the call and transfers it to Station C, which resides at the originating node. A second PRI trunk is established to handle the new call.
- Station B completes the call transfer, which leaves Station A connected to Station C (which is in a ringing state) by using the two PRI trunks. The PRI trunks remain tromboned until Station C answers the call.

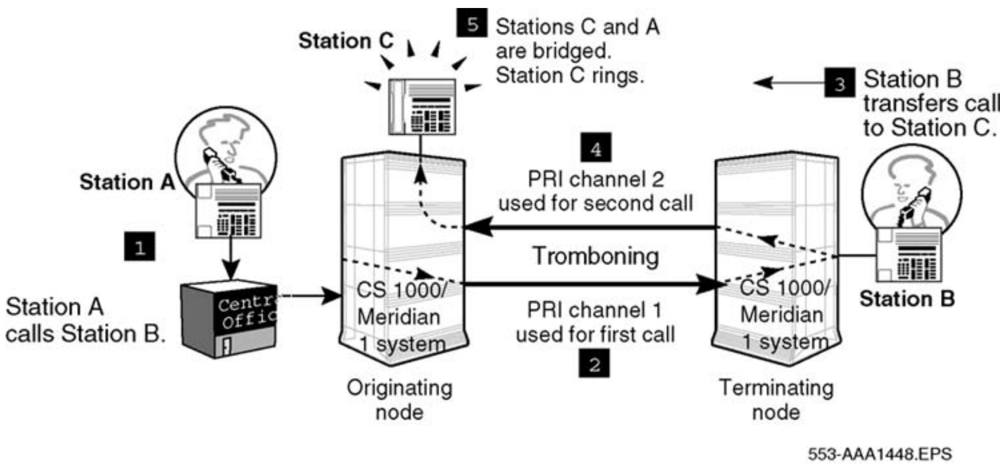

Figure 59: Prior to Trunk Anti-Tromboning operation

Figure 60: After Trunk Anti-Tromboning operation on page 418 illustrates how the TAT application eliminates the redundant ISDN PRI B-channels forming the loop-back. After Station C answers the call, the originating node bridges Station A and Station C. If the trunks involved are associated with the same primary D-channel and the same customer, TAT releases the redundant trunks. The TAT operation eliminates the use of extra network trunking facilities for the duration of the call.

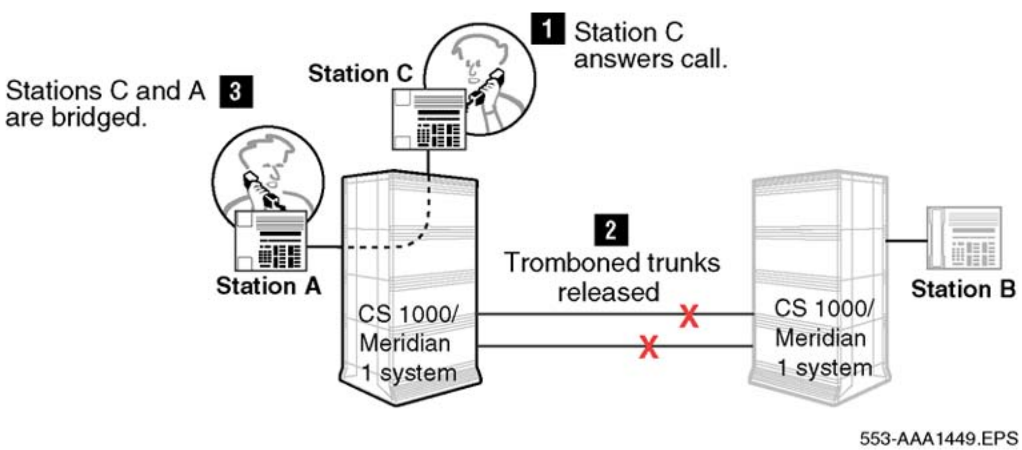

Figure 60: After Trunk Anti-Tromboning operation

Note:

If the originating or terminating node does not support the TAT feature, or the originating node is unable to bridge the call between Station A and Station C, then Station A and Station C remain connected for the duration of the call through the tromboned trunks. Also, TAT does not release the tromboning trunks if both Station A and Station C are attendants.

TAT and TRO-BA equipped on the same system

You can configure TAT and TRO-BA (including Virtual TRO-BA) together on the same system.

TAT and TRO-BA provide Trunk Route Optimization capabilities. Each feature optimizes trunks differently.

- If you configure both TAT and TRO-BA on the same system, TRO-BA takes precedence over TAT (refer to TRO-BA takes precedence over TAT on page 419). TRO-BA attempts to optimize a route before a call is answered, and TAT attempts to optimize trunks after the call is answered. The TAT feature enhances this capability (both CO trunks and PRI trunks are optimized) by eliminating redundant trunks between the system and DMS-250 switches equipped with the MCDN Release Link Trunk (RLT) feature.
- Both TAT and TRO-BA eliminate redundant trunks for calls that NCFAC, NCFNA, NCFB, and NHNT redirect.
- TRO-BA does not optimize tromboned trunks resulting from a Call Transfer. TAT optimizes tromboned trunks resulting from a Call Transfer.
- TRO-BA does not optimize tromboned trunks resulting from an incoming trunk call. TAT optimizes tromboned trunks resulting from an incoming trunk call.
- In call triangulation, TRO-BA attempts to eliminate tromboned trunks, while TAT does not. However, after TRO-BA optimizes, tromboning can result. In this case, TAT attempts to optimize the trunks. Refer to TRO-BA and TAT functionality in a call triangulation scenario on page 424.

TRO-BA takes precedence over TAT

Figure 61: TRO-BA and TAT operating together before optimization in a Call Forward scenario on page 420 shows how TRO-BA takes precedence over TAT in a call forward scenario.

- Station A on Node 1 calls Station B on Node 2 over an ISDN PRI/ISL/VNS trunk.
- Station B on Node 2 is forwarded, using the Call Forward All Calls feature, to Station C on Node 1 over another PRI/ISL/VNS trunk (redirected call). Tromboning exists between Node 1 and Node 2.

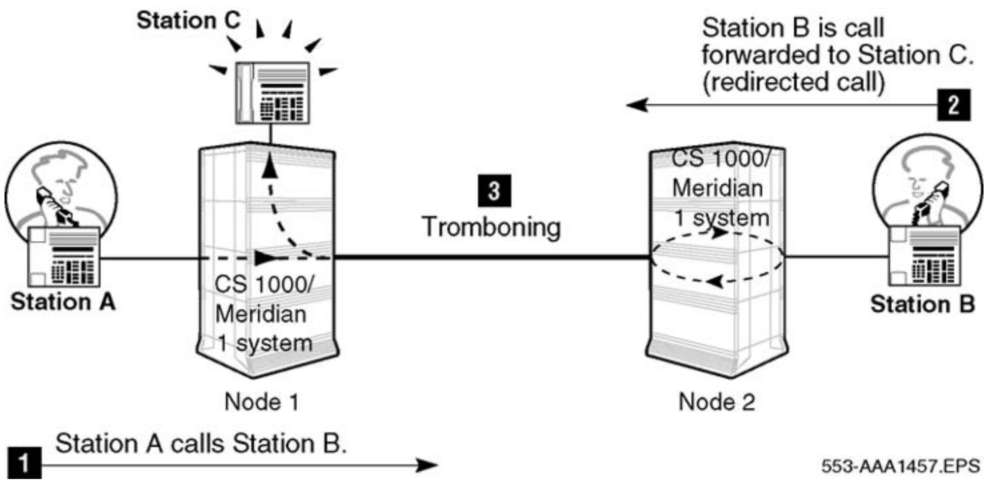

Figure 61: TRO-BA and TAT operating together before optimization in a Call Forward scenario

In Figure 62: After TRO-BA applies optimization on page 420, before Station C answers, TRO-BA releases the tromboned trunks between Node 1 and Node 2, and bridges Station A and Station C locally. The system does not invoke TAT because there are no tromboned trunks.

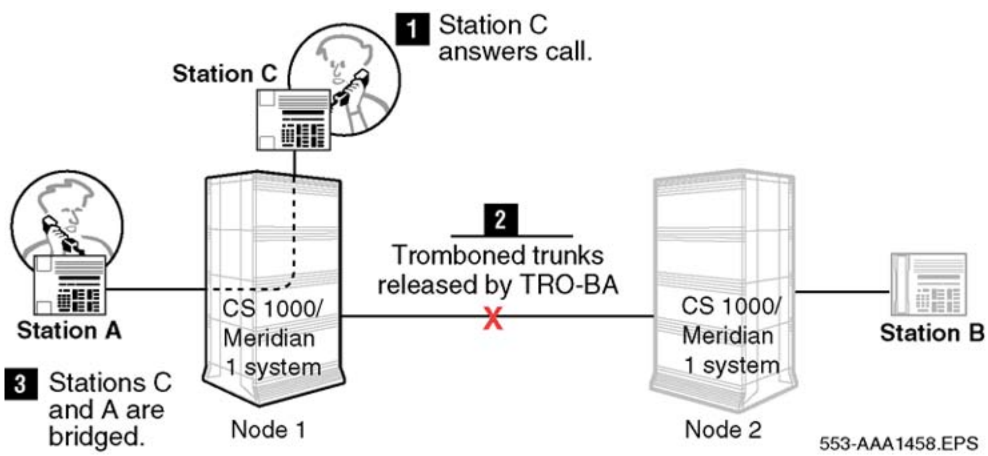

Figure 62: After TRO-BA applies optimization

TRO-BA does not optimize trunks resulting from a call transfer

TRO-BA does not optimize trunks resulting from a call transfer. In this case, TRO-BA completes anti-tromboning after the call is connected. TAT optimizes the trunks after the call is answered. Refer to Figure 65: TRO-BA and TAT operating together before optimization in a Call Transfer scenario on page 422.

- Station A on Node 1 calls Station B on Node 2 over a PRI/ISL/VNS trunk (first call).
- Station B initiates call transfer to Station C on Node 1 over another PRI/ISL/VNS trunk, and completes the call transfer while Station C is in a ringing state. Trombonning exists between Node 1 and Node 2 (second call).

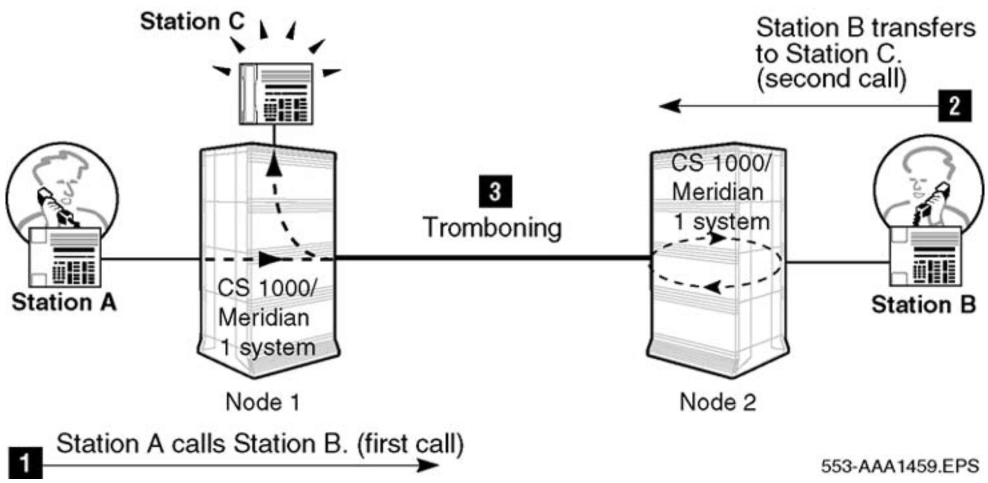

Figure 63: TRO-BA an d TAT operating together before optimization in a call transfer scenario

Since TRO-BA does not release tromboned PRI trunks resulting from a call transfer, the trunks between Node 1 and Node 2 remain tromboned until Station C answers the call transfer.

While the call is still in a ringing state, TRO-BA does not release the tromboned trunks. After Station C answers, TAT releases the tromboned trunks between Node 1 and Node 2, and bridges Station C and Station A locally. Refer to Figure 64: After TAT applied to tromboned trunks due to a call transfer on page 421.

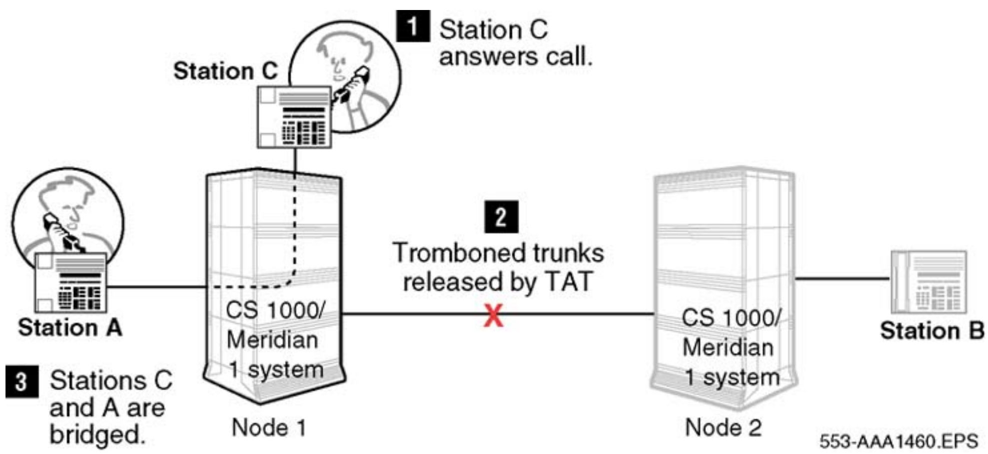

Figure 64: After TAT applied to tromboned trunks due to a call transfer

Trunk Route Optimization with call redirection resulting from a call transfer

Following is an example of TRO-BA and TAT interaction in the case of a call redirection initiated on the transfer key. Refer to Figure 65: TRO-BA and TAT operating together before optimization in a Call Transfer scenario on page 422:

- Station A on Node 1 calls Station B on Node 1.
- Station B initiates a call transfer to Station C on Node 2 over a PRI/ISL/VNS trunk (first B-channel).
- Station C forwards the call to Station D on Node 1, using Call Forward No Answer over another PRI/ISL/VNS trunk (second B-channel due to call redirection). Trunk tromboning occurs between Node 1 and Node 2.

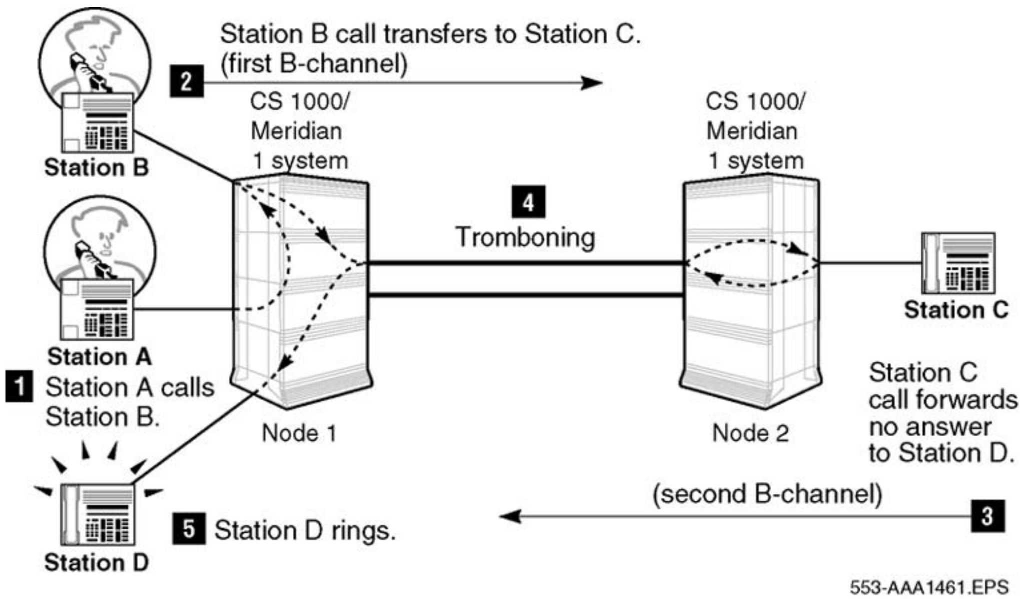

Figure 65: TRO-BA and TAT operating together before optimization in a Call Transfer scenario

Station B completes the call transfer while Station C is in A ringing state. The system (Node 1) software routes the call to Station D; then TRO-BA optimizes the trunks, and locally bridges Station A and Station D. Refer to Figure 66: Tromboned trunks released by TRO-BA on page 423.

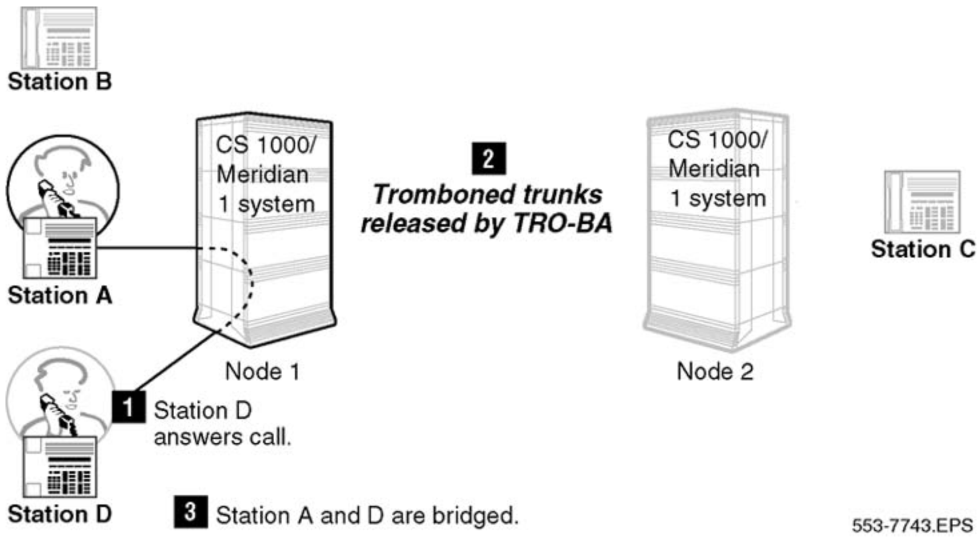

Figure 66: Tromboned trunks released by TRO-BA

- If Station B does not complete the call transfer while Station C is ringing, but waits until Station D answers, TRO-BA does not perform optimization.
- After Station D answers, TAT applies anti-tromboning to release the trunks between Node 1 and Node 2, and locally bridges Station A and Station D. Refer to Figure 67: Tromboned trunks released by TAT on page 423.

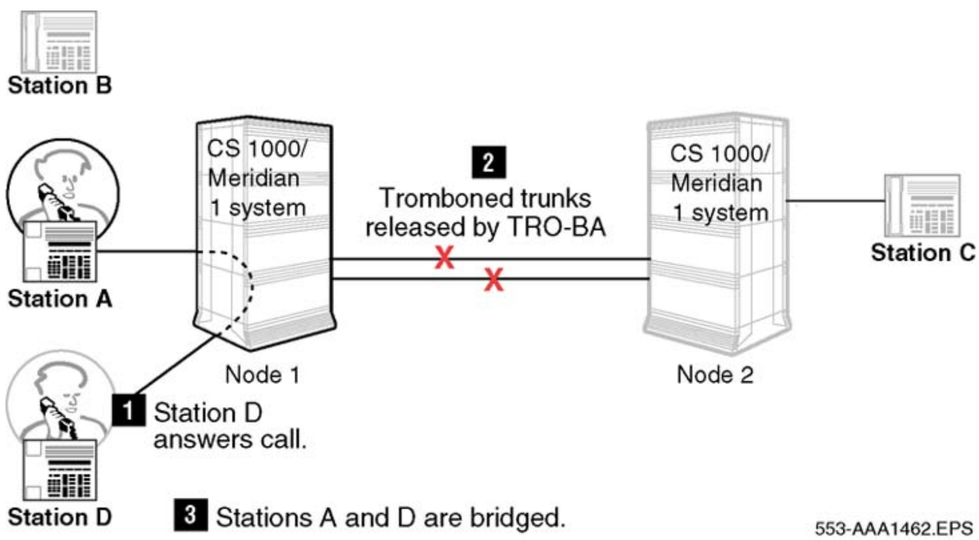

Figure 67: Tromboned trunks released by TAT

TRO-BA and TAT functionality in a call triangulation scenario

In a call triangulation scenario, TRO-BA attempts to eliminate tromboned trunks. TAT cannot perform this operation because a second D-channel is involved. Refer to Figure 68: Call path before TRO-BA is applied on page 424:

- Station A on Node 1 calls Station B on Node 2 over a PRI/ISL/VNS trunk (first call).
- Station B on Node 2 is call forwarded or hunts to Station C on Node 3 over another PRI/ISL/VNS trunk (redirected call). Two trunks are being used to handle one call.

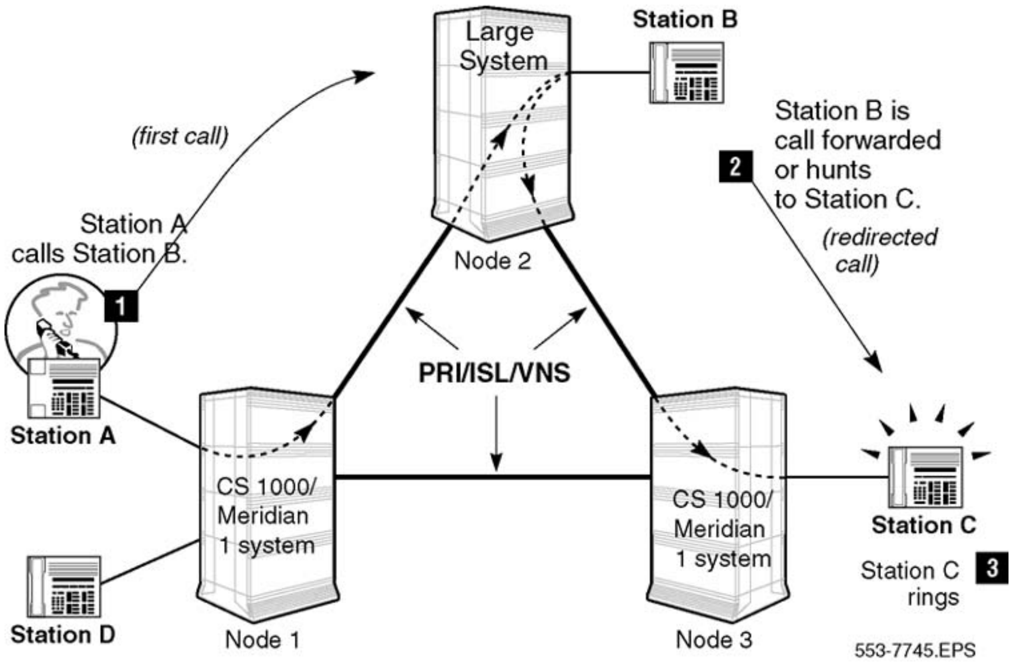

Figure 68: Call path before TRO-BA is applied

Before Station C answers, TRO-BA releases the trunks between Node 1 and Node 2, and between Node 2 and Node 3, and establishes a new PRI/ISL/VNS trunk connection between Node 1 and Node 3. Refer to Figure 69: Call path after TRO-BA is applied on page 425.

Note:

The TAT feature cannot provide this functionality because multiple D-channels are used.

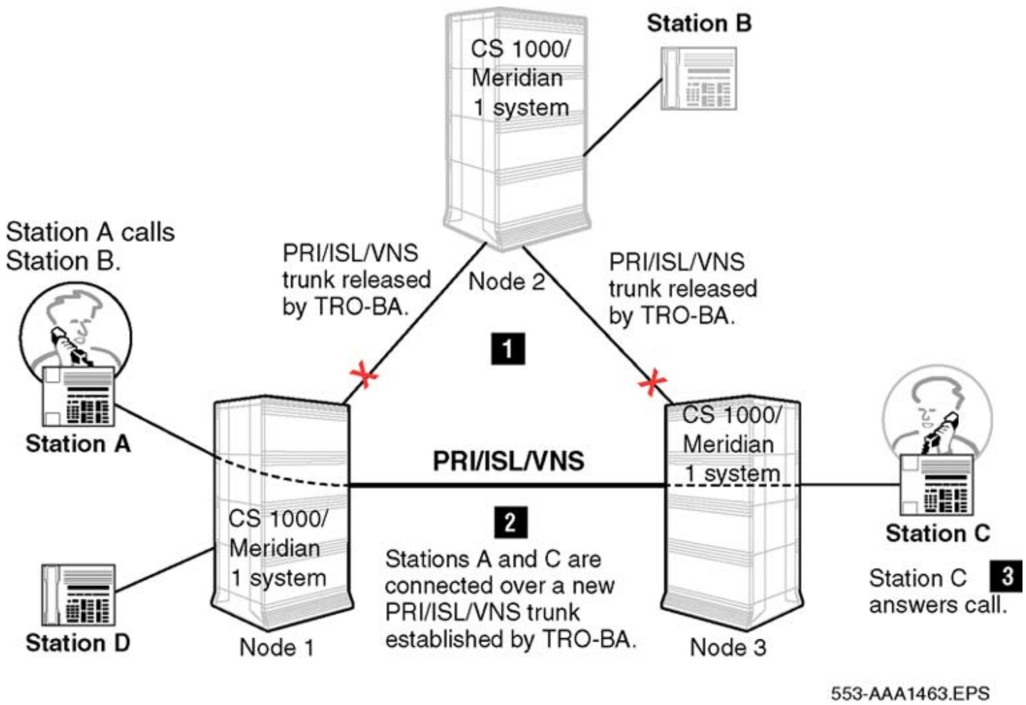

Figure 69: Call path after TRO-BA is applied

Tromboning can result after TRO-BA performs optimization. In this case, TAT attempts to optimize the trunks. This scenario occurs in the following situation.

- Station C answers the call and initiates a call transfer to Station D on Node 1 over a separate PRI/ISL/VNS trunk. This results in tromboning between Node 1 and Node 3. Refer to Figure 70: Tromboning of trunks after TRO-BA is applied on page 426.

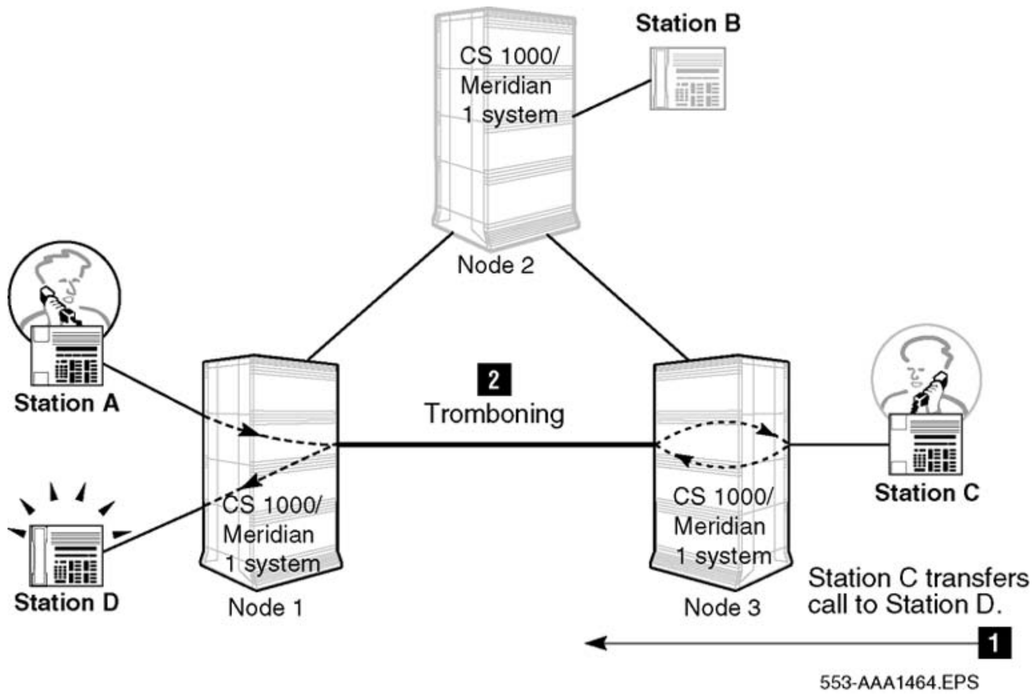

Figure 70: Tromboning of trunks after TRO-BA is applied

- After Station D answers the call, and Station C completes the call transfer, TAT releases the tromboned trunks between Node 3 and Node 1, and leaves Station D and Station A bridged locally. Refer to Figure 71: Tromboned trunks released by TAT on page 426.

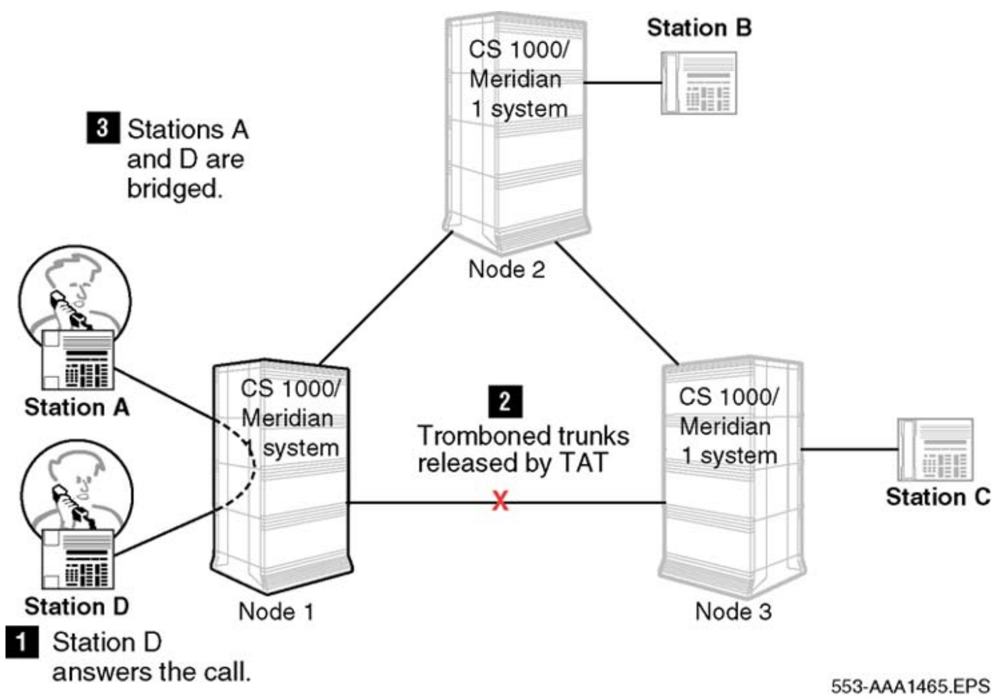

Figure 71: Tromboned trunks released by TAT

SIP trunk anti-tromboning

Consider Set A and Set C in the same CS 1000 node, for example Node A. Consider Set B in Node B running a third party SIP Client. When Set A calls Set B (in another node) and Set B transfers the call back to Set C (on the same node as SET A) using the second trunk, tying up two trunks, SIP trunk anti-tromboning (SIP TAT) feature will release the first trunk optimizing DSP resources.

Important:
CS 1000 only requires SIP TAT when it communicates with a third party node over SIP. If both nodes are in CS 1000, then the existing MCDN TAT feature optimizes these trombone trunks between two CS 1000 nodes.

Trunk Route Optimization-Call Modification

TRO-CM optimizes trunks after call modification in scenarios that are not handled by TRO-BA and TAT.

The TRO-CM feature depends on the TRO-BA feature. It requires all the packages and the configuration of TRO-BA.

TRO-CM optimizes trunks for the following call scenarios:

- blind-transferred from a station
- transferred after consultation (supervised transfer)
- extended by the attendant console
- reverting to a point-to-point call when one party disconnects from a three-party conference
- answered by voicemail and subsequently blind-transferred by Dial 0, Revert DN, or Automated Attendant service
- entering or leaving the private network on PSTN trunks; private network trunks are optimized after any call modification

Events that trigger TRO-CM

The system triggers TRO-CM in the following scenarios:

- transfer trigger The System invokes TRO-CM for calls transferred from a station across a network. The transfer can be blind or supervised.
    - manual transfer The user can manually initiate call transfer from a phone. For example, Station A (on Node 1) calls Station B (on Node 2). Station B answers the call and initiates call transfer to Station C on a different node.
    - automated transfer The System can also initiate call transfer using the Auto-attendant, Thru-dial or Call Sender features of Avaya CallPilot/Meridian Mail. For

example, Station A (on Node 1) calls Station B (on Node 2). Station B activates Call Forward to voicemail. Station A is connected to CallPilot/Meridian Mail. Station A activates the Dial 0 Revert DN feature. This invokes blind transfer to Station C at Node 3. CallPilot/Meridian Mail completes the transfer.

- attendant extending call The System triggers TRO-CM when the attendant at the tandem node extends the call to a station on another node and drops out of the call. This occurs only when the station answers the call. The attendant is able to drop out of the call until the station answers the call.
- conference call on disconnection The System triggers TRO-CM when a conference call reverts to a two-party call.

TRO-CM basic operation

In Figure 72: TRO-CM basic operation on page 428, Figure 72: TRO-CM basic operation on page 428, Station A calls Station B. Station B answers the call and transfers to Station C. Station C answers the call and Station B completes the transfer.

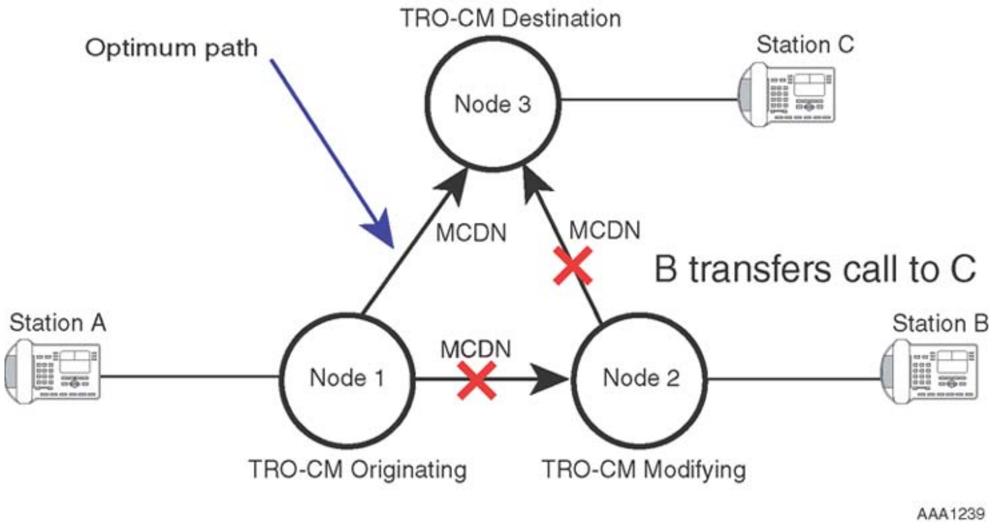

Figure 72: TRO-CM basic operation

Operating parameters

TRO-BA operating parameters

The system only supports TRO-BA if the originated call is not answered.

For TRO-BA to be supported on all nodes involved, you must set the TRO prompt to YES in the Route Data Block (LD 16). Also, each phone redirecting the call must have a Call Forward/

Hunt feature allowed. If the originating phone and the redirecting phone reside on the same node, the system does not support the TRO-BA operation.

Trunk routes targeted for optimization must be listed in the Route List Index (RLI entry 0).

The system only supports ISDN PRI/ISL trunks. If the system uses an analog or digital trunk (not controlled by a D-channel) between the originating and redirecting node, then TRO-BA does not operate. The call continues on the original path.

Trunk Route Optimization operates independently of the phone type used for a call. TRO-BA works for both voice and data calls between systems.

Only system-to-system connections are supported. If non-system switches can send the TRO-BA messages, they can operate as tandem switches.

When the system redirects the call, the redirecting system begins a two-second timer while waiting for a response message from the originating node. If the timer expires, the call continues along the original path, and TRO-BA does not operate.

Note:

Carefully analyze traffic estimates for all routes targeted for TRO-BA. This ensures that enough trunks and routes are available for all routing possibilities.

The system does not support TRO-BA with mixed dialing plans. Use caution when implementing TRO-BA on a network that uses a Uniform Dialing Plan (UDP) and a Coordinated Dialing Plan (CDP) at the same time. TRO-BA can direct calls to the wrong location because location codes are not used between CDP locations. Duplicating CDP Directory Numbers (DNs) at other TRO-BA locations can cause TRO-BA to redirect the call to the wrong DN.

TRO-BA does not support Trunk Route Optimization for the following call types:

- A Direct Inward Dialing (DID) trunk call at Node A goes to Station B, (on Node B), and NCFAC, NCFNA, or NHUNT to Station C. This is a mixed dialing plan. Refer to Figure 73: TRO-BA non-support on page 430.
- A DID trunk call from Node A to Station A (that has NCFAC, NCFNA, or NHUNT) to Station B (that has NFAC, NCFNA, or NHUNT) to Phone C. Refer to Figure 73: TRO-BA non-support on page 430.
- Station D (at Node D) calls Station B (at Node B), which has NCFAC, NCFNA, or NHUNT, to Station C (at Node C), where Node D is connected by non-ISDN link to Node C. Refer to Figure 73: TRO-BA non-support on page 430.
- The attendant extends a DID or Incoming trunk call to Phone B (at Node B) and releases, and Phone B is CFNA to Phone C (at Node C). After three rings, the call is forwarded to Phone C, but not optimized. Refer to Figure 73: TRO-BA non-support on page 430.

  If the attendant remains with the call, TRO-BA functions.
- Phone A uses Transfer or Conference to Phone B when Phone B has NCFAC, NHUNT, or NCFNA to Phone C. Refer to Figure 73: TRO-BA non-support on page 430.

- Calls to Meridian Mail auto attendant functions are not optimized because the call is viewed as being answered.
- If the system exceeds the network redirection counter limits, TRO-BA does not initiate.
- ACD Night Call Forward calls.
- ACD Interflow calls.

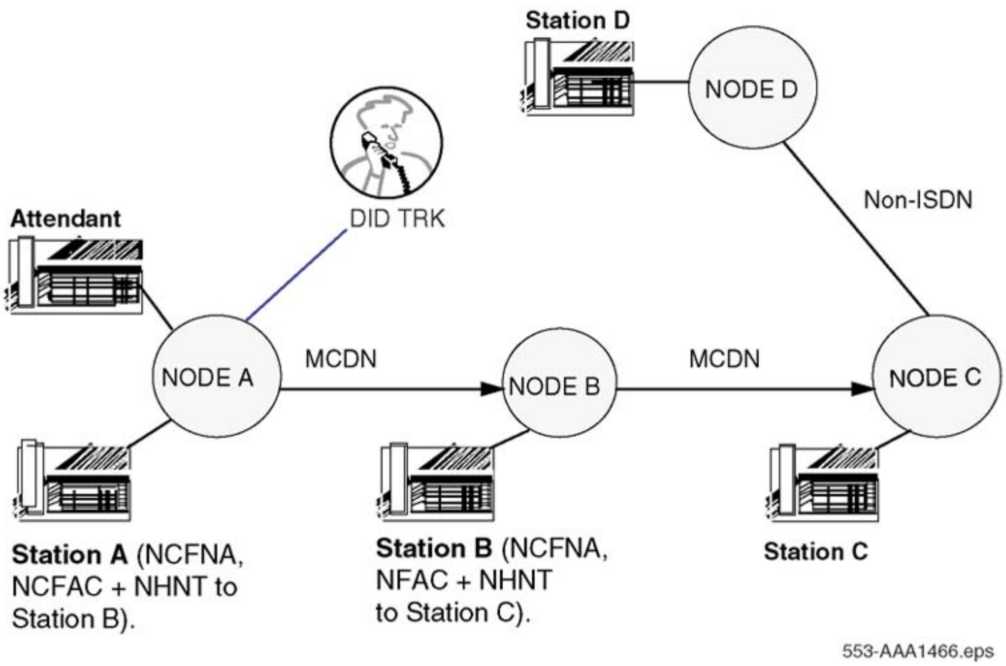

Figure 73: TRO-BA non-support

TAT operating parameters

TAT only performs anti-tromboning:

- after the third party answers
- if tromboning PRI/ISL/VNS or analog trunks are associated with the same primary D-channel (with or without a backup D-channel)
- if the trunks are associated with the same customer

The system only supports Trunk Anti-Tromboning on the Multi-purpose Serial Data Link (MSDL) card for D-channel handling.

Note:

To support the Trunk Anti-Tromboning feature within a dedicated ISL/VNS configuration, an NTAK02 (minimum vintage BB) Serial Data Interface (SDI)/D-channel (DCH) circuit card must be used.

TAT does not perform Anti-tromboning:

- if the tromboning trunks belong to different customers on the same node (even though they are associated with the same primary D-channel)
- for a tromboned call between two attendants on the same node
- if non-ISDN PRI trunks are involved in a call transfer call, and therefore ISDN signaling messages cannot be sent
- for tromboned trunks associated with a call originating on a phone and routed back to the same phone
- for BRI trunks, except if the trunks are VNS bearer trunks

TAT protocols

TAT operations use two types of protocols, depending on the interface type.

- system-to-system interface
- system to DMS-250 Sprint load equipped with the MCDN RLT feature

TAT can cause a momentary interruption in data transmission during optimization. When the system performs TAT operations at multiple tandem nodes, the effect is cumulative (in the milliseconds range.) Therefore, the impact of this loss depends upon the terminals on both ends of the transmission and can be recovered through re-transmission.

Anti-Tromboning scenarios

The Anti-Tromboning scenarios in this section provide examples for a system interworking with another system, and a system interworking with a DMS-250 Sprint load equipped with Release Link Trunk (RLT).

Trunk Anti-Tromboning scenario legend

Figure 74: Notation for illustrations on page 432 shows the notations used for the graphics in the TAT section.

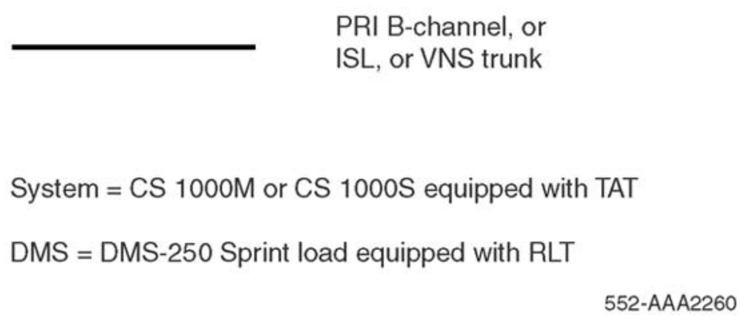

Figure 74: Notation for illustrations

Note:

In the scenarios that follow, the system does not have the TRO-BA feature configured.

Anti-Tromboning operation for NCRD (case 1) PBX interworking with DMS

The following example shows TAT being applied in an NCRD scenario (in the example, Call Forward is used), with two system switches interworking with a DMS-250. Refer to Figure 75: Anti-Tromboning for NCRD (case 1), PBX/DMS on page 433.

- Station A, (located at the originating switch [CO or PBX] or a DMS node), makes an internodal call through a DMS-250 and a tandem system node to Station B, (located at a terminating system node). This is the first call.
- Station B, located at the terminating system node, is call forwarded through the tandem system node and the DMS-250, to Station C located at the originating node (redirected call)
- Station C answers.
- Station A connects to Station C.

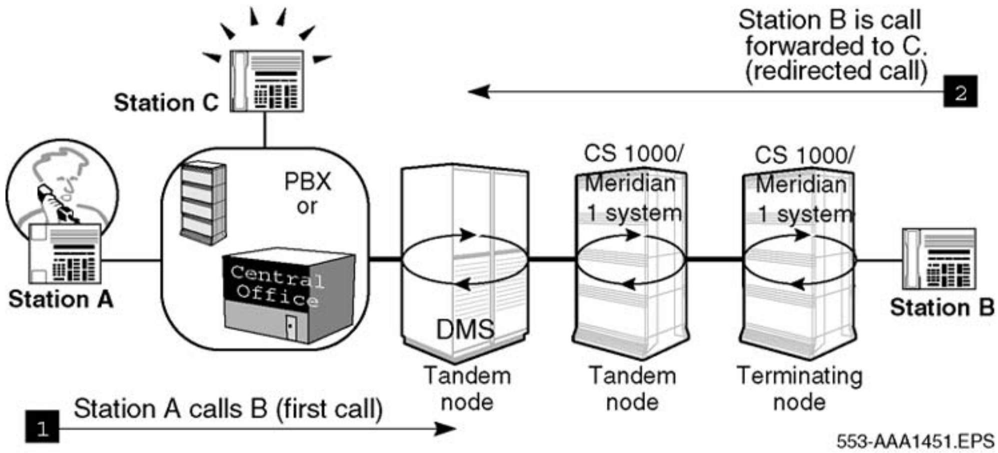

Figure 75: Anti-Tromboning for NCRD (case 1), PBX/DMS

The following occur as a result of anti-tromboning after Station C answers a call (refer to Figure 76: Results of anti-tromboning for NCRD (case 1), PBX/DMS on page 433):

- The DMS tandem node bridges the call between A and C.
- TAT releases the trunks between the terminating system and the tandem system.
- The RLT feature releases the trunks between the tandem system and the DMS.

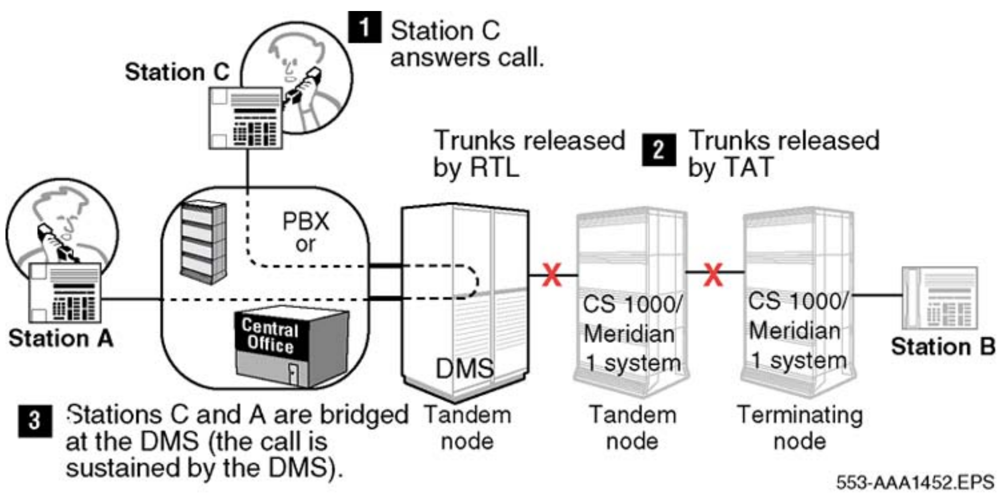

Figure 76: Results of anti-tromboning for NCRD (case 1), PBX/DMS

Anti-tromboning operation for NCRD (case 2) - the system interworking with DMS

In Figure 77: Anti-tromboning for NCRD (case 2), system/DMS on page 434, TAT optimizes redundant trunks due to a call forward operation. In this case, TAT optimizes the trunks between the terminating node and the tandem node. The originating node is a DMS-250. Station C is a centralized attendant or a Meridian Mail position.

- Station A, (located at an originating switch [CO or PBX]), makes an internodal call through a DMS-250 tandem node and the system tandem node to Station B, (located at the terminating node) (first call).
- The terminating node performs call forward from Station B to Station C, (located at the tandem node) (redirected call).
- Station C answers.
- Station A connects to Station C.

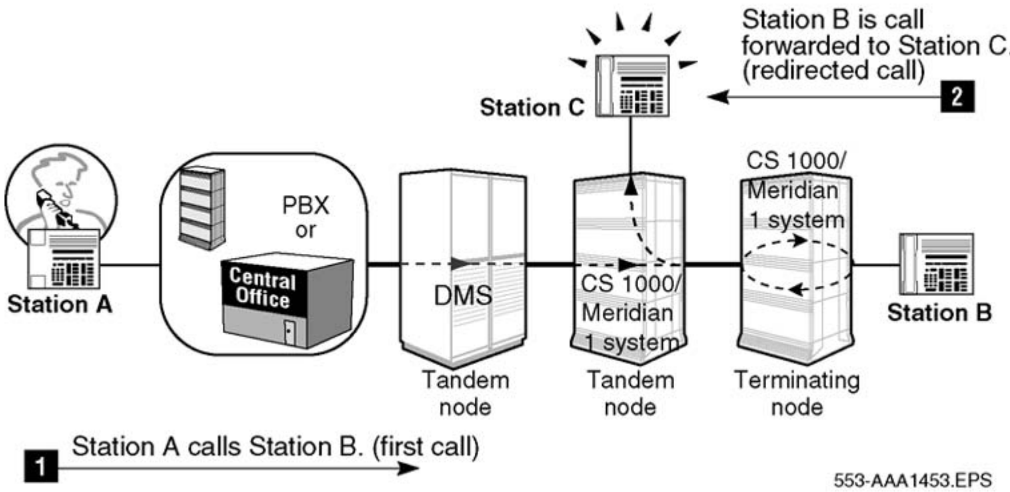

Figure 77: Anti-tromboning for NCRD (case 2), system/DMS

The following are the results of anti-tromboning after Station C answers the call (refer to Figure 78: Results of anti-tromboning for NCRD (case 2) - system interworking with DMS on page 435):

- Station C and Station A are connected.
- TAT releases the trunks between the terminating node and the tandem node.

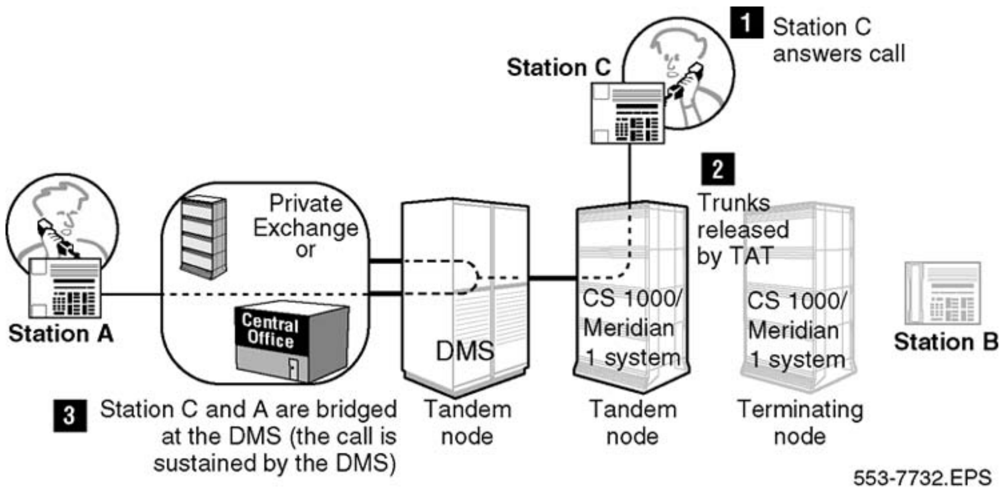

Figure 78: Results of anti-tromboning for NCRD (case 2) - system interworking with DMS

Anti-tromboning operation for call modification - DMS interworking with the system

The following case shows TAT applied to a Call Modification scenario with a DMS interworking with a system. In the example a call transfer is used.

Note:

The same effect takes place if Station B conferences in Station C and then drops out, leaving Station A and Station C connected.

Refer to Figure 79: Anti-tromboning for Call Modification - DMS/System on page 436.

- Station A, (located at the originating node), makes an internodal call through the DMS tandem node to Station B, (located at the terminating node) (first call).
- Station B answers the call and initiates a call transfer through the DMS tandem node to Station C, (located at the originating node) (second call).
- Station C answers the call.
- Station B completes the Call Transfer operation.

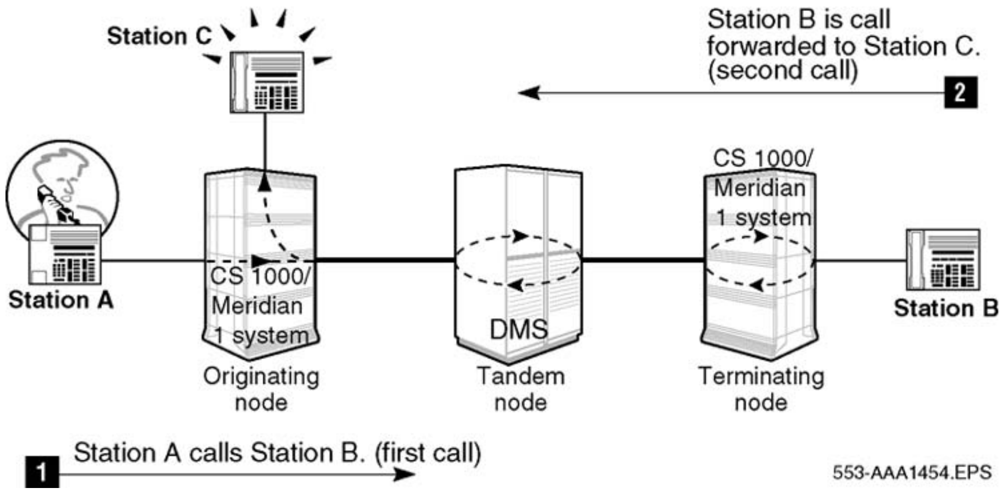

Figure 79: Anti-tromboning for Call Modification - DMS/System

The following are the results of anti-tromboning after Station C answers the call (refer to Figure 80: Results of anti-tromboning for Network Call Transfer - DMS/System on page 436):

- The system originating node bridges the call between A and C.
- The RLT feature releases the trunks between the terminating node and the DMS, and between the DMS and the originating node.

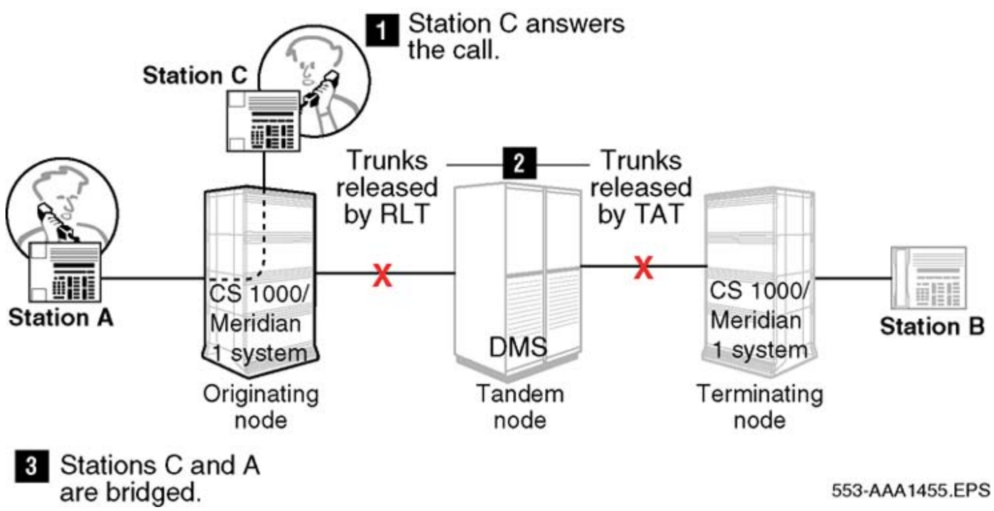

Figure 80: Results of anti-tromboning for Network Call Transfer - DMS/System

Anti-tromboning operation for Call Modification - the system interworking with another system

The following scenario shows TAT applied to a call modification scenario with the system interworking with another system (in the example, Call Transfer is used.) Refer to Figure 81: Anti-tromboning for Network Call Transfer - system/system on page 437.

- Station A, (located at the originating node), makes an internodal call through the tandem node to Station B, located at the terminating node (first call).
- Station B answers the call and initiates a call transfer through the DMS tandem node to Station C, (located at the system originating node) (second call).
- Station C answers the call.
- Station B completes the Call Transfer operation.

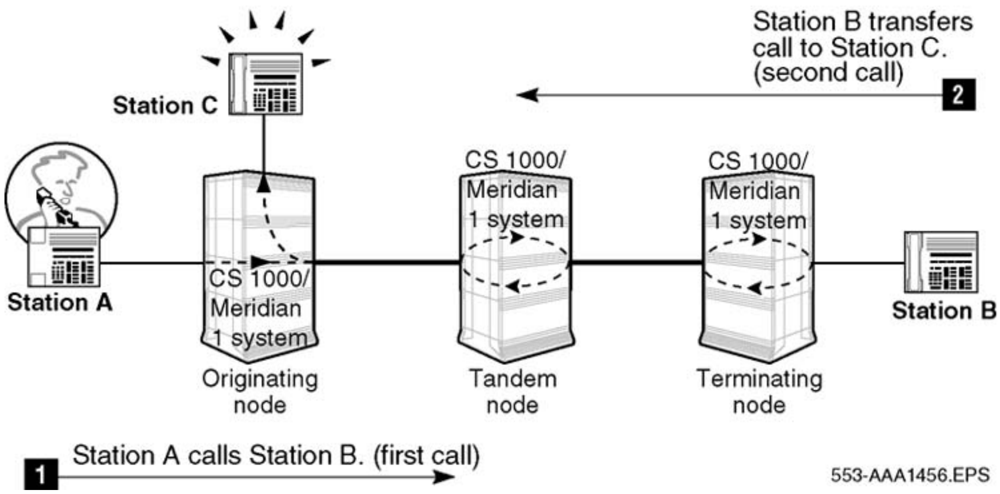

Figure 81: Anti-tromboning for Network Call Transfer - system/system

The following are the results of anti-tromboning after Station C answers the call (refer to Figure 82: Results of anti-tromboning for Network Call Transfer - system/system on page 438):

- The originating node bridges the call between Station A and Station C.
- TAT releases the tromboning trunks between the terminating node and the tandem node, and between the tandem node and the originating node.

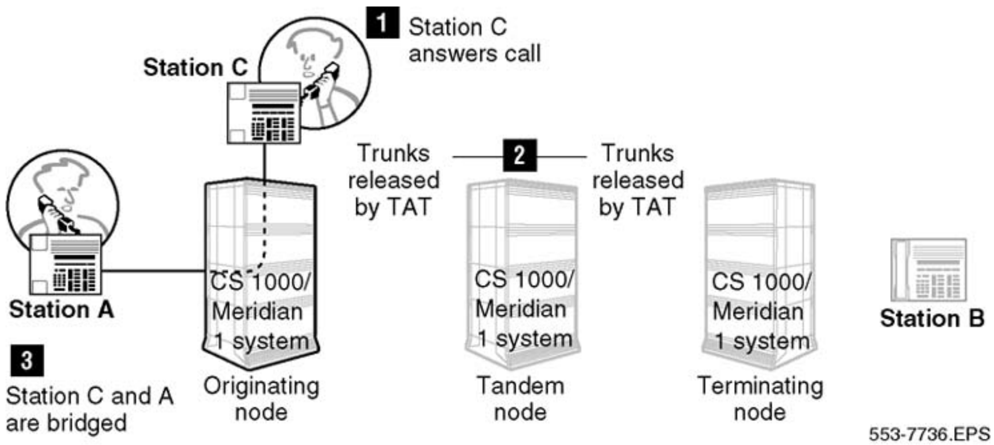

Figure 82: Results of anti-tromboning for Network Call Transfer - system/system

TRO-CM operating parameters

The TRO-CM feature depends on the TRO-BA feature. It requires all the packages and the configuration of TRO-BA.

Only MCDN connections support TRO-CM.

Anti-tromboning

TRO-CM does not release the call when an outgoing trunk call comes back to the same node either on the same D-channel or on two different D-channels. Also, if two different Customer Groups are on the same D-channel on outgoing trunk calls, TRO-CM does not release the call.

However, if the same D-channel holds the outgoing call and the incoming transferred call, then TAT triggers and releases the trunks. See Tromboning.

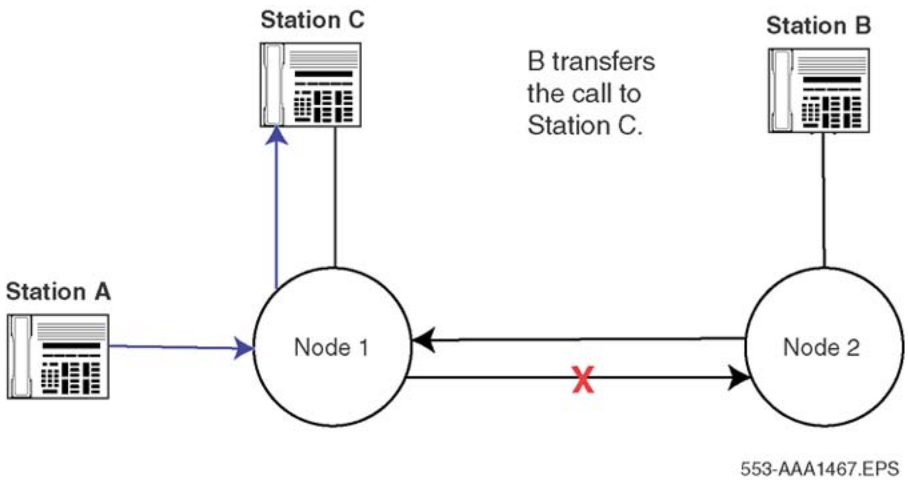

Figure 83: Tromboning

Attendant calls

If the originator of the call is an Attendant on the TRO-CM originating node, the system defers the TRO-CM request while the attendant is active on the call. The system accepts TRO-CM when the attendant leaves the call.

Call originator transfers

TRO-CM does not optimize the call when the call originator transfers the call to another node.

For example, in Originating party transfers the call, Station B calls Station A. Station A answers the call. Station B transfers the call to Station C. TRO-CM fails.

TRO-CM fails when the conference originator drops out of the conference.

For example, in Figure 84: Originating party transfers the call on page 440, Station B calls Station A. Station A answers the call. Station B conferences Station C and Station B drops out of the conference. TRO-CM fails.

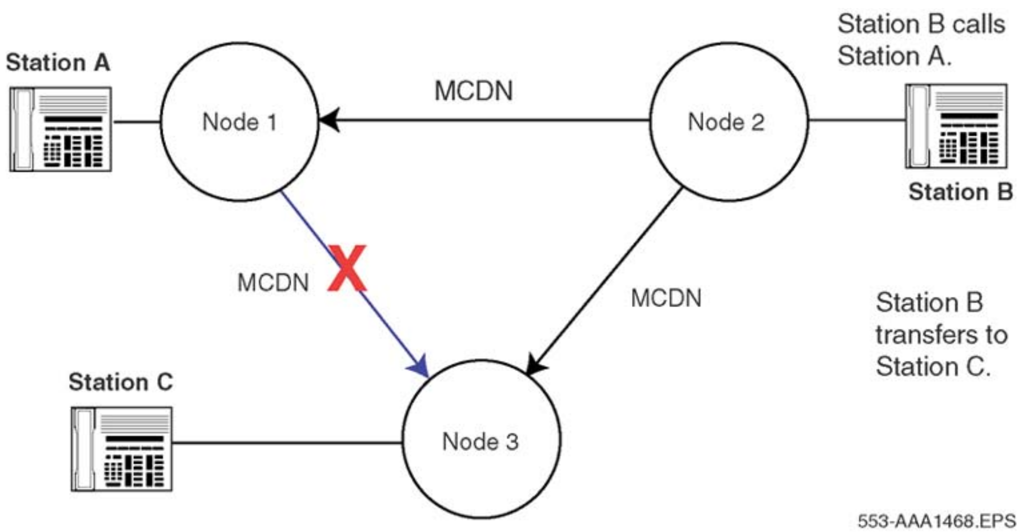

Figure 84: Originating party transfers the call

Conference call on disconnection

The system triggers TRO-CM when a conference call reverts to a two-party call.

For example, in Figure 85: TRO-CM operation after conference call on page 440, Station A (Node 1) calls Station B (Node 2). Station B answers the call. Station B initiates the conference to Station C on Node 3. Station C answers the call. Station B completes the conference. The three parties are in conference. Station B drops out of conference. The system triggers TRO-CM to optimize the path between Station A and Station C.

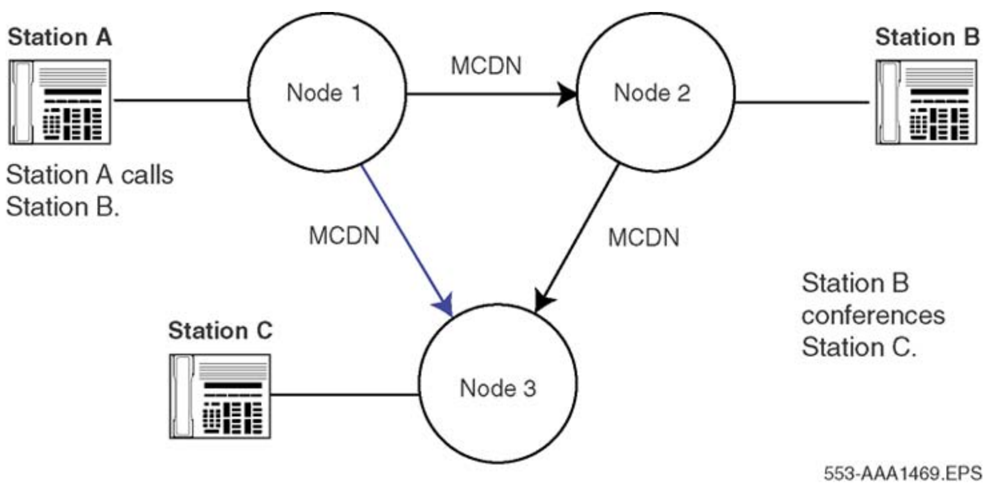

Figure 85: TRO-CM operation after conference call

Congestion trigger

Unlike QSIG Path Replacement (QPR), the system does not trigger TRO-CM if non-optimum path results exist because of congestion.

Refer to Figure 86: Network congestion on page 441. Station B receives an incoming call from Station A. The system routes the call through Node 2 because the link between Node 1 and Node 3 is congested. Station B answers. Upon reception of a connect indication from Node 3, Node 1 does not initiate optimization. The link between Nodes 1 and 3 stays in place for the duration of the call. The system does not optimize TRO-CM.

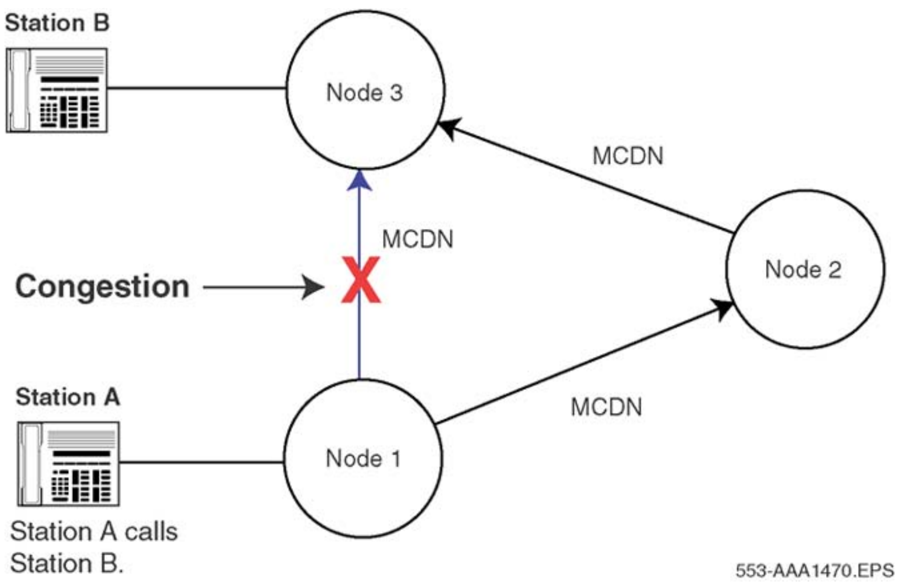

Figure 86: Network congestion

Data and fax calls

The system can lose or corrupt data during speechpath swapping due to the following:

- pads introduced by the conference card
- continuous conference warning tone

Data applications, such as fax machines, which use normal voice line cards and configuration, are subject to momentary loss of speech during the change-over of speechpaths. This change-over can cause a loss of synchronization between the devices. The system does not trigger TRO-CM during data calls because this affects data transmission.

The TRO-CM feature does not optimize a call involving an analog (500/2500-type) phone configured with the Fax Allowed (FAXA) Class Of Service (COS). This also applies to T.38 Fax calls because these machines use FAXA for COS.

First choice route

The system attempts TRO-CM only on the first choice route on the TRO-CM originating node.

If the systems run Succession 3.0 software, the system attempts TRO-CM on all tandem nodes on the first choice route. If the tandem nodes run an earlier software release, the system selects any available route for the optimized call.

If the system cannot find an idle trunk on the first choice route when trying to optimize the call, the system does not attempt TRO-CM on the TRO-CM originating node and on all the tandem nodes on Succession 3.0 software.

Gateway functionality

TRO-CM does not support Gateway functionality with other equivalent features, such as QSIG Path Replacement (QPR), DPNSS Route Optimization (RO), EuroISDN Explicit Call Transfer (ECT), and RLT on DMS100/ DMS250 features.

Refer to Figure 87: Gateway functionality on page 442. Node 4 rejects the QPR trigger from Node 5 when the system completes the transfer. The system does not map QPR messages into equivalent TRO-CM messages.

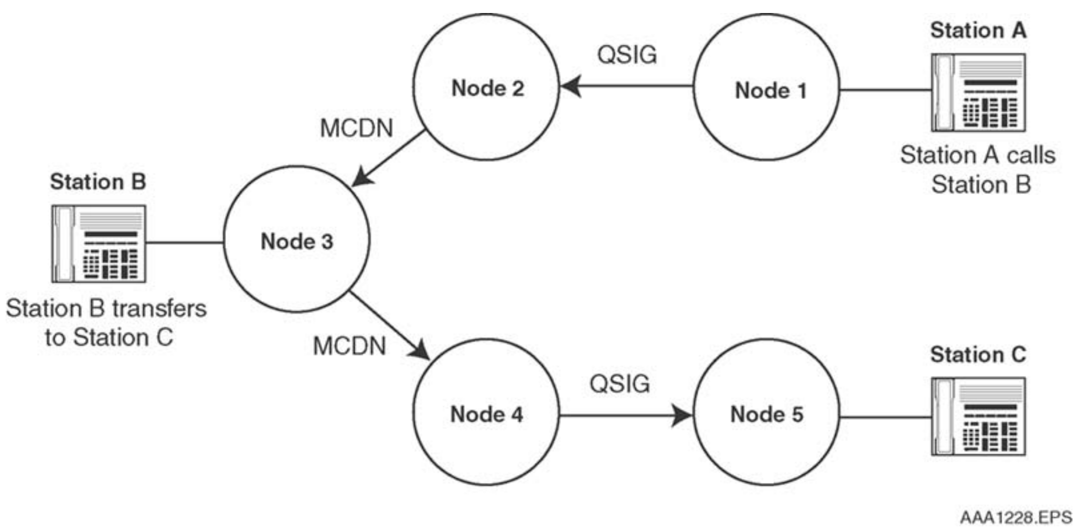

Figure 87: Gateway functionality

Initialization

The system releases conferences when it initializes.

On the TRO-CM destination node

If a system initialization occurs on the TRO destination node, the system aborts all TRO-CM operations.

During call process optimization, when the old and the new paths are in conference on the TRO-CM destination node, an initialization on the destination node causes the call to be lost.

On the TRO-CM originating node

A system initialization causes all received TRO-CM requests to be lost. The system does not inform the TRO-CM destination node that the request was cancelled.

If the TRO-CM originating node initializes before setting-up the new connection, then the TRO-CM destination node resends the TRO-CM trigger. If the TRO-CM originating node initializes after the system sets up the new connection, then it disconnects the new path on the expiry timer T2.

Interworking

The system invokes TRO-CM at the interworking node. For example, the system optimizes calls entering or leaving the private network on Public Switched Telephone Network (PSTN)/ private network trunks after any call modification. However, the system only optimizes the MCDN network. Refer to Figure 88: TRO-CM successful at an interworking node on page 444 and Figure 89: Non-MCDN trunk terminations on page 444.

Duplicate CDN entries and SPN codes in a TRO enabled private network can direct calls to the wrong location or fail the call.

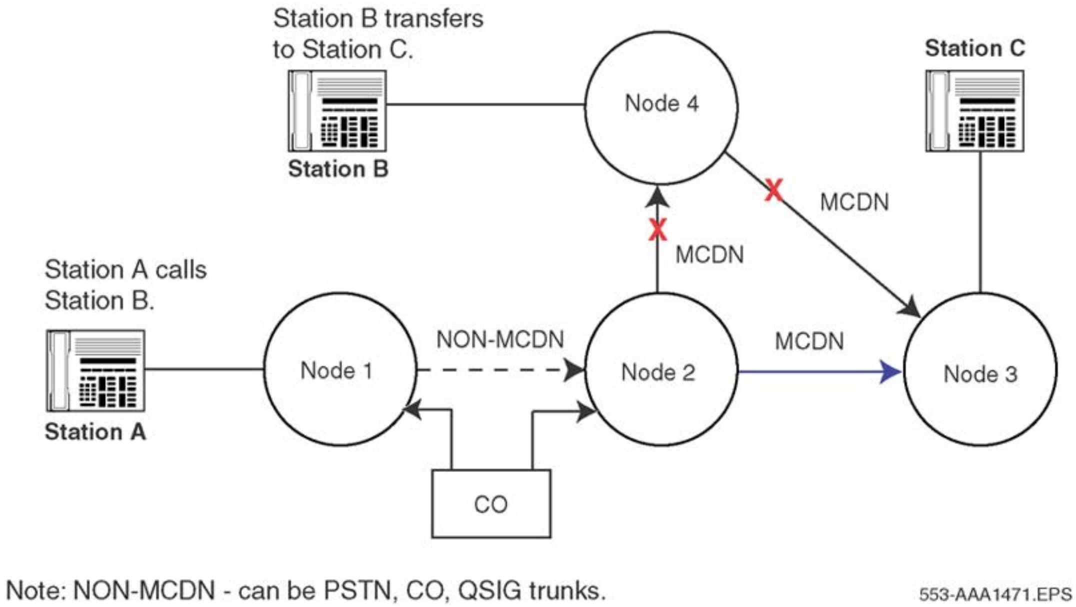

Figure 88: TRO-CM successful at an interworking node

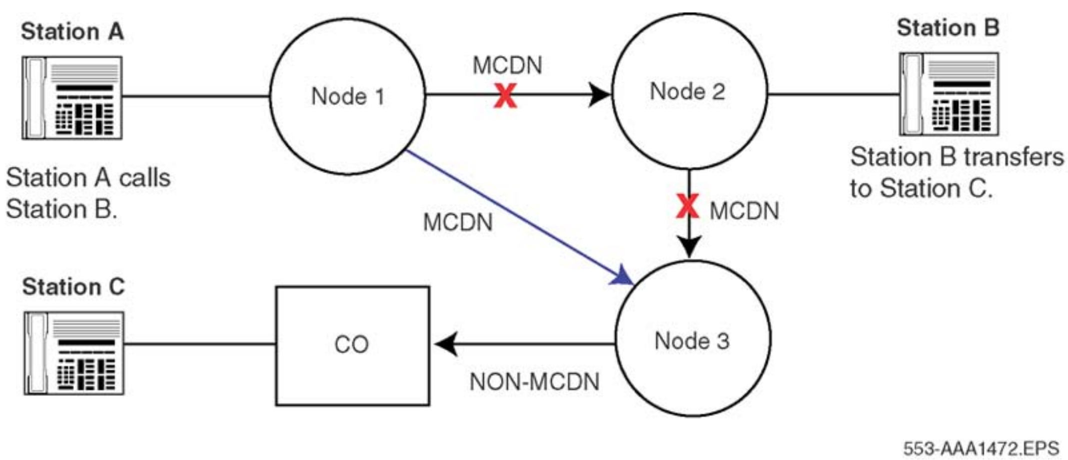

Figure 89: Non-MCDN trunk terminations

MCDN Release Link Trunk

TRO-CM does not support interworking with DMS switches or SL-100 systems equipped with the MCDN RLT feature.

For example, in Figure 90: Interworking with DMS-100 on page 445, the system triggers TRO-CM to optimize the MCDN nodes, or triggers RLT on the CO trunks to optimize the trunks between Nodes 1 and 5. The optimization attempt is unsuccessful.

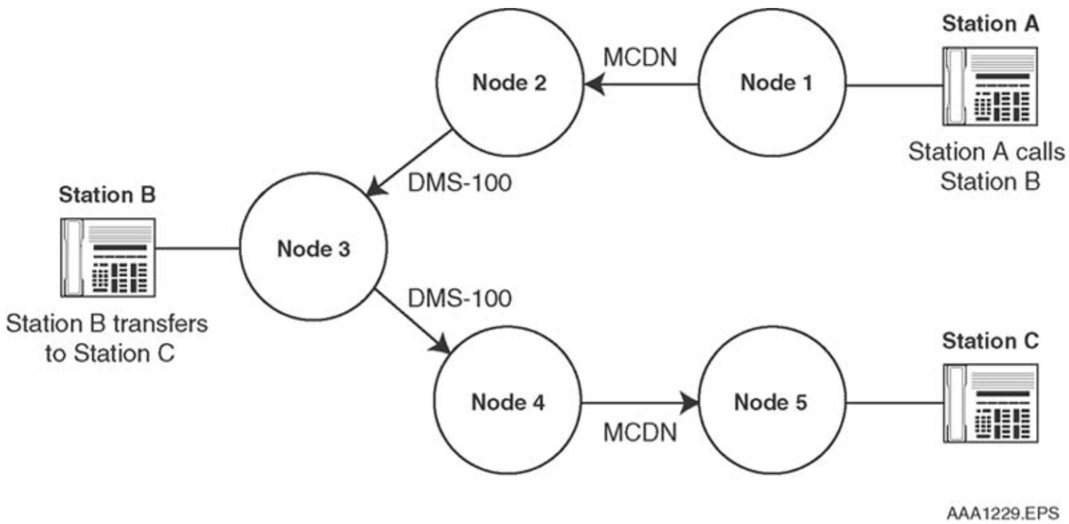

Figure 90: Interworking with DMS-100

Numbering plans

You must choose either the CDP or UDP for the MCDN. The system requires a consistent numbering plan for the correct operation of the TRO-CM feature.

TRO-CM does not support:

- route access codes
- the use of transit nodes to modify digits
- a mix of CDP and UDP

Optimum path - non-MCDN link

The optimum path must be an MCDN link. In Figure 91: TRO-CM fails when the optimum path is not an MCDN trunk on page 446, Station A calls Station B. Station B is transferred to station C. Node 1 initiates a new call, but the optimum path from Node 1 to Node 3 is a QSIG link. The system does not optimize when the optimum path is on a VNS Trunk Route, because the bearer trunks are non-MCDN trunks. TRO-CM fails.

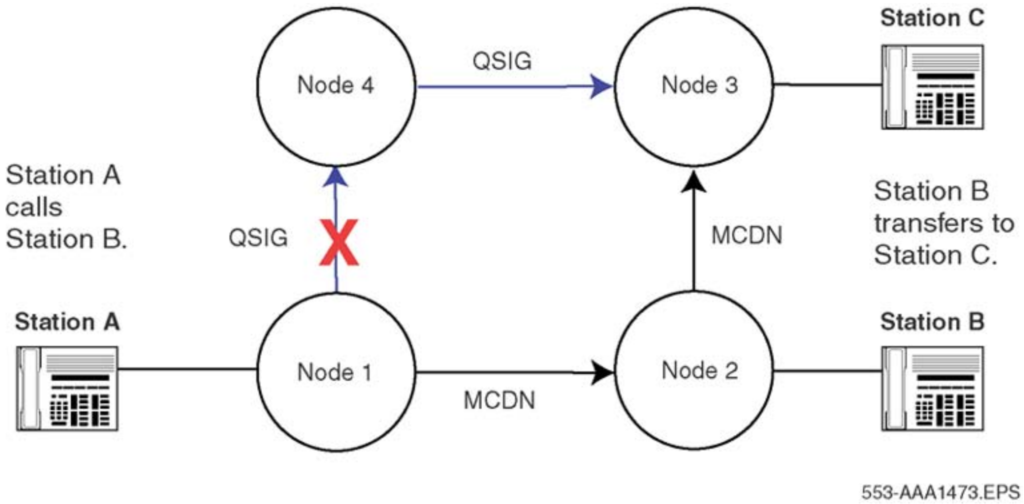

Figure 91: TRO-CM fails when the optimum path is not an MCDN trunk

The system supports TRO-CM only on MCDN trunks on an end-to-end basis. In the scenario in Figure 92: Non-MCDN trunks on page 446, the system does not optimize the call.

Station A calls Station B. The call tandems through Node 2. Station B answers the call and transfers the call to Station C. The system has no direct MCDN TIE between Node 2 and Node 3. The system does not optimize the call.

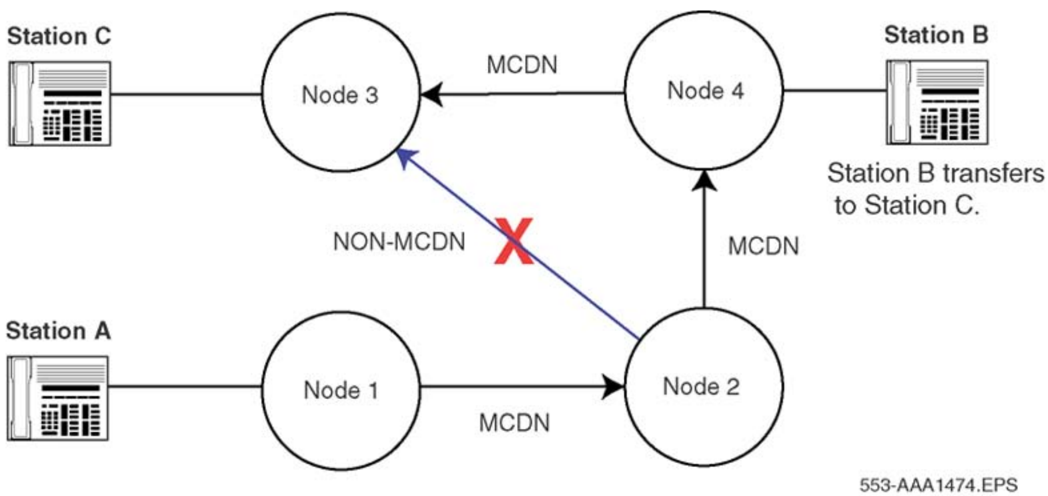

Figure 92: Non-MCDN trunks

Route access code

The system attempts TRO-CM only when the system makes the call through the Electronic Switched Network (ESN) UPD or CDP. TRO-CM does not support calls initiated with a route access code.

Feature interactions

TRO-BA feature interactions

With the exception of those discussed here, call redirection features are not affected or supported.

Call Forward Forwarding

If you configure the database to use the forwarding set Class of Service when a call is redirected (OPT = CFF in OVL 15), the originating set Class of Service can restrict an optimized call to the redirection DN, and the redirecting Class of Service can allow the call to be completed.

Attendant calls

Attendant extended calls for TRO-BA are shown in the following:

- Station A, a DID trunk call, or an incoming trunk calls the attendant. The attendant extends the call to Station B, which has NCFAC, NHUNT, to Station C. The system optimizes the call to Station C. Refer to Attendant extended call.

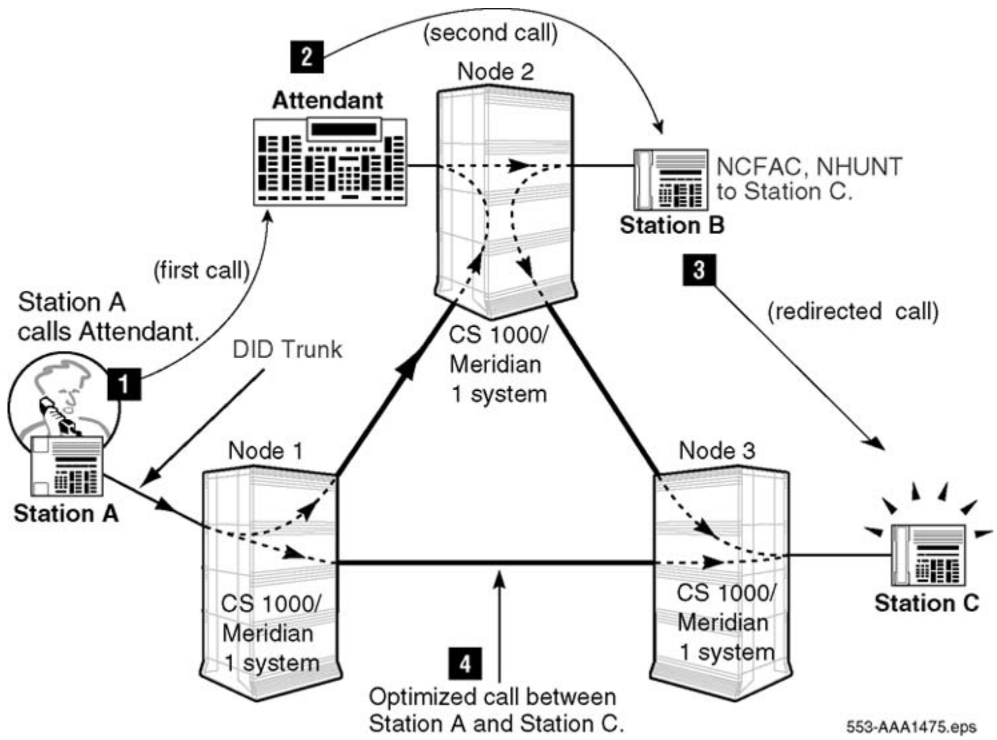

Figure 93: Attendant extended call

- The attendant extends a DID trunk or an incoming trunk call to Station B. The attendant does not release the call. Station B utilizes NCFAC to Station C. After three rings, the call forwards to Station C, and the attendant releases the call. The system optimizes the call to Station C. Refer to Attendant Controlled Call.

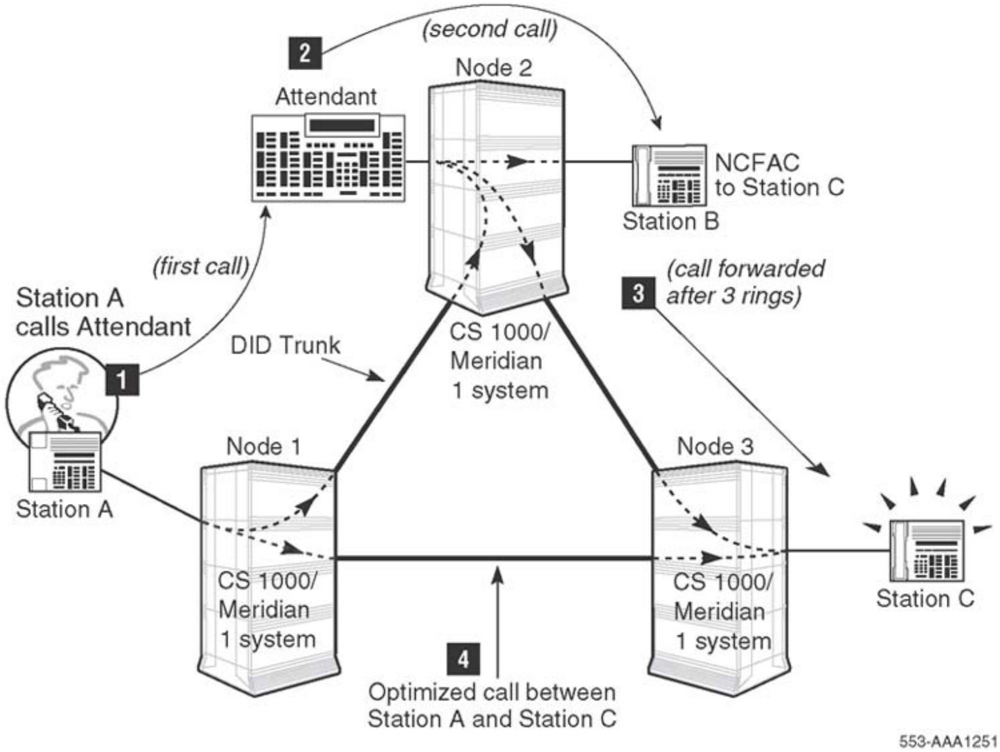

Figure 94: Attendant Controlled Call

BARS/NARS

BARS/NARS operation is not changed. BARS/NARS is used to determine route availability to terminate the optimized call. TRO-BA only supports the UDP and the CDP. Direct Trunk Access Codes are not supported.

Call Forward

Trunk Route Optimization before transfer

The system triggers TRO-BA before the terminating party answers the call when a call originating from a Transfer key (that is, the incoming call is in a held state and a new call is originated using the Transfer key) encounters call forward (for example, Call Forward All Calls, Call Forward Busy, and Hunt).

For example, in Trunk Route Optimization before transfer, Station A calls Station B. Station B initiates the transfer to Station C. Call forward is active on Station C on Node 3. All calls forward to Station D on Node 4. Node 3 sends the TRO-BA offer to Node 2. Node 2 accepts the offer, drops the old connection, and sets up a new connection between Node 2 and Node 4.

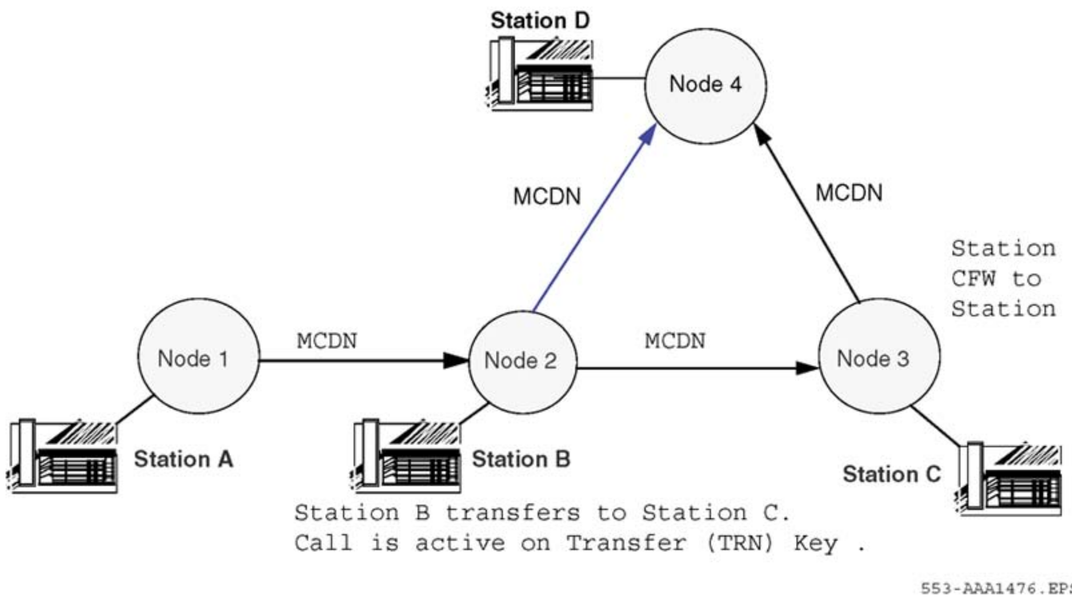

Figure 95: Trunk Route Optimization before transfer

Call Forward No Answer

Trunk Route Optimization before transfer

TRO-BA on Transfer (TRN) key

TRO-BA optimizes calls originated from the TRN key.

For example, in TRO-BA on TRN key, Station A calls Station B. Station B initiates the transfer to Station C. Station C is Call Forward No Answer (CFNA) to Station D. Upon CFNA timer expiry, while Station A is still in a held state, Node 3 sends the TRO-BA request to Node 2. Node 2 accepts the TRO-BA offer, drops the old connection and sets-up a new direct connection from Node 2 to Node 4 on the TRN key.

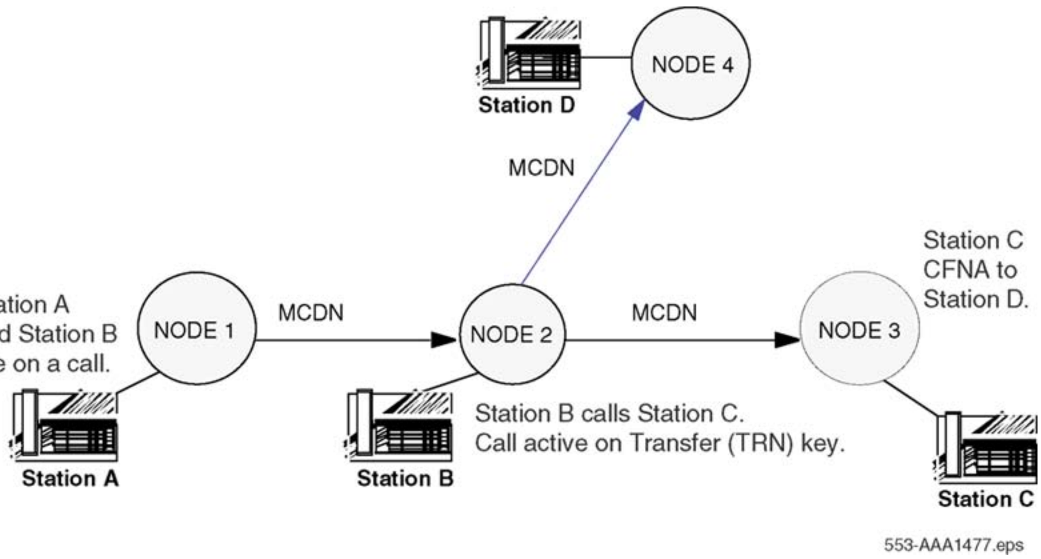

Figure 96: TRO-BA on TRN key

Trunk Route Optimization after blind transfer

The system triggers TRO-BA when CFNA follows blind transferred calls. For example, in [Figure 97: Blind transfer followed by CFNA](#) on page 451, Station A calls Station B. Station B performs a blind transfer to Station C. CFNA is active on Station C. All calls Forward No Answer to Station D. Upon CFNA timer expiry, the TRO-BA offer is sent to Node 1. Node 1 accepts the TRO-BA offer, drops the old connection, and sets-up a new direct connection from Node 1 to Node 4.

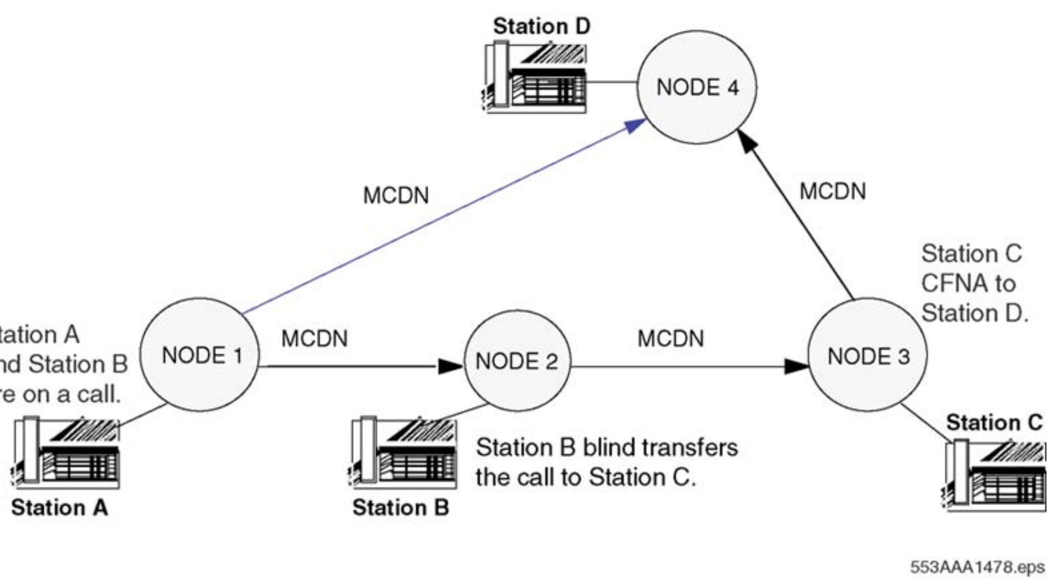

Figure 97: Blind transfer followed by CFNA

Call Party Name Display

When the system optimizes a call, the name or number does not appear on the receiving party's display.

Dialed Number Display

Calls modified by NCRD and TRO-BA can affect the display results on the answering phone. The dialed number/name does not appear on the called phone's display.

EuroISDN Trunk - Network Side

If the call originated from a EuroISDN Trunk - Network Side connectivity interface, the MCDN does not support Trunk Route Optimization-Before Answer.

Network Call Forward by Call Type (NCFCT)

For calls containing Calling Line Identification (CLID) in the setup message, the numbering plan type identified within the setup message supersedes the RCLS prompt. Incoming trunk calls answered at Node A, prior to entering the TIE trunk link using call modification, contain a CLID as a result of the call modification. This modification can result in internal call treatment at the terminating node.

Refer to the NCRD examples on Figure 57: Example of TRO-BA when NCRD is enabled on each node on page 415 Trunk Anti-Tromboning on page 417. Consider the NCRD feature when configuring the network.

Network Call Redirection (Network Call Forward All Calls [NCFAC], Network Call Forward No Answer [NCFNA], Network Hunt (NHNT))

TRO-BA depends on NCRD messages over the D-channel. Allow NCRD for all routes targeted for TRO-BA calls. When TRO-BA redirects a call, the originating node receives the redirecting information. The originating node suspends the redirection, and establishes a direct connection. If a route is not available when the call is placed, the call can be blocked.

Network Call Transfer

Trunk Route Optimization does not operate for Network Call Transferred calls. Station and attendant extended calls do not utilize TRO-BA.

Network Message Service

TRO-BA occurs when the node activates the Meridian Mail Call Sender. Through dialing or operator revert features do not provide the DN to Meridian Mail. Therefore, optimization does not take place. The original called-party information included in the setup message determines where Meridian Mail terminates the call.

Radio Paging (RPA) Calls

Trunk Optimization does not occur when RPA is involved in the call.

TAT feature interactions

If you configure TRO-BA and TAT on the same system, TRO-BA takes precedence over TAT.

Note:
For the TAT features described in this section, assume that you configured only the TAT feature (and not TRO-BA) on the system.

Attendant

If an attendant activates Busy Verify or Barge-in at the same time that the system receives a message to invoke TAT, the system aborts the Anti-tromboning operation.

Automatic Call Distribution (ACD)

The Trunk Anti-Tromboning feature performs anti-tromboning operations to eliminate the PRI trunks associated with the same D-channel due to the following ACD operations:

- Enhanced Network Call Forward
- Network ACD
- Interflow Options
- Enhanced Interflow

If a supervisor attempts to observe an ACD agent at the same time the system receives a message to invoke TAT, the system aborts the Anti-tromboning operation.

If a Recorded Announcement (RAN) answers an incoming PRI call in the ACD queue, the system only performs the Anti-tromboning operation after an ACD agent answers the call.

Call Park Network Wide

If you program the feature at all the interim Private Branch Exchanges (PBXs) in the call, the system invokes the Trunk Anti-Tromboning feature.

Conference

If the system activates the Conference feature, the Trunk Anti-Tromboning feature only performs the anti-tromboning operations when two parties:

- remain in the call
- use PRI trunks associated with the same D-channel

Figure 98: Conference call before TAT on page 454 shows a conference call before TAT:

- Station A or an incoming DID trunk call at the originating node is connected to Station B at the terminating node over a PRI/ISL/VNS or analog trunk (first call).
- Station B conferences in Station C, also located at the originating node, over a second PRI/ISL/VNS or analog trunk that is associated with the same D-channel as the first call.
- For the duration of the three-party conference call, the two trunks are tromboned.

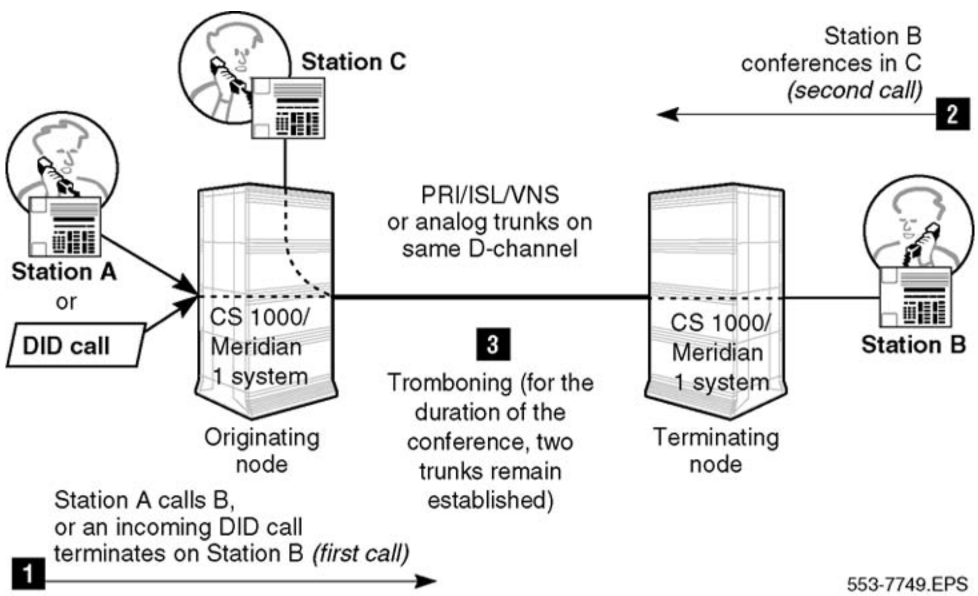

Figure 98: Conference call before TAT

When Station B drops out of the conference, the system invokes anti-tromboning. The system does not invoke TAT as long as the conference call situation exists. The two tromboned trunks are released. The system software bridges Station A or the DID trunk, and Station C. Refer to Conference call after TAT.

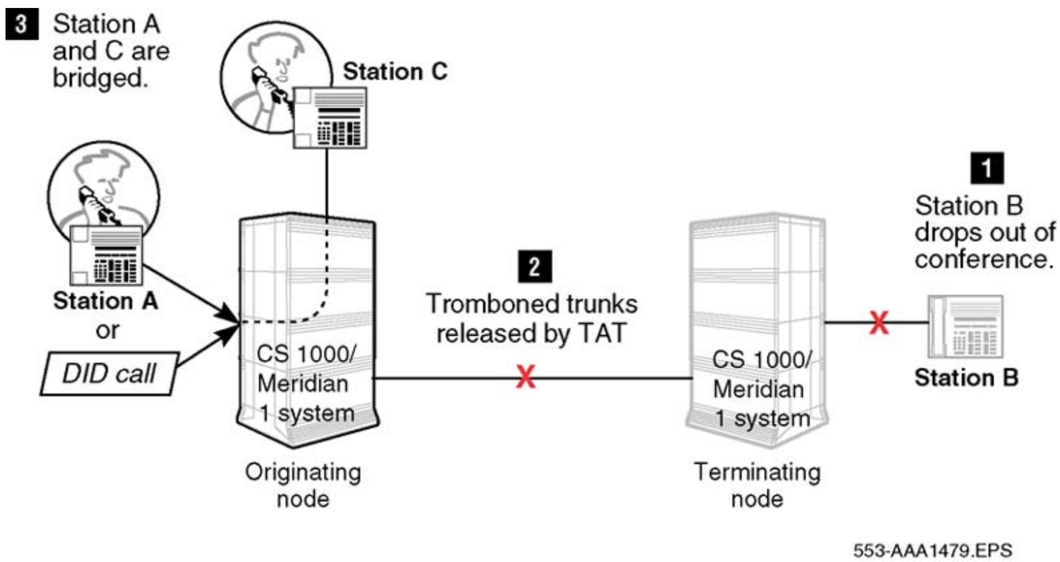

Figure 99: Conference call after TAT

End-To-End Signaling

If End-To-End Signaling is present when the system invokes TAT, the system aborts anti-tromboning.

External Recorded Announcement.

If an attendant originates a call, which through call modification or call redirection creates tromboned trunks and eventually terminates on an external RAN announcement, TAT does not optimize the trunks.

INIT ACD Queue Call Restore

The system does not support Trunk Anti-Tromboning on a call restored by INIT ACD Queue Call Restore.

Internal Call Forward (system to system)

TAT does not affect the operation of Internal Call Forward between two systems while applying anti-tromboning to trunks. Refer to Figure 100: Internal Call Forward before TAT on page 456:

- Station A or an incoming TIE trunk on Node 1 calls Station B at Node 2. The call routes to Station B at Node 2 over a PRI/ISL trunk (first call).
- Station B on Node 2 is call forwarded to Station C on Node 1 (redirected call). The trunks are tromboned.
- If the call is determined to be internal, and Station C is Internal Call Forwarded to Station D, the call is automatically forwarded to Station D on Node 2 over a third PRI/ISL trunk.

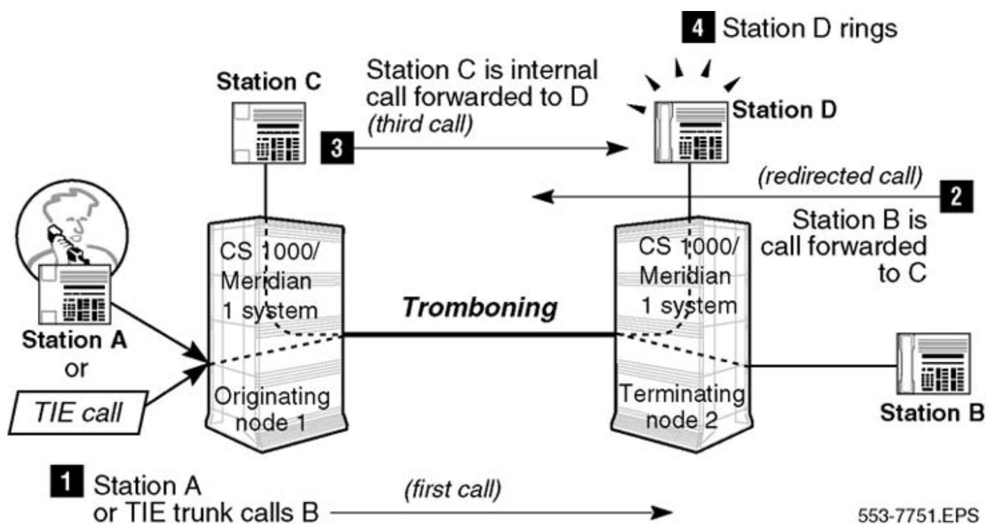

Figure 100: Internal Call Forward before TAT

- After Station D answers the call, TAT releases the tromboned trunks between Node 1 and Node 2. Refer to Internal Call Forward after TAT.

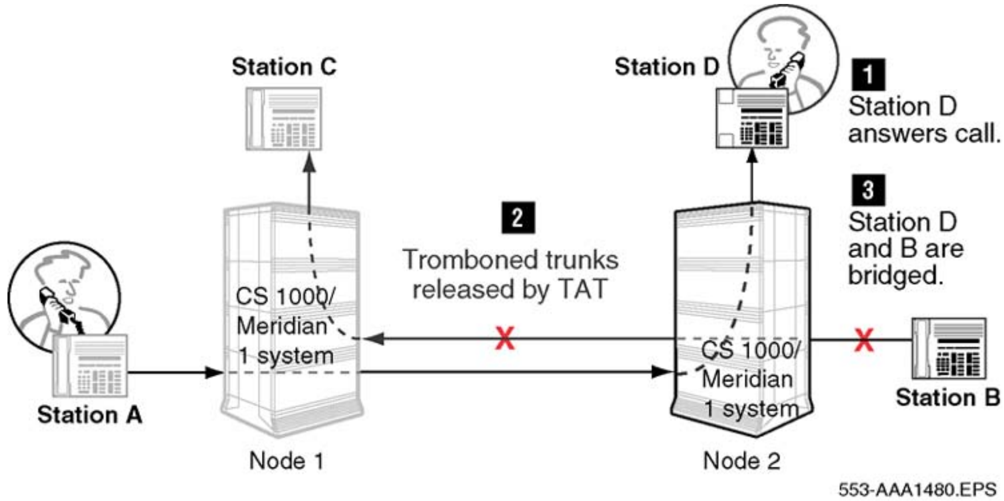

Figure 101: Internal Call Forward after TAT

Meridian Mail

The TAT feature releases tromboned PRI/ISL/VNS trunks arising from the application of the Auto Attendant, Thru-Dialing, and Operator Revert capabilities of Meridian Mail.

If Network Message Services is activated, the associated Call Sender capability does not require an additional trunk when it is activated. Therefore, the system does not apply TAT.Figure 102: Call Sender operation with Network Message Services active on page 458 shows Call Sender operation with Network Message Services active.

- Station A on Node 1 retrieves a message from a Meridian Mail station located on Node 2.
- The system activates Call Sender with Station B (the sender) located on Node 1.
- Station A directly conferences in Station B. The system establishes a conference between Station A, Station B, and the Meridian Mail station over one PRI/ISL/VNS trunk.

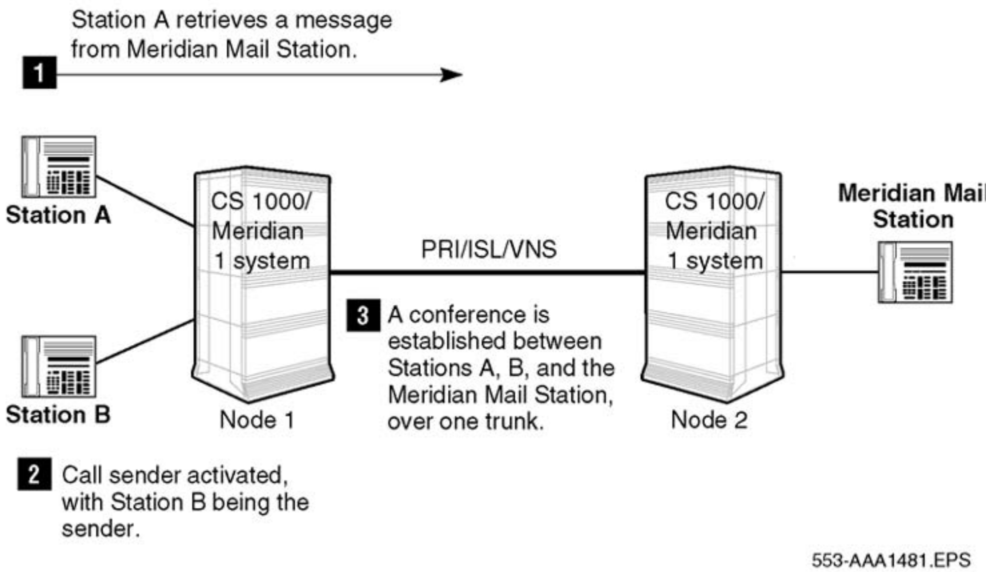

Figure 102: Call Sender operation with Network Message Services active

Network Attendant Service (NAS)

If you equip both TAT and NAS in a system network, and if you equipped NAS end-to-end, the NAS feature takes precedence over TAT. NAS and TAT do not interwork. Refer to Figure 103: NAS and TAT interworking on page 459 for the following calling scenarios.

Scenario 1

Station C at Node 2 calls the attendant at the remote Node 3 over a PRI trunk. The attendant extends the call to Station D at Node 2 over a separate PRI trunk. These trunks are tromboned.

Case 1 - TAT and NAS are equipped on all nodes

The NAS functionality drops the tromboned trunks, and the system bridges Station C and Station D when Station D answers.

Case 2 - NAS is not equipped

If you did not equip the system with NAS, TAT performs anti-tromboning operations by removing the tromboned trunks and bridging Station C and Station D.

Scenario 2

Station A at Node 1 calls the attendant at Node 3. The attendant extends the call to Station B on Node 1.

Case 1 - TAT and NAS are equipped on all nodes

If you equipped NAS and TAT between Node 1 and Node 2, and between Node 2 and Node 3, then NAS takes precedence over TAT to optimize the tromboned trunks between Node 1 and Node 2, and between Node 2 and Node 3.

Case 2 - NAS is not equipped

If you only equipped TAT between Node 1 and Node 2, and between Node 2 and Node 3, then TAT releases the tromboned trunks between Node 1 and Node 2, and between Node 2 and Node 3.

Case 3 - NAS is equipped between Node 1 and Node 2, and TAT is equipped between Node 2 and Node 3

If you only equipped NAS between Node 1 and Node 2, and equipped TAT between Node 2 and Node 3, then TAT releases the tromboned trunks between Node 2 and Node 3. The call is bridged at Node 2. NAS does not optimize the tromboned trunks between Node 1 and Node 2.

Case 4 - TAT is equipped between Node 1 and Node 2, and NAS is equipped between Node 2 and Node 3

If you only equipped TAT between Node 1 and Node 2, and only equipped NAS between Node 2 and Node 3, the system does not perform anti-tromboning because you did not equip NAS end-to-end.

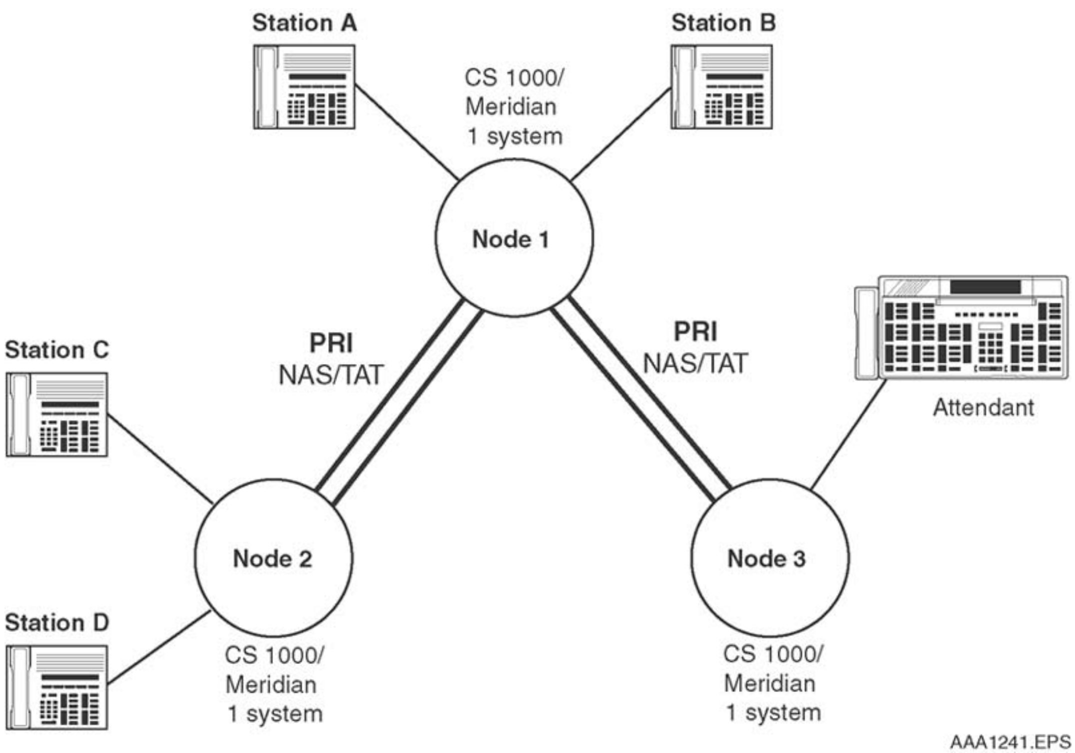

Figure 103: NAS and TAT interworking

Network Call Pickup

The TAT feature optimizes tromboned trunks arising from the operation of the Network Call Pickup feature. For example, in Figure 104: Network Call Pickup before TAT on page 460, Station A on Node 1 makes a call to Station B on Node 2 over a PRI/ISL/VNS or analog trunk. Station C on Node 1 picks up the call over a separate PRI/ISL/VNS or analog trunk. After

Station C picks up the call, TAT applies anti-tromboning to release the two tromboned PRI trunks. The system connects Station A and Station C locally. Refer to Figure 105: Network Call Pickup after TAT on page 460.

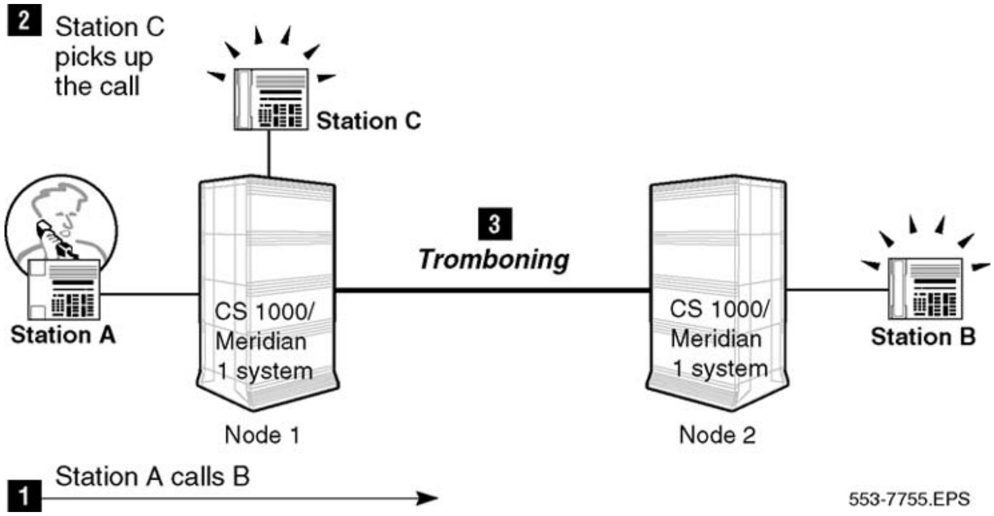

Figure 104: Network Call Pickup before TAT

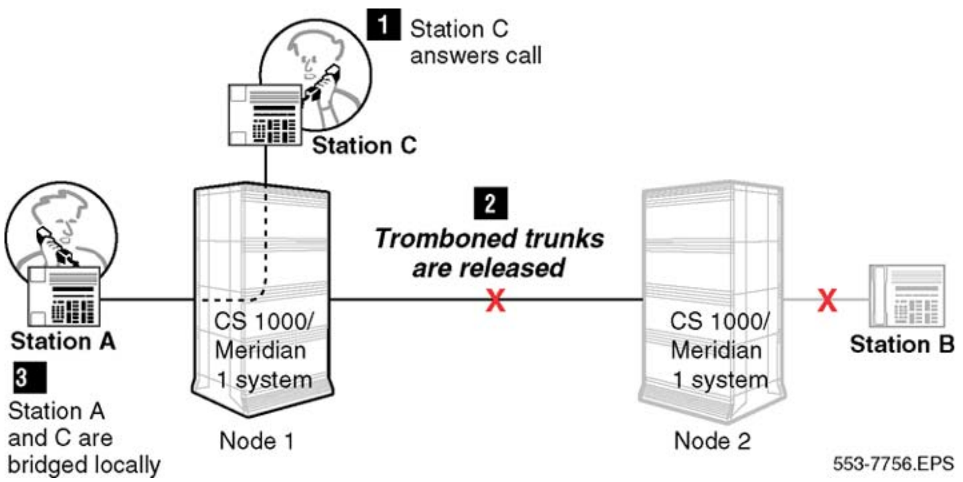

Figure 105: Network Call Pickup after TAT

Network Call Redirection

The Trunk Anti-Tromboning feature eliminates the tromboning of PRI/ISL/VNS or analog trunks resulting from the operation of the following NCRD features:

- Network Call Forward Unconditional
- NCFNA
- Network Call Forward Busy

- Network Call Forward by Call Type
- NHNT
- Internal Call Forward

Figure 106: NCRD before TAT on page 461 illustrates the following scenario:

- Station A (on the originating node) calls Station B (on the terminating node) across a tandem node over a PRI/ISL/VNS trunk (first call).
- Station B is call forwarded or hunts over another PRI/ISL/VNS trunk to Station C located on a tandem node (redirected call). This causes tromboning between the terminating node and the tandem node.

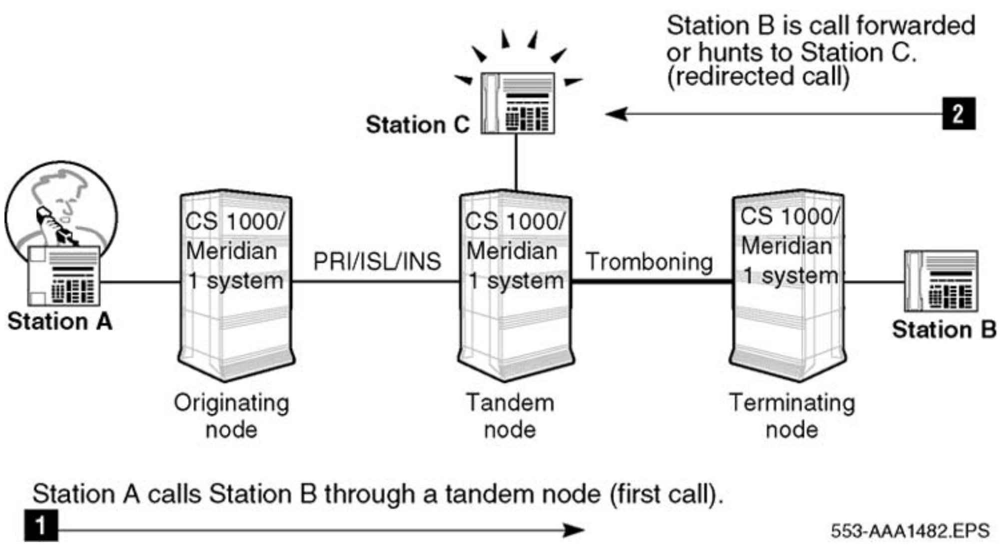

Figure 106: NCRD before TAT

The system invokes anti-tromboning after Station C answers. This causes the release of the tromboned trunks. The tandem node connects Station A and Station C. Figure 107: NCRD after TAT on page 462 shows the results of this anti-tromboning.

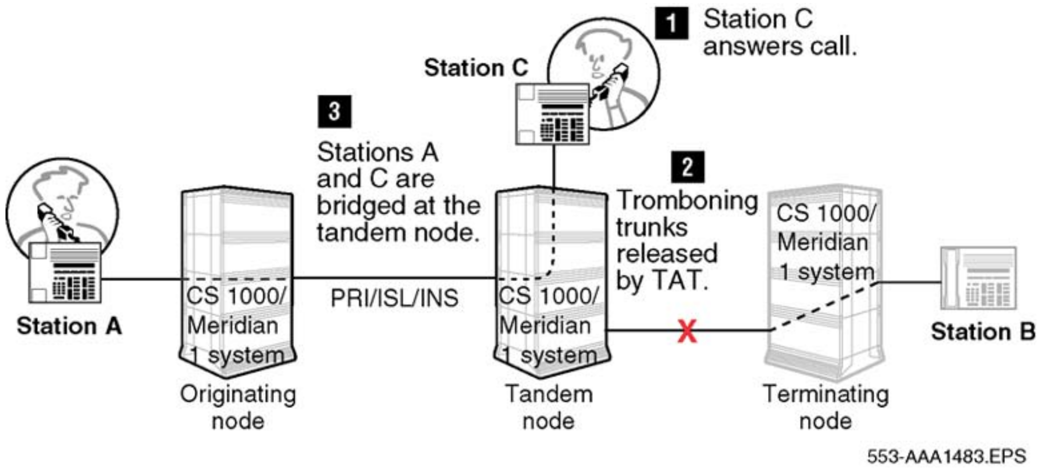

Figure 107: NCRD after TAT

Radio Paging System

If an attendant originates a call, which through call modification or call redirection, creates tromboned trunks, and eventually terminates on Radio Paging equipment, TAT does not optimize the trunks.

Trunk Route Optimization - Before Answer

See TAT and TRO-BA equipped on the same system on page 419.

Virtual Network Services

The TAT feature performs anti-tromboning operations to eliminate tromboned trunks (physical B-channels) associated with the same VNS D-channel. In Figure 108: VNS before TAT on page 463, Station A, at the originating node, calls Station B, at the terminating node, over a VNS D-channel trunk. Station B transfers the call to Station C, at the originating node. The physical B-channel trunks associated with the D-channels are tromboned.

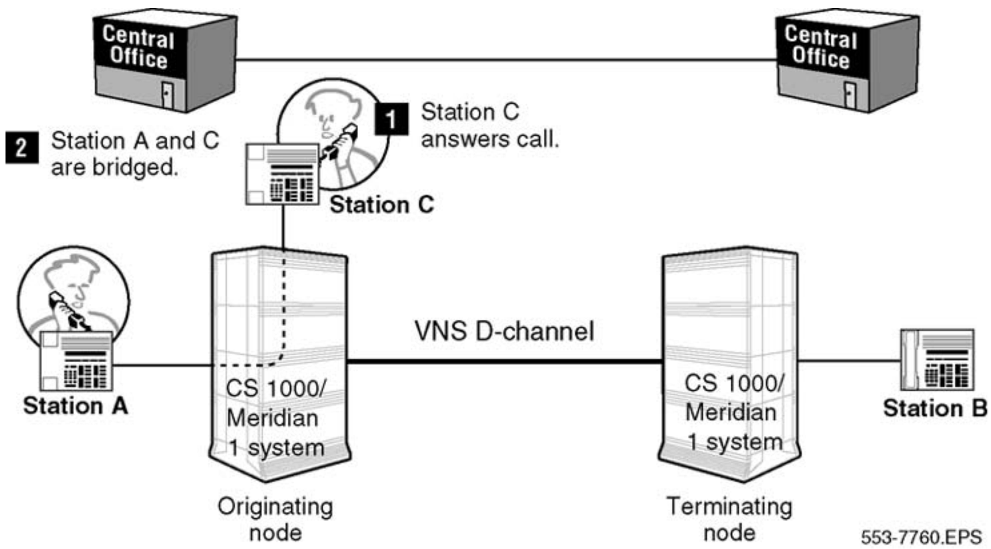

Figure 108: VNS before TAT

After Station C answers, the tromboned trunks are released, and Station A and Station C are bridged. Refer to Figure 109: VNS after TAT on page 463.

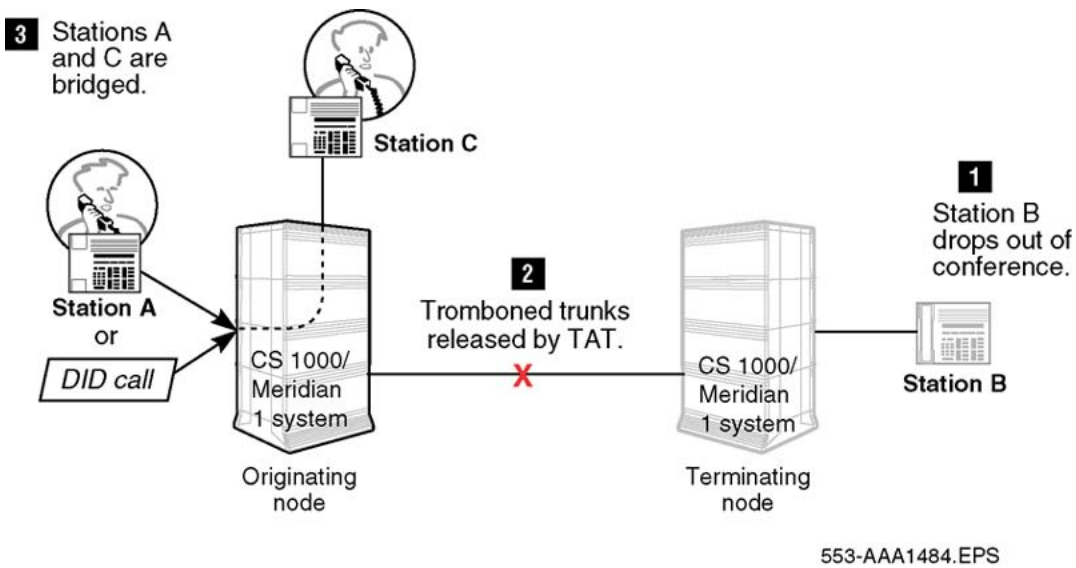

Figure 109: VNS after TAT

TRO-CM feature interactions

Networkwide Break-in

The system does not optimize any call that is a result of pre-dial or post-dial break-in. If the call is eligible for TRO-CM after break-in, the system attempts optimization (for example, calls transferred or attendant extended calls).

In Figure 110: Attendant Break-In on page 464, Station C is on a call with Station D. Station A calls the attendant on Node 2. The attendant performs a pre-dial or post-dial break-in to Station C. This does not trigger TRO-CM.

The attendant completes the extension of the incoming call when Station D disconnects. The system treats the call as a normal modified call. The system triggers TRO-CM from Node 3.

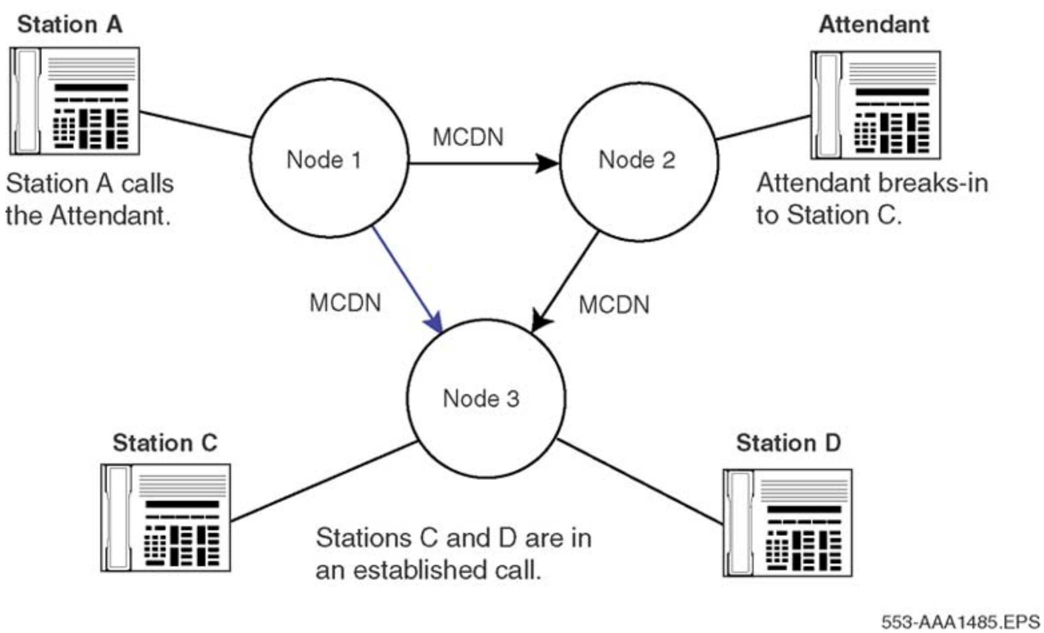

Figure 110: Attendant Break-In

If the attendant attempts break-in on Station C on the TRO-CM destination node before the new setup message is received, the system aborts TRO-CM. See Figure 111: Before TRO-CM operation on page 465.

When TRO-CM is in progress on the TRO-CM destination node, and when the original path and the new path are in conference, break-in is not possible.

When the system receives the TRO-CM Trigger on the originating node and Station A is broken-into, the system rejects TRO-CM due to the terminated status of the call. See Figure 111: Before TRO-CM operation on page 465.

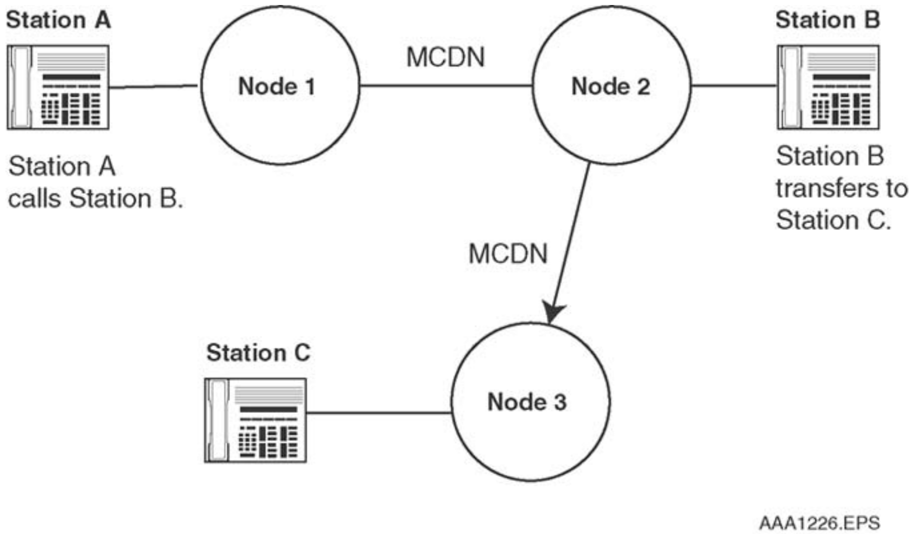

Figure 111: Before TRO-CM operation

Automatic Call Distribution (ACD)

The system triggers the TRO-CM feature when the ACD agent at the TRO-CM destination node answers the call.

Barge-in

Barge-in calls are attendant-originated. They do not optimize.

Call Detail Recording

In Figure 112: Triangulation on page 466, Station A calls Station B. Station B transfers the call to Station C. Station C answers the call. Station B completes the transfer. The system triggers TRO-CM, and sets-up a new connection between Node 1 and Node 6 through Node 4.

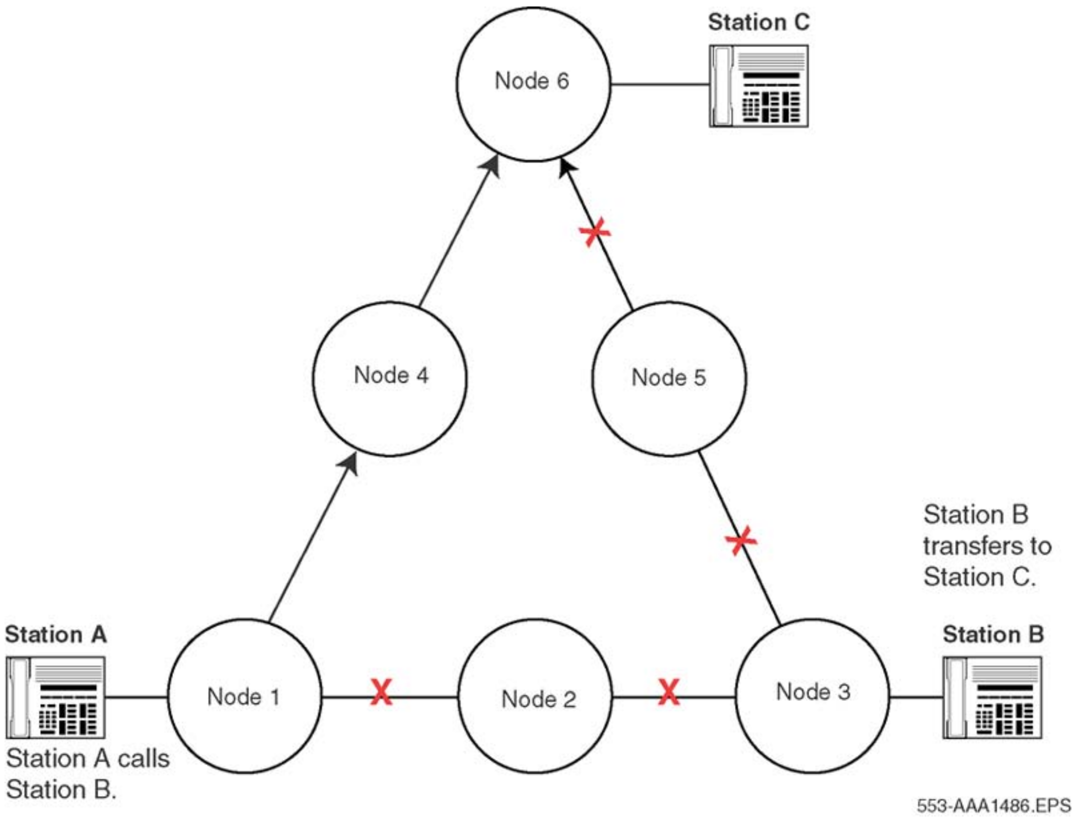

Figure 112: Triangulation

Old path disconnect

The following occurs during TRO-CM when the system disconnects the old path (refer to Figure 112: Triangulation on page 466):

- The TRO-CM originating node and TRO-CM destination node (Node 1 and Node 6) do not print CDR records for the old connection.
- The tandem nodes (Node 2 and Node 5) print CDR information that shows the release of the old connection.
- Node 3 prints an end record to indicate the release of the old connection.

Cleared call between Station A and Station C

The following occurs when the system clears the call between Station A and Station C (refer to Figure 112: Triangulation on page 466):

- The CDR records printed on Node 1 and Node 6 indicate the call started when the system made the old connection. Node 1 displays Station A (the originator of the new connection) as the originator of the old connection. Node 6 displays Station C (the terminator of the new connection) as the terminator of the old connection. See Figure 112: Triangulation on page 466.
- Node 4 (tandem node) prints CDR information that shows the release of a connection, which started when the new connection was made.

Call Forward

Trunk Route Optimization after transfer

When Call Forward Busy, Call Forward All Calls, and Call Forward Hunt follow a blind or supervised transfer, the system only triggers TRO-CM after the terminating party answers the call.

For example, in Figure 113: Trunk Route Optimization after transfer on page 467, Station A calls Station B. Station B initiates a transfer to Station C. CFNA is active on Station C. All calls Forward No Answer to Station D. Station D answers the call, then Station B completes the transfer. TRO-CM optimizes the call between Station A and Station D.

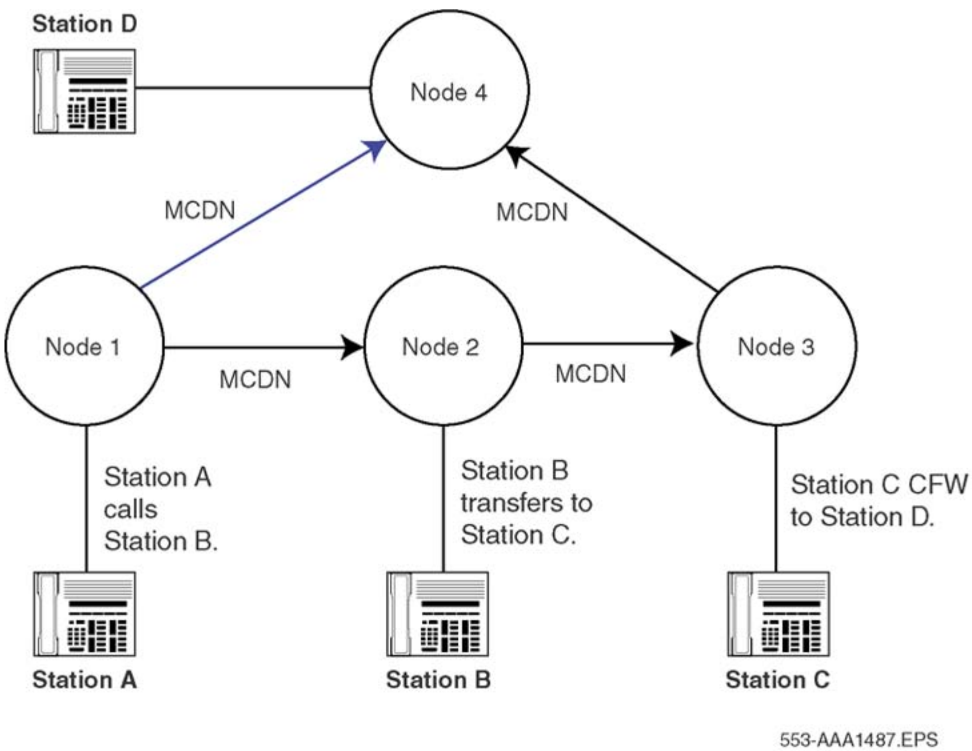

Figure 113: Trunk Route Optimization after transfer

Supervised transfer

The system triggers TRO-CM upon answer, only if CFNA follows a supervised transfer. The system optimizes CFNA calls only on answer.

In Figure 114: Supervised transfer followed by CFNA on page 468, Station A calls Station B. Station B initiates a transfer to Station C. CFNA is active on Station C. All calls Forward No Answer to Station D. Station D answers the call. Station B completes the transfer. TRO-CM optimizes the call between Station A and Station D.

However, if Station B performs a blind transfer to Station C, the system does not trigger TRO-CM.

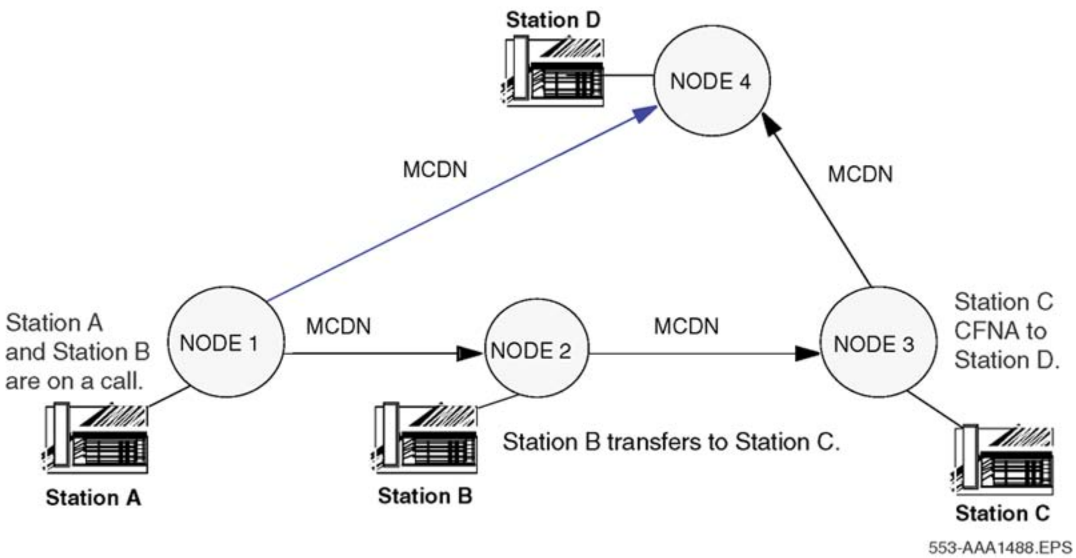

Figure 114: Supervised transfer followed by CFNA

Note:

The system optimizes calls originating from Conference keys (Three Party Conference key [A03], Six Party conference key [A06], and No Hold Conference key [NHC]). In the example in Figure 115: Trunk Route Optimization before transfer on page 468, the system does not trigger TRO-CM when a transfer is in progress. When the transfer is completed, a new connection is set up from Node 1 to Node 4.

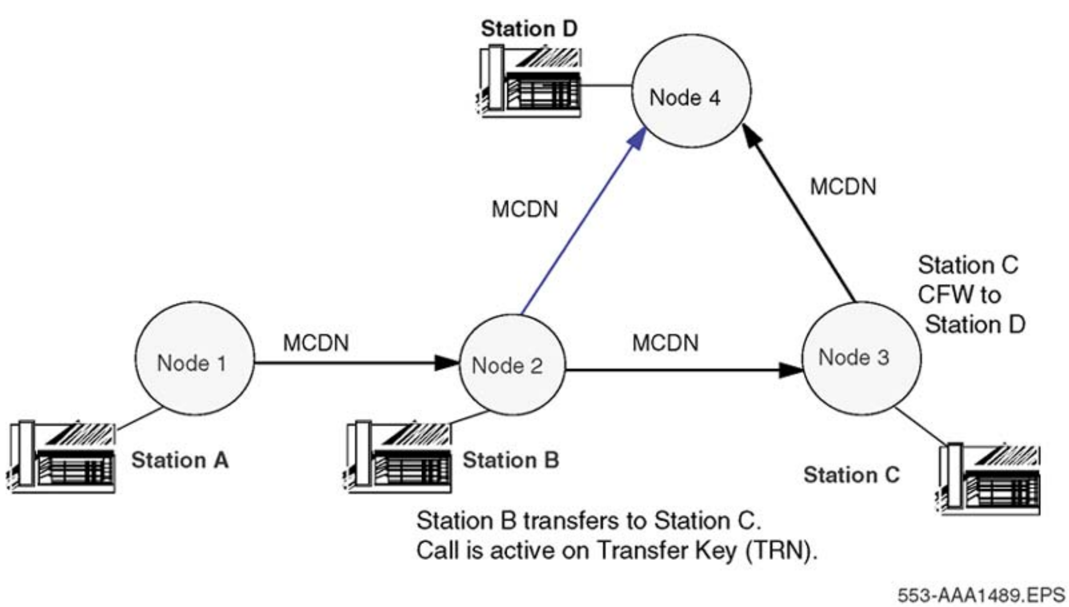

Figure 115: Trunk Route Optimization before transfer

Call Hold

The system aborts the TRO-CM operation when the terminating party or originating party attempts to put a call on hold.

If the call on the TRO-CM originating node is on hold when the TRO-CM Trigger is received, the system rejects TRO-CM due to the non-terminated status of the call.

Call Park

The system does not optimize Parked calls. For example, when Station A on Node 1 calls Station B on Node 2, Station B transfers the call to Station C on Node 3. Station C parks the call. Station B completes the transfer. The system does not trigger TRO-CM.

When Station A on Node 1 calls Station B on Node 2, Station B initiates a transfer to Station C on Node 3. Station B completes the transfer. The system triggers TRO-CM. When Station C attempts to park the call, the system aborts the TRO-CM process.

If Station A parks the call on the TRO-CM originating node when the TRO-CM trigger is received, the request is rejected.

If station A parks the call on the TRO-CM originating node, the destination node rejects the request when the originating node receives the TRO-CM trigger.

If Station A attempts to park the call when a TRO-CM setup facility has been sent to the TRO-CM destination node, the system cancels the TRO-CM operations.

Network Call Pick-up

The system does not optimize picked-up calls. For example, Station A on Node 1 calls Station B on Node 2. Station B initiates a transfer to Station C on Node 3. While Station C is ringing, B completes the transfer. Station D (on the same node or on a different node) picks up Station C's call. The system does not trigger TRO-CM. See Figure 115: Trunk Route Optimization before transfer on page 468.

The system triggers TRO-CM if Station B does a supervised transfer.

Call Transfer

When the system sends the trigger from the TRO-CM destination node and before the originating node receives the new setup, if Station C attempts to transfer the call, the system aborts TRO-CM operations. See Figure 111: Before TRO-CM operation on page 465. See Figure 111: Before TRO-CM operation on page 465.

When TRO-CM is in progress on the TRO-CM destination node, and when the original path and the new path are in conference, a transfer is possible.

If Station A on the TRO-CM originating node performs a transfer when the TRO-CM trigger is received, or completes the transfer before the TRO-CM trigger is received, the request is rejected.

When Station A attempts to transfer when a TRO-CM setup facility message is sent to the TRO-CM destination node, the system aborts TRO-CM operations.

The system updates the display on the phones when the system completes the transfer. The system invokes TRO-CM only after the system updates the display on the phones. TRO-CM does not alter the display of the users.

A local Call Transfer does not trigger a TRO-CM request.

Call Waiting

The system does not invoke TRO-CM on a waiting call. However, the system invokes TRO-CM, if eligible, when the intended party answers the waiting call.

For example, in Figure 111: Before TRO-CM operation on page 465, Station A calls Station B, if Station C is busy on another call. Station B attempts to transfer the call to Station C. Station B's call is waiting on Station C. This does not trigger TRO-CM. However, when Station C picks up the waiting call, the system triggers TRO-CM.

Camp-On

The system does not invoke TRO-CM on a camped-on call. However, the system invokes TRO-CM, if eligible, once the intended party answers the camped-on call.

For example, in Figure 110: Attendant Break-In on page 464, Station A calls the attendant on Node 2. Station C is busy on another call. The attendant camps the call on Station C. This action does not trigger TRO-CM. However, once Station C is free and answers the camped-on call, the system triggers TRO-CM.

Conference

The system does not send a TRO-CM request for a user involved in an established conference.

The system rejects any TRO-CM request from a destination node when the target station is in an established conference.

The system initiates TRO-CM when it releases the conference.

In Figure 116: Conference at the TRO-CM originating node on page 471, when Station D transfers (blind or supervised) to Station E, and Station E answers, Node 1 rejects the TRO-CM request and the system aborts TRO-CM.

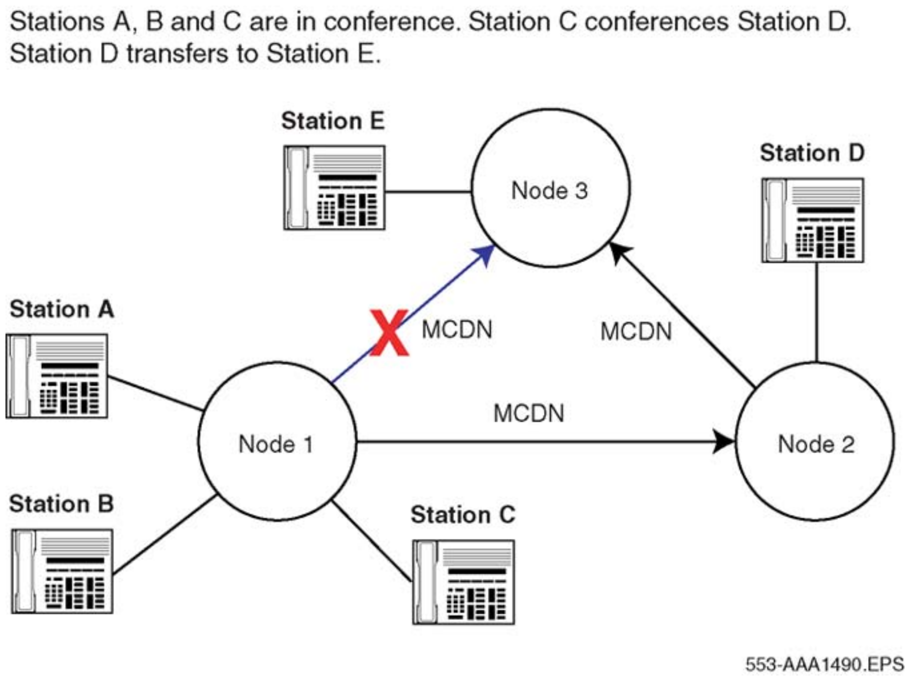

Figure 116: Conference at the TRO-CM originating node

In Figure 117: Conference at the TRO-CM destination node on page 472, Station A calls Station B. Station B initiates a transfer to Station C. Station C answers the call and conferences Station D. Station B completes the transfer. The system does not invoke the TRO-CM request.

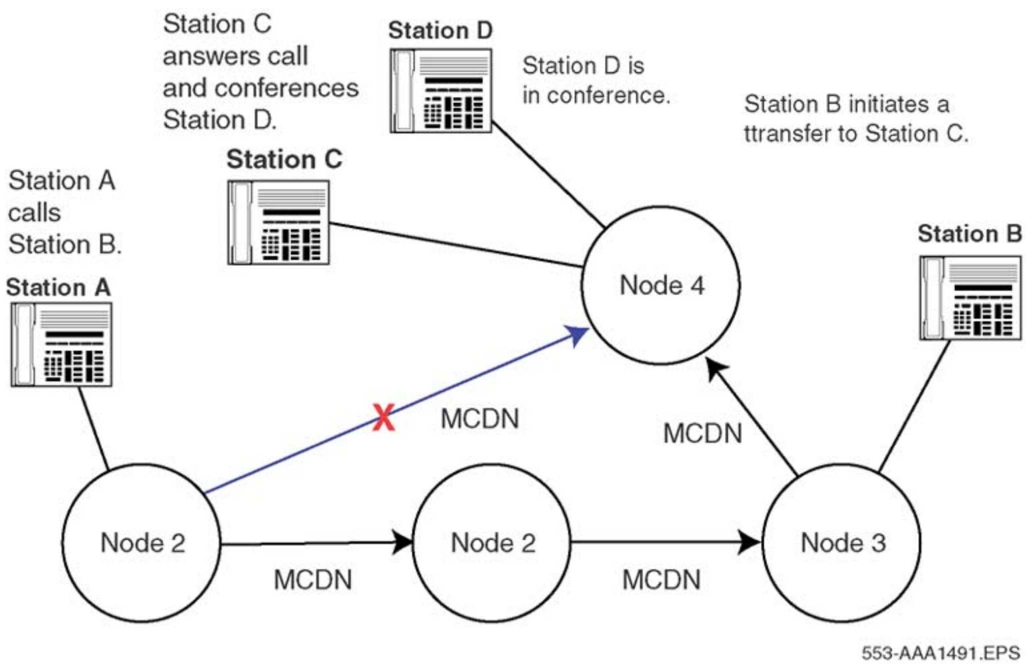

Figure 117: Conference at the TRO-CM destination node

End-to-End Signaling

The system delays TRO-CM when it detects the use of End-to-End Signaling. The TRO-CM destination node reattempts TRO-CM twice. If End-to-End Signaling completes within this time, TRO-CM is successful.

Music

If the system connects the call on the TRO-CM destination node to the Music trunk, the system does not trigger TRO-CM. The system temporarily rejects any call on a music trunk. The TRO-CM destination node reattempts TRO-CM twice. If the system withdraws Music from the call within this time, TRO-CM is successful.

Radio Paging

The system does not invoke TRO-CM on a paged call. Any request from the TRO-CM destination node is permanently rejected.

Recorded Announcement

If the system connects the call on the TRO-CM destination node to the RAN trunk, it does not trigger TRO-CM. If the TRO-CM destination node makes any request on a call that has RAN provided, the system rejects the request. The TRO-CM destination node reattempts TRO-CM twice. If the system withdraws RAN during this time, then TRO-CM is successful.

Feature packaging

The TRO-BA and TRO-CM features require Advanced Network Services (NTWK) package 148.

The Trunk Anti-Tromboning feature requires the following packages:

- Integrated Services Digital Network (ISDN) package 145
- Primary Rate Access (PRA) package 146 or Integrated Service Digital Network Signaling Link (ISL) package 147 or 2.0 Mbit Primary Rate Interface (PRI2) package 154 and optionally
- Advanced ISDN Network Services (NTWK) package 148
- Multi-purpose Serial Data Link (MSDL) package 222
- Trunk Anti-Tromboning (TATO) package 312

Example of TRO-BA in operation when ARDN = YES or NO shows an example of TRO-BA in operation when the ARDN feature is set to YES or NO.

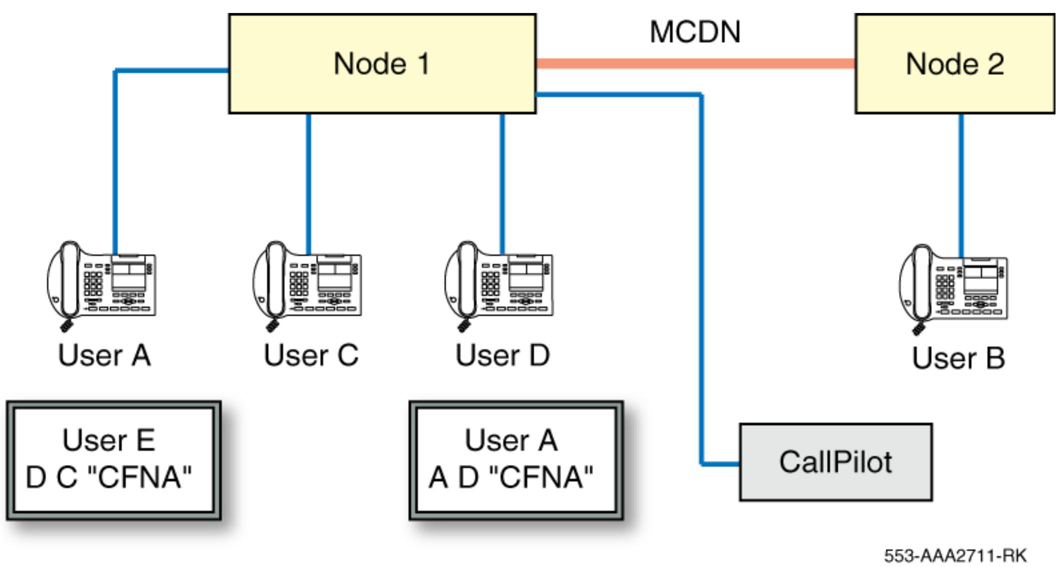

Figure 118: Example of TRO-BA in operation when ARDN = YES or NO

Figure 118: Example of TRO-BA in operation when ARDN = YES or NO on page 473illustrates the following:

- User A calls User D.
- User D sets Call Forward No Answer (CFNA) to User B.

- User B CFW to User C.
- TRO = YES on MCDN routes.
- If ARDN = YES or NO and CLS of all users are CNDA, NAMA, and DDGA.

The User C telephone displays DN of User A, followed by DN of User D, and the reason for redirection associated with the original redirection (CFNA) instead of DN of User A, followed by DN of User B, and the reason for redirection associated with the final redirection (CFW).

Note:
The ARDN feature is not effective when all the trunks are dropped due to TRO. Hence the terminating user telephone displays the originally called number (DN of User D) and not the last redirected number (DN of User B).

Feature implementation

TRO-BA and TRO-CM

The following is a summary of the tasks in this section:

1. Table 192: LD 16: Configure Trunk Route Optimization. on page 474

   Note:
   Configure TRO-BA and TRO-CM by setting TRO = YES in the Route Data Block. Configure TAT by setting RCAP = TAT in the D-Channel data block.

2. Table 193: LD 17: Configure ADAN. In the case of a VNS D-channel, make the required change to ADAN. on page 475

   Note:
   Configure the RLI entry 0 as the direct route to the destination node. The system chooses the RLI entry 0 to route the new optimized call. If a direct route is not possible, configure the shortest route to reach the destination node.

Table 192: LD 16: Configure Trunk Route Optimization.

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	RDB	Route Data Block
CUST		Customer number

Prompt	Response	Description
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
ROUT		Route number
	0-511	Range for Large System , Media Gateway 1000B, and CS 1000E system.
DTRK	(NO) YES	Digital Trunk Route Must be YES to prompt ISDN
ISDN	(NO) YES	Integrated Services Digital Network
IFC	SL1	Interface type
NCRD	(NO) YES	Network Call Redirection. Allows Network Call Redirection messages to be sent (or blocks messages if NCRD = NO). Must be YES to prompt TRO.
TRO	YES	Trunk Route Optimization

Table 193: LD 17: Configure ADAN. In the case of a VNS D-channel, make the required change to ADAN.

Prompt	Response	Description
REQ	CHG	Change existing data
TYPE	ADAN	Change or add information to the data block
ADAN	CHG DCH xx	Action Device and Number
USR		User
	VNS SHAV	Virtual Network Services Shared Virtual Network Services
...		
VCRD	YES	Network Call Redirection Allowed
VTRO	YES	VNS TRO allowed

Timers

All TRO-CM timers implemented on the system are not service-changeable.

Table 194: TRO-CM Timers

Timer	Description	Value	Applicable node	Action on expiry
T1	Started by the TRO-CM destination node to protect	30s	TRO-CM destination	When timer T1 expires, the system sends TRO-CM

Timer	Description	Value	Applicable node	Action on expiry
	against the absence of a response to TROCMTrigger invoke Facility. The response can be a TROCMTrigger return error IE or a TROCMSetup invoke IE.			Trigger again. The system attempts TRO-CM twice. If the system does not succeed in the second attempt, all TRO-CM operations are cancelled.
T2	Started by the TRO-CM destination node to protect against failure to release the old connection.	20s	TRO-CM destination	The TRO-CM destination node disconnects the new connection on expiry.

TAT

Table 195: LD 17: Configure TAT functionality on the D-channel.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	ADAN	Action Device and Number.
- ADAN		
	NEW DCH x CHG DCH x	Add D-channel x. Change D-channel x.
- CTYP		Card type.
	MSDL	Multi-purpose Serial Data Link.
- PORT	0-3 1	Port number on MSDL cards.
...		
- IFC	SL1 S100 D100 D250	Interface type for D-channel.
...		
- RLS	xx	Release ID of the switch at the far end of the D-channel.
- RCAP	TAT	Remote Capabilities. TAT must be entered to enable Trunk Anti-Tromboning.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 51: Trunk to Trunk Connection

The Trunk to Trunk Connection feature introduces the following capabilities:

- transfer on ringing of external trunks across the network
- transfer of one supervised outgoing external trunk to another
- conference of external trunks
- outgoing trunk to trunk charging

These capabilities are available on an analog (500/2500-type) phone, Meridian 1 Proprietary Phone, or an Attendant Console.

Refer to *Avaya Features and Services Fundamentals, NN43001-106* for complete information.

Chapter 52: UIPE D-channel Monitoring Tool Enhancement

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The UIPE D-Channel Monitoring Tool Enhancement enables the Q.931 message monitoring to support the decoded message format. For enabled messages, it supports channel-based, message-based, and SET TN-based filtering.

The UIPE D-Channel Monitoring Enhancement modifies the monitor output so the debug option prints in three formats. It also removes the existing password protection for the Q.931 monitor.

If the monitor is enabled and the number of Call Registers in the idle queue drops below 10%, message monitoring is suspended. If the monitor is enabled and the number of idle call registers exceeds 10%, message printing starts again. For UIPE messages, the UIPE D-Channel Monitoring Tool Enhancement includes a real-time clock stamp on all messages printed on the terminal.

LD 96 introduces commands to support message filtering based on the ISDN TNs and the message type for Q.931 messages.

LD 96 also introduces a command to set filtering options for a D-channel based on terminals. This filtering option is a filtering paradigm that applies to UIPE proprietary messages and Q.931

messages. In the data block called MON_DATA, the system accepts TNs for phone-based filtering based on user input at new prompts. Phone-based filtering applies only to digital and analog terminals.

The LD 96 command that prints the monitor options status for a D-channel is modified to print the newly supported levels and options for the Q.931 messages.

For UIPE proprietary messages and Q.931 messages, the system provides the ON or OFF status of phone-based filtering.

Points of monitoring

Figure 119: Points of monitor on page 482 shows the two monitors available for the Meridian 1 and CS 1000M systems:

- Q.931 debug monitor for UIPE interfaces
- UIPE proprietary messages monitor (Internal Software Monitor)

Monitor category 1 (Debug Monitor) indicates messages exchanged between the Meridian 1 and CS 1000M systems and the external world (Q.931 messages). Monitor category 2 (Internal Software Monitor) indicates messages (UIPE proprietary) exchanged between system software and the Multi-purpose Serial Data Link (MSDL) card.

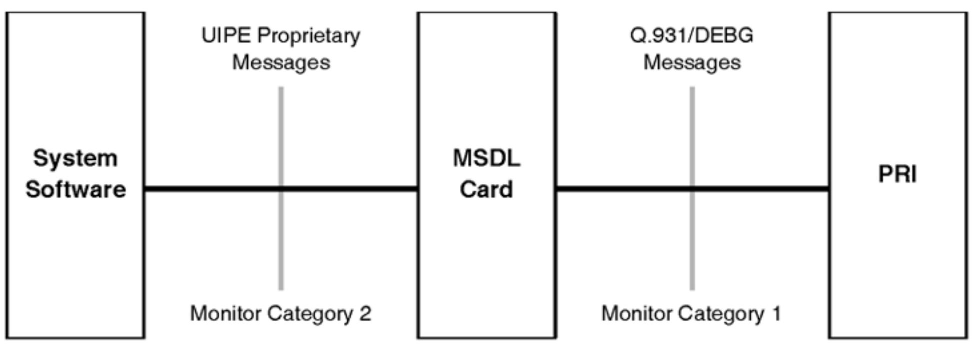

Figure 119: Points of monitor

Enhancement summary

Enhancement summary shows enhancements to the UIPE and Q.931 monitoring tool.

Table 196: Enhancement summary

Message Type	Monitor level			Based on		
	0	1	2	Channel	Message	Phone TN
Q.931	û	ü	û	û	û	û

Message Type	Monitor level			Based on		
	0	1	2	Channel	Message	Phone TN
UIPE	ü	ü	ü	ü	ü	û
ü Existing with continued support û Supported after enhancements						

Outgoing messages

Outgoing messages indicates the message mnemonics for outgoing messages for UIPE proprietary and Q.931 messages.

Table 197: Outgoing messages

Message Mnemonic	UIPE Proprietary
ALER	CC_ALERT_REQUEST
DISC	CC_DISCONNECT_REQUEST
FAC	CCC_FAC_REQUEST
FRNC	CC_FAC_REG_NULL_CRF
FJNC	CC_FACREJ_REQ_NULL_CRF
INFO	CC_INFORMATION_REQUEST
MIFO	CC_MORE_INFO_REQUEST
NOTF	CC_NOTIFY_REQUEST
PROC	CC_PROCEEDING_REQUEST
PROG	CC_PROGRESS_REQUEST
REJ	CC_REJECT_REQUEST
RLS	CC_RELEASE_RESPONSE
RLSR	CC_RELEASE_RESPONSE
STP	CC_SETUP_REQUEST
STPR	CC_SETUP_RESPONSE
STEN	CC_STATUS_ENQ_REQUEST
STAT	CC_STATUS_REQUEST
RST	CC_RESTART_REQUEST
RSTR	CC_RESTART_RESPONSE
SVC	SERVICE MESSAGES
SVCR	SERVICE RESPONSE

Message Mnemonic	UIPE Proprietary
RSTJ	CC_RESTART_REJECT

Incoming messages

Incoming messages indicates the message mnemonics for incoming messages for UIPE proprietary and Q.931 messages.

Table 198: Incoming messages

Message Mnemonic	UIPE Proprietary	Q.931 Messages	Support on Q.931
ALER	CC_ALERT_INDICATION	ALERTING	ü
DISC	CC_DISCONNECT_INDICATION	DISCONNECT	ü
FAC	CCC_FAC_INDICATION	FACILITY	ü
FIDC	CC_FAC_IND_NULL_CRF	FACILITY	ü
FJDC	CC_FACREJ_IND_NULL_CRF	FACILITY REJECT	ü
INFO	CC_INFORMATION_INDICATION	INFORMATION	ü
MIFO	CC_MORE_INFO_INDICATION	SETUP ACK	ü
NOTF	CC_NOTIFY_INDICATION	NOTIFY	ü
PROC	CC_PROCEEDING_INDICATION	CALL PROCEEDING	ü
PROG	CC_PROGRESS_INDICATION	PROGRESS	ü
RLSC	CC_RELEASE_CONFIRMATION	RELEASE COMPLETE	X
RLS	CC_RELEASE_INDICATION	RELEASE	ü
REJ	CC_REJECT_INDICATION	RELEASE COMPLETE	ü
STP	CC_SETUP_INDICATION	SETUP	ü
STPC	CC_SETUP_CONFIRMATION	CONNECT	ü
STEN	CC_STATUS_ENQ_INDICATION	STATUS ENQUIRY	ü
STAT	CC_STATUS_INDICATION	STATUS	ü
RST	CC_RESTART_INDICATION	RESTART	X

Message Mnemonic	UIPE Proprietary	Q.931 Messages	Support on Q.931
RSTC	CC_RESTART_CONFIRMATION	RESTART ACK	X
SVC	SERVICE MESSAGES	SERVICE	ü
SVCR	SERVICE RESPONSE	SERVICE RESPONSE	ü

Operating parameters

UIPE D-channel Monitoring Tool Enhancement is not applicable for BRI, because the debug option is not supported for BRI.

For phone-based monitoring, attendant consoles and ISDN terminals are not supported.

For phone-based filtering of messages, incoming calls to a phone are not supported.

For channel-based monitoring, the messages that do not have channel ID IE or call reference in the call reference table are not supported. This is also applicable for phone-based monitoring.

Note:
Messages that do not have channel ID IE or valid call references in the call reference table always have the channel number printed as NCAL in the message header.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

This feature requires the following packages:

- Integrated Services Digital Network (ISDN) package 145
- Primary Rate Access (PRA) package 146
- International Primary Rate Access (IPRA) package 154
- Multi-purpose Serial Data Link (MSDL) package 222

The UIPE D-Channel Monitoring Tool Enhancement does not introduce a software package.

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. LD 15 - Enter the TNs of the phones to be monitored (Set-Based Monitoring).
2. LD 96 - Enable or disable the monitor.
3. LD 96 - Query the status of the monitor and the filtering options.
4. LD 96 - Set monitor level.
    a. Mon. 0 for Craft level monitoring
    b. Mon. 1 for Raw format
    c. Mon. 2 for IE level decoded

Table 199: LD 15: Enter the TNs of the phones to be monitored (Set-Based Monitoring). on page 486

LD 15 accepts new data for phone-based monitoring. Enter the TNs of the phones to be monitored. If UIPE Set-Based Monitoring (USBM) is set to YES, the subsequent TN prompts are prompted. If USBM is set to NO, the values for the TN are cleared.

Note:
The TNs entered are data dumped and retained after sysload.

Table 199: LD 15: Enter the TNs of the phones to be monitored (Set-Based Monitoring).

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	MON	Monitoring
USBM	(NO) YES	Accept and prompt the next prompts if YES. If NO is entered, subsequent prompts are not prompted, and all the TNs configured earlier are flushed. If <CR> previously stored value taken.
TN1		Terminal Number 1

Prompt	Response	Description
	l s c u	Format for Large System , Media Gateway 1000B, and CS 1000E system where l = loop, s = shelf, c = card, u = unit.
TN2		Terminal Number 2
	l s c u	Format for Large System , Media Gateway 1000B, and CS 1000E system where l = loop, s = shelf, c = card, u = unit.
TN3		Terminal Number 3
	l s c u	Format for Large System , Media Gateway 1000B, and CS 1000E system where l = loop, s = shelf, c = card, u = unit.
TN4		Terminal Number 4
	l s c u	Format for Large System , Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
TN5		Terminal Number 5
	l s c u	Format for Large System , Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.
TN6		Terminal Number 6
	l s c u	Format for Large System , Media Gateway 1000B, and CS 1000E system, where l = loop, s = shelf, c = card, u = unit.

Table 200: LD 96: UIPE D-channel Monitoring Tool Enhancement commands on page 487

In LD 96 you can:

- Enable or disable the monitor.
- Query the status of the monitor and the filtering options.
- Set the monitor level.
  - Mon. 0 for Craft level monitoring
  - Mon. 1 for Raw format (Default)
  - Mon. 2 for IE level decoded

Table 200: LD 96: UIPE D-channel Monitoring Tool Enhancement commands

Command	Description
ENL MSGI <dch> DEBG MSG msg1 msg2 msg3	
	Enable the debugging of all monitored incoming messages from D-channel This command can be entered more than once. In one command, only 3 message mnemonics can be given.
ENL MSGO <dch> DEBG MSG msg1 msg2 msg3	

Command	Description
	Enable the debugging of all monitored outgoing messages from D-channel This command can be entered more than once. Only 3 message mnemonics can be given in one command.
DIS MSGI <dch> DEBG MSG msg1 msg2 msg3	Disable the debugging of all monitored incoming messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.
DIS MSGO <dch> DEBG MSG msg1 msg2 msg3	Disable the debugging of all monitored outgoing messages from D-channel. This command can be entered more than once. Only 3 message mnemonics can be given in one command.
ENL MSGI <dch> DEBG CH <loop><channel>	Enable the debugging of all monitored incoming messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.
ENL MSGO <dch> DEBG CH <loop><channel>	Enable the debugging of all monitored outgoing messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.
DIS MSGI <dch> DEBG CH <loop><channel>	Disable the debugging of all monitored incoming messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.
DIS MSGO <dch> DEBG CH <loop><channel>	Disable the debugging of all monitored outgoing messages from D-channel card. A maximum of 5 channels are monitored at a time. Only one channel number can be entered in one command.
ENL MSGI <dch> DEBG SET	Enable debug SET on all incoming messages from D-channel. This phone-based filtering is enhanced for UIPE proprietary messages.
ENL MSGO <dch> DEBG SET	Enable debug SET on all outgoing messages from D-channel. This phone-based filtering is enhanced for UIPE proprietary messages.
DIS MSGI <dch> DEBG SET	Disable debug SET on all incoming messages from D-channel. This phone-based filtering is enhanced for UIPE proprietary messages.
DIS MSGO <dch> DEBG SET	

Command	Description
	Disable debug SET on all outgoing messages from D-channel. This phone-based filtering is enhanced for UIPE proprietary messages.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 53: Virtual Network Services

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

The Virtual Network Services (VNS) feature offers a means to use Integrated Services Digital Network (ISDN) networking features when two systems are linked by a D-channel and an available Public Switched Telephone Network (PSTN) trunk exists. The PSTN trunks in this configuration serve as the B-channel for the call's duration.

VNS is an enhancement of the ISDN Signaling Link (ISL) interface. The enhancement allows the voice and the signaling of a call to take different physical paths. In the case of an ISL call, the D-channel is used for signaling, whereas the voice/data uses a TIE trunk (system to system connection only). The VNS feature extends the number of trunk types supported for the voice path by including the possibility of using different public trunks (for example, COT, DID, DOD).

Figure 120: VNS Interface/ISL Interface Comparison on page 492 depicts the difference between two nodes linked by an ISL interface and two nodes linked using VNS.

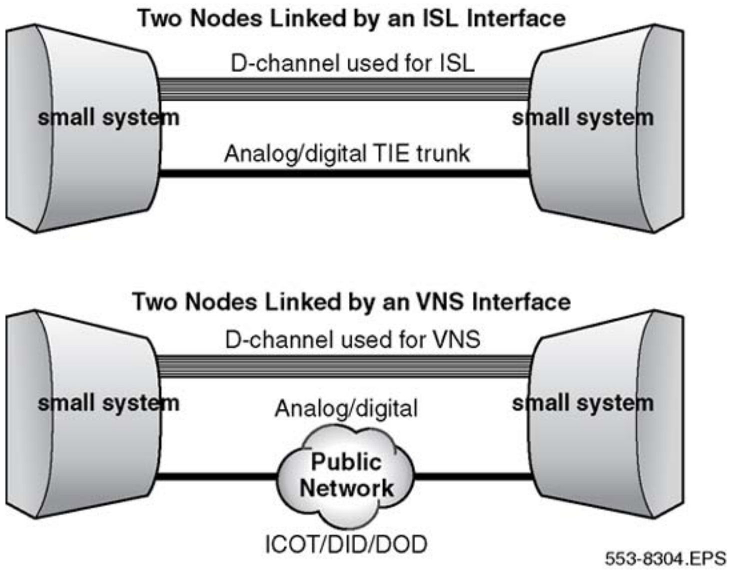

Figure 120: VNS Interface/ISL Interface Comparison

Similar to the case of an ISL interface, the D-channel used for VNS can be shared with the D-channel of a Primary Rate Interface (PRI) that links two system switches, or it can use a D-channel that communicates with the far end through a pair of dedicated line modems, dial-up modems, or system data adapters.

When the D-channel used by VNS is on a PRI, the D-channel mode is defined as USR = SHAV, in LD 17, meaning that VNS, ISL and ISDN PRI calls can share this D-channel. In the other situation, the D-channel is defined as USR = VNS in LD 17 which allows ISL, and VNS calls to use this D-channel for signaling.

The VNS D-Channel is similar to an ISL D-Channel for a Modem/Data circuit. In LD 17 in dedicated mode, the USR is VNS and when connecting system to system over PRI shared mode, the USR is SHAV. The VNSP must be set accordingly. The VNSP is the PNI of the target system programmed in the CDB LD 15.

The following types of trunks and connectivities can be used for VNS calls:

- PRI trunks with: Meridian Customer Defined Network (MCDN) connectivity.
  - PRI2 trunks with: AXE10, NUMERIS, SwissNet 2, 1TR6, and Meridian Customer Defined Network (MCDN) connectivity.
  - Analog trunks with: disconnect supervision.
- 1.5 Mbit Digital Trunk Interface (DTI) trunks with: Digitone Signaling (DTN), or Dial Pulse Signaling (DIP) connectivity.
  - 2.0 Mbit Digital Trunk Interface (DTI2) trunks with: Multifrequency Compelled Signaling (MFC), Digitone Signaling (DTN), or Dial Pulse Signaling (DIP) connectivity.
  - EuroISDN and QSIG trunks with: PRI and Basic Rate Interface (BRI).
  - Digital Private Network Signalling System No.1 (DPNSS1) or Digital Access Signalling System No.2 (DASS2) trunks.

All trunks are being referenced throughout this document as the VNS Bearers, or simply the Bearer trunks.

Although the VNS feature can use Central Office Trunks (COT), Direct Outward Dialing (DOD), and Direct Inward Dialing (DID) trunks to link two system nodes, VNS calls are presented, handled, and interact with other features as though private ISDN TIE trunks are used for that purpose. The exceptions that apply are stated in the "Feature interactions" section.

Note:
TIE trunks can also be used with VNS. When this is the case, the connection does not necessarily need to be a direct system to system connection (e.g., when QSIG is used).

Speechpath availability

When extending a call to a Remote node, the attendant relies on the tones and lamp states to determine if it is possible to extend a call, camp-on a busy extension, break-in to a conversation, etc.

When using a VNS Bearer trunk, the tones can be those of the PSTN (especially for "intelligent" trunks such as ISDN connectivity). For example, when extending a call to a busy phone over an ISDN PSTN Bearer, the attendant hears busy tone (from the PSTN) instead of silence.

If Attendant Console operation has to remain the same with VNS, an answer signal has to be sent right away to the PSTN for attendant extended calls, whatever the state of the terminating party. This allows the attendant to hear the tones coming from the terminating system node, instead of tones from the PSTN.

The prompt VRAT exists for the incoming Bearer route (LD 16) to allow or disallow automatic answering of attendant extended calls. The Network Attendant Service (NAS) feature must be configured to provide this functionality.

When a route is configured with VRAT = YES, tones are similar to those provided on a private ISDN PRI network; however, some unanswered calls can be charged. If a route is configured with the default value (VRAT = NO), tones heard when extending a call from the attendant might be different than the ones provided over a private ISDN network. Users are not charged for unanswered calls.

PSTN clearing of unanswered calls

In some countries, a PSTN call left unanswered is disconnected after a few minutes, in order to reduce the usage of equipment that has not been paid for. This creates a major difference between private networks using TIE lines and private networks using VNS. For example, with VNS a call left in a camp-on state would be cleared by the public network after several minutes.

The VNS Set Speechpath (VSS) timer of the incoming Bearer route (LD 16) can be configured to avoid this situation. It defines the interval after which an answer signal is sent from the terminating system node to the Public Exchange/Central Office.

The configuration of the VSS timer has an impact on the cost of the calls, because the public network starts charging upon the reception of the answer signal.

Numbering Plan

A requirement of VNS is that customers have to configure VNS DNs (VDNs) as part of their numbering plan. The VNS VDN expansion feature sets a new limit on the number of VDNs at 4000. VDNs are configured on LD 79.

The VDNs must be mapped onto the DID range of numbers for the PBX they serve. Do not assign the VDN numbers to any station.

The VDNs are defined in sets of blocks. Each block can contain any number of contiguous VDNs, as long as the total number does not exceed 4000. Within a block, it is possible to define a range of VDNs as well as individual VDNs. For example, a customer can define the following VDNs (in this example, the customer is defining a total of 164 VDNs.)

7200-7299 7320-7325 7355 7400-7455 7676

A customer can remove a block of contiguous VDNs, as long as there is no VNS call using a VDN in the block. To remove a block of contiguous VDNs, the block has to be first disabled in LD 79 (by entering DIS against the REQ prompt), to prevent new VNS calls from using any of the VDNs in the block. Once the block has been disabled, the system administrator has to wait until all the VNS calls, using any of the VDNs in the block, are cleared.

The system administrator can determine the number of VDNs used by VNS calls, by printing VNS information using the PRT command in response to the REQ prompt in LD 79 (note that the block of VDNs must be first disabled.) Once all of the VDNs are free (unused), the block of VDNs can be removed by using the OUT command.

An Electronic Switched Network (ESN) call is identified as being VNS once a valid entry configured when the prompt VNS = YES has been found in a Route List Block (LD 86) used for the digits dialed. A SETUP message is sent to the terminating node on the VNS D-channel. Manipulation of the digits included in the SETUP message is performed, if needed, using the digits dialed and according to the content of the Digit Manipulation Table referenced with the prompt VDMI.

In LD 86, the VDCH entry indicates the VNS D-channel used for call routing. DMI indicates the Digit manipulation table index for VNS B-channel. VDMI indicates the digit manipulation table index for the D-channel. Usually, the DMI table inserts 1+NPA/NXX of the target switch and is usually the only DMI needed. The system automatically inserts the VDN returned from the target system.

On reception of the SETUP request, the terminating node sends one of its Virtual DNs back to the originating node. The terminating node expects to receive a call for that Directory Number

(VDN) from one of its trunks linked to the public network. The originating node, upon reception of the VDN, seizes a trunk and dials a number consisting of the VNS Virtual DN affected by the manipulations defined in the Digit Manipulation Table referenced by the prompt DMI. These manipulations are performed in order to dial the Virtual DN through the public network to the destination node.

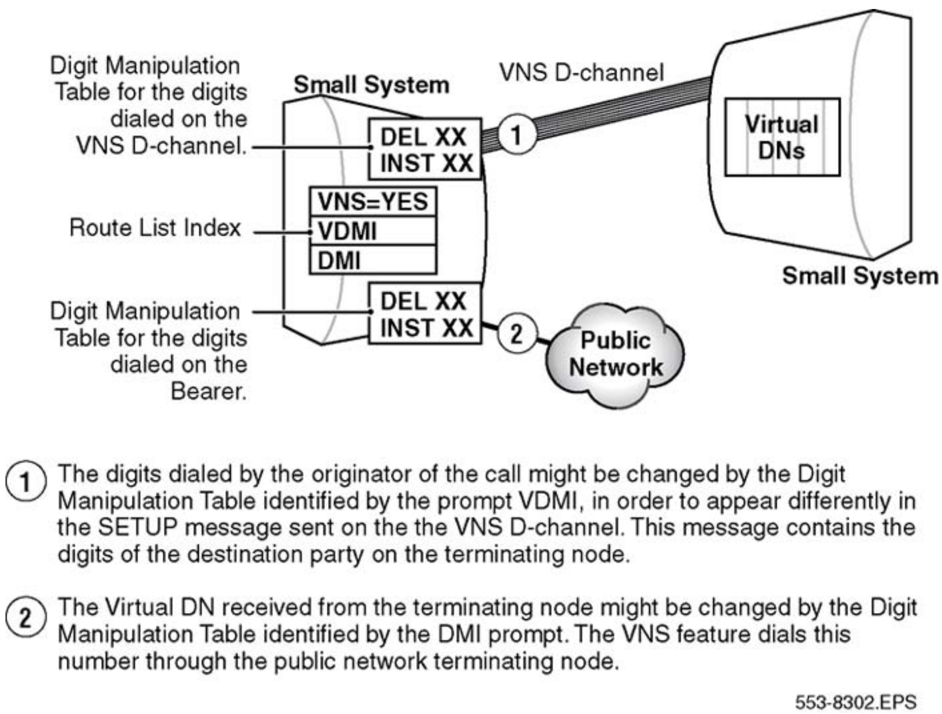

Figure 121: Digit Manipulation

Every active VNS call makes use of 2 VDNs. There is one VDN at the source node and one VDN at the target node. The VDNs are used for the duration of the call. The number of VDNs at the source node and the target node must be identical to number of VNS trunk types. It is strongly recommended that a dedicated trunk group be programmed to carry VNS traffic. The VNS trunk group should have one trunk for each VDN.

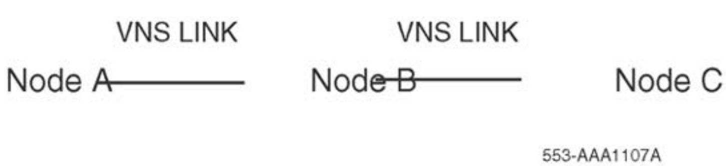

Figure 122: VNS Links

In Figure 122: VNS Links on page 495, Node A and Node B are connected by a VNS link. Node B and Node C are connected by a VNS link. Node B should have 15 VDNs configured for 10 Simultaneous VNS calls between Node A and Node B and 5 simultaneous VNS calls between Node B and Node C.

When using AUTH CODES at the CO level, the DMI in the RLB can insert the AUTH CODE ahead of the public number. This configuration must be negotiated with the CO.

When programming network features in LD 15, such as NACD, the HLOC programmed in the target system's NET DATA must match the dialed LOC at the source switch. The target switch can have more than one HLOC programmed, but the one in LD 15 is the only one used for network feature operation. This HLOC is embedded in the facility messages that control proprietary feature operation.

Failure of VNS D-channel

If the D-channel is not operable, the VNS route list entry is chosen, and then this entry is bypassed. In a network VNS environment, calls will remain queued at the source node.

If the VNS D-channel fails when a call is established, the call remains established. This is, however, without the ability to use the networking features normally supported by the VNS feature.

Failure of Bearer

Failure of the VNS Bearer trunk results in the VNS call being cleared.

Operating parameters

VNS requires a contiguous block of existing unused DNs (virtual DNs) at both the originating and the terminating nodes, which are a subset of the DID range of the customer. VNS virtual DNs can be up to seven digits long. A maximum of 100 virtual DNs can be assigned for each customer.

VNS D-channel

VNS requires an established D-channel between the originating and terminating nodes for signaling. No intermediate nodes are permitted.

A VNS D-channel belongs to only one customer and cannot be shared by other customers for VNS calls.

VNS does not support Backup D-channels for VNS signaling.

D-channels provided by Basic Rate Interface (BRI) are not supported as VNS D-channels.

VNS reverts back to conventional signaling if the VNS D-channel fails.

VNS Bearer Trunks

Disconnect supervision is mandatory for all trunks, while answer supervision is not. In cases when it is not available, VNS will assume that the Bearer is answered as soon as the "end-of-dialing" timer has expired.

The following trunks are not supported as VNS Bearer trunks:

- Autoterminate trunks;
- Analog Private Networking Signalling System (APNSS); and
- Basic Rate Interface trunks (used for NUMERIS, 1TR6 or MCDN).

The following signaling systems are not supported for VNS:

- Japan D70; and
- Multifrequency Extended Signaling for Socotel (MFE).

Any Incoming Digit Conversion on the incoming VNS Bearer trunk causes a VNS call to fail.

Data calls are supported only if the Bearer supports data calls.

Maximum number of VNS calls

Different elements control the maximum number of simultaneous VNS calls that can be processed by a system. The number depends on the resources allocated for the VNS feature itself, the resources to be used for the voice path (Bearer trunks) and the resources available for VNS signaling over the D-channel.

For each customer

It is not possible to perform more VNS calls (incoming and outgoing) than the number of Virtual DNs defined for the customer in LD 79.

The number of VNS calls is limited by the number of available Bearer trunks. When all Bearers defined to be usable with VNS are busy, no other VNS calls can be made.

For each D-channel of the customer

The maximum number of VNS calls allowed to use a D-channel is limited by the value defined to the D-channel by the VNSM prompt in LD 17.

For each entry in a Route List Block

The maximum number of VNS calls that can be performed on a route listed in an entry of a Route List Block in LD 86 is limited by the value entered in response to the VTRK prompt.

On a network level

In the case of a non-symmetrical configuration between originating and terminating VNS nodes, the call limitation imposed by the more restrictive node applies.

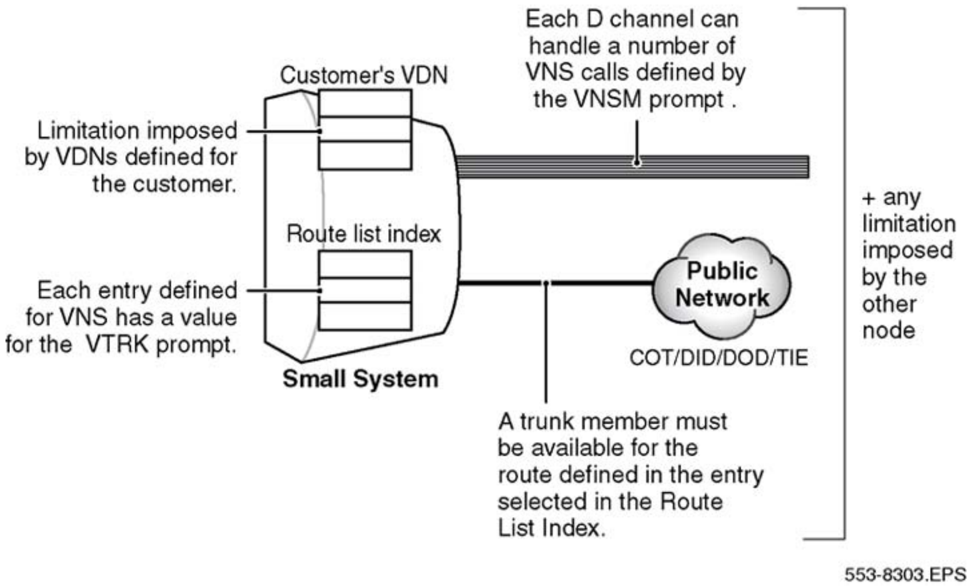

Figure 123: VNS Call Limitations

Troubleshooting failed VNS calls and useful tips

VNS uses PSTN facilities to provide "tie trunk-like connectivity". Only the source system can determine the availability of an outgoing DOD/COT trunk member. The status of the incoming DID trunk at the target system is not known until the call is attempted. VNS attempts to complete the call regardless of All Trunks Busy for the DID trunk group at the Target node. VNS considers the non availability of the trunks as bearer failure. The system outputs an error ERR5428 at the source node. ERR5428 indicates a Failure on a bearer trunk used by VNS.

VNS can generate more than one error message for a single VNS call failure. An on-site technician interprets this as a serious issue, but it is the expected behavior of the feature. On-site technicians need to analyze these messages to take appropriate action. The bearer failure could be due to network blockage or an insufficient number of VDNs. If there are multiple call failures, multiple bug messages are generated, which can hamper the normal TTY operation, which results in an INI.

The most common errors generated are the following:

- ERR5428 (refers to BEARER FAILURE)
- BUG5180 (refers to VNS call processing GENERAL ERROR MESSAGE)
- BUG5182 (refers to NO VNS DN FOUND corresponding to the request)

The only alternative to the multiple bug messages generated because of multiple call failures is to use LD 17 to XBUG. If further BUG and ERR monitoring is required, configure a 9600 BD modem on the Core with USR BUG. Only configure TTY for BUG in these extreme situations.

While using VNS over NACD, ensure enough Call Registers are available to buffer the messaging by doing the following:

- Use MON 0.
- Use pdt to determine the number of call registers used in the print queue. pdt > sl1Qshow
- If needed, use LD 48 to flush the buffers.

When troubleshooting a VNS problem, the dialed number is the key. Extract the dialed number from the Bug. Perform a Ras Trace on the Bug to determine the call flow. ISA B-channels left in MBSY state, as a result of VNS call failures, can generate pages of bugs.

Typical VNS bugs

The following are typical VNS bugs:

- Bug 5180: Wait while the Virtual Network Service (VNS) performs some call processing.
- Bug 5181: A nil pointer is found during Virtual Network Service (VNS) call processing.
- Bug 5182: There is a PRA call reference mismatch affecting the VNS Index pointer. Run an audit.

Note:

This bug is generated if a DID call is made to a VDN through a misdial from the public network. If the only output is many 5182 bugs, then a PRA call reference mismatch affecting the VNS Index pointer is the probable cause.

Troubleshooting tips to isolate VNS related issues

Many issues can arise when installing VNS for the first time.

The following are tips to find the cause of VNS issues:

- Verify the ESN programming when using CDP/LOC. This ensures the proper RLB is used.
- Verify that the VPNIs on the VNS D-Channels match.
- Verify that the VDMI and DMI entries in the VNS RLB are correct.

Examples of problems encountered while installing a VNS Network:

- The customer is using NACD over VNS and the target queues do not open even though agents are available.

  This problem can be related to LOC HLOC mismatch. Check that the LOC of the dialed queue matches the HLOC defined in LD 15 of the target system.

- VNS calls do not complete during test scenarios.

  The problem can be related to the DMI. Verify that the DMI and VDMI for the VNS RLB is correct. The VDMI should not require Digit manipulation as long as the CDP/UDP dialed number can be translated at the target system. The DMI is critical, because it determines the PSTN portion of the call. The DMI must point to an outgoing COT/DOD/TIE RLB and includes everything except the VDN. The system automatically inserts the VDN.

  Example: The target DID number is 4167432888. 2888 is a VDN at the target system. The DMI should, in this case, be 61416743 using NARS/BARS. The system negotiates the insert of the 2888 as it is a VDN at the target switch.

  Also, verify the target trunks. It is possible that the target trunks are not set up as DID in the CO. Customers can try to configure VNS, because they do not know that the CO needs to translate the VDNs to a valid DID range at the target.

- Outgoing trunks require an auth code.

  Some customers use outgoing toll trunks that require an auth code at the CO level. This can be overcome by inserting the auth code ahead of the DMI in the VNS RLB. This must also be negotiated with the CO.

- NACD calls are terminating to an ACD Queue that is NCFW to an ACD Queue that uses NACD over VNS.

  This scenario is not supported as the design intended.

Typical VNS error

VNS Errors, as a rule, do not provide much useful information when trying to isolate a VNS issue. Extract the dialed number for the Err message to determine the call scenario.

When troubleshooting VNS Errors, insist that access to both source and target systems is available, and that trained technicians are present in both switch rooms to make test calls.

Err5428: Failure on a bearer trunk used by VNS. This is a common VNS Err and is generated for a VNS call that does not complete to the target system.

Typical call scenarios causing this error are:

- All Trunks Busy at the target node
- NACD call reject due to the expiration of the RAGT
- target agent rejecting the call by MSBY/LOGOUT
- blockage at the CO of the source system

This message is output at each system at the time of call failure. The dialed number from the VNS D- channel can be output in reverse format. Use this to determine the source of the call.

To isolate an ERR5428 use the following procedure:

1. Determine the called number from the ERR.

   For example: ERR5428 52 00002348 0029C261 00001005 00008018 00001E4C 00000000 19 00223979 002E1D39 00 _000000 0 2090 00000084 0000A9A2 00000000 00000000 00000000 00000000 00000000 000

   In this case 2348 is the packed TN of the outgoing trunk, and the 2090 is a target NACD Queue. Note that the A9A2 is in reverse format and A = 0.

   For example: ERR5428 3 00001D90 00274031 00000607 00008318 00001F18 00001D90 0 00000000 00000000 0000 _ 0000 0 2090 00000108 00002225 00003A34 00000000 00000000 00000000 00000000 00000

   In this case 1D90 is the packed TN of the outgoing trunk, and 2090 is the source Queue and 52224303 is a UDP target NACD Queue.

   Note:
   Not all ERR5428s indicate the dialed number, but it is a good start.
2. Determine the calling pattern with personnel familiar with the network.
3. If the calling pattern can be established, use the D-Channel monitor to associate the ERR5428 with a specific call.
4. If the switch is busy, use monitor 0 only.
5. Turn on the outgoing setup only at the source and the incoming only at the target for the D-Channels associated with the public part of the call.
6. Use monitor 0 on the VNS D-Channel in the same manner.

   This reveals all the call information at the time of the ERR5428 without causing a real time load on the network.
7. Use the collected information to establish the root cause of the ERR.

Some causes are due to programming errors, such as:

- ESN Errors
- CO blockage due to translations
- faulty facilities (for example:)
    - bad analog trunks
    - all trunks busy at the target system
    - call rejections from ACD Agents

Feature interactions

In LD 17, set NASA to "yes" for the MCDN supplementary features to work across the DCH.

The following features are supported over VNS routes:

- Attendant Barge-In
- Attendant Break-In
- Attendant Recall with Splitting
- Basic Authorization Code
- Basic Rate Interface/Primary Rate Interface Interworking
- Calling Party Number
- Call Party Name Display
- Call Selection (ICI + loop)
- Console Digit Display
- Control of Trunk Group Access
- Digit Display
- Display of Calling Party Denied
- Electronic Lock Network Wide/Electronic Lock on Private Lines
- Network Attendant Service
- Network Call Redirection
- Network Class of Service
- Network Flexible Feature Codes
- Network Message Center
- Network Message Service to Meridian Mail
- Network Ring Again
- Network Ring Again No Answer

- Originator Routing Calls
- Radio Paging
- Trunk Route Optimization Before Answer

In addition, VNS has interactions with the following features:

Access Restriction

When a user has trunk access barred, for example, through Trunk Group Access Restriction (TGAR), New Flexible Call Restriction (NFCR), or Toll Denied Class of Service), the user will still be able to make a VNS call.

If a customer wants users to be toll restricted even for VNS calls, the Minimum Facility Restriction Level (FRL) in the Route List Block (i.e., LD 86) can be used.

Analog Private Networking Signalling System (APNSS)

APNSS trunks cannot function as VNS Bearer trunks.

Attendant Call

When an attendant extends a call over a VNS network, it is not possible to release the call before the status of the destination is known. This applies regardless of Network Attendant Service (NAS) configuration.

Autoterminate

Autotermination on VNS Bearer trunks is not supported, because a VNS Virtual DN is expected on a VNS Bearer exactly the way it was passed back on the VNS D-channel.

Call Detail Recording (CDR)

Call Detail Recording is supported on VNS routes with the exception of the 911 CDR Improvement and Meridian 911 ANI in CDR features. The CDR output is controlled by the Bearer trunk (i.e., CDR output defines the details of the call made on the Bearer, and not the VNS D-channel). The Calling Line Identity will be output in the CDR record for incoming calls.

Call Pickup Network- Wide

The Call Pickup Network Wide feature will not work in conjunction with the Virtual Network Services feature.

Calling Line Identification

Calling Line Identification is supported on VNS routes. All display information is taken from messages on the VNS D-channel. The VNS Bearer does not drive the display of such information.

Charge Display at End of Call

In the case of VNS calls, no charge information is displayed.

Data Calls

Data calls are supported on DPNSS1 or DASS2 VNS Bearer trunks if the DPNSS1 or DASS2 VNS Bearer trunks are configured to support data calls. Similarly, data calls are supported on DPNSS1 or DASS2 Bearer trunks in VNS to DPNNS1/DASS2 gateways, if the DPNSS1 or DASS2 VNS Bearer trunks are configured to support data calls.

Digital Trunk Interface (DTI) - Commonwealth of Independent States (CIS)

Virtual Network Services through CIS DTI2 is not supported.

Direct Inward Dialing (DID) Treatment

Since VNS is handling calls as though they were made using ISDN TIE trunks even when VNS DID Bearer trunks are used, the VNS feature does not adhere to the special treatment given to regular DID trunks.

Distinctive Ringing

Except in the case of Network Distinctive Ringing, the Distinctive Ringing feature is not supported by VNS. An incoming call using VNS on a Bearer trunk defined with the prompt DRNG = YES will ignore this value and will perform the same treatment as though the value was DRNG = NO (i.e., no distinctive ringing provided).

DPNSS1 Attendant Call Offer

DPNSS1 Attendant Call Offer is not supported over VNS Bearer trunks (DPNSS1 Attendant Call Offer allows an attendant-extended call, routed over a DPNSS1 trunk, to be camped-on to a remote busy extension.) Standard ISDN Camp-on can be provided instead, if NAS is configured over the VNS Bearer trunks.

DPNSS1 Attendant Timed Reminder Recall and Attendant Three-Party Service

DPNSS1 Attendant Timed Reminder Recall and Attendant Three-Party Service are not supported over VNS Bearer trunks. If NAS is configured over the VNS Bearer trunks, NAS call extension and Attendant Recall will be offered instead.

DPNSS1 Call Back When Free and Call Back When Next Used

DPNSS1 Call Back When Free and Call Back When Next Used are not supported over VNS Bearer trunks. Network Ring Again or Network Ring Again on No Answer can be provided instead, if Network Ring Again or Network Ring Again on No Answer are configured over the VNS Bearer trunks.

DPNSS1 Diversion

DPNSS1 Diversion is not supported over VNS Bearer trunks. Network Call Redirection and Trunk Route Optimization can be provided instead, if configured over the VNS D-Channel.

DPNSS1 Extension Three-Party Service

DPNSS1 Extension Three-Party Service is not supported over VNS Bearer trunks. Network Call Redirection and Trunk Route Optimization can be provided instead, if configured over the VNS D-Channels.

DPNSS1 Loop Avoidance

DPNSS1 Loop Avoidance is not supported over VNS Bearer trunks (DPNSS1 Loop Avoidance prevents a call from being looped through a DPNSS1 network by placing a limit on the number of channels that a call can use.) The ISDN Call Connection Limitation is provided, if it is configured over the VNS D-Channel.

DPNSS1 Route Optimization

DPNSS1 Route Optimization is not supported over VNS Bearer trunks.

DPNSS1 Route Optimization/ISDN Trunk Anti-Tromboning Interworking

ISDN Trunk Anti-Tromboning can be applied to the VNS part of the call, if configured on the VNS D-Channel.

DPNSS1 Route Optimisation/MCDN Trunk Anti-Tromboning Interworking

The Route Optimisation/Trunk Anti-Tromboning Interworking feature is not supported over VNS trunks, since VNS uses only MCDN signaling. DPNSS1 is not supported.

DPNSS1 Step Back On Congestion

DPNSS1 Step Back On Congestion handles high traffic situations when congestion is encountered by DPNSS1 trunks. The following scenarios apply for interworking with VNS.

Homogeneous Networks

DPNSS1 Step Back On Congestion is supported over VNS Bearer trunks, if all the transit nodes within the DPNSS1 network used for VNS are configured accordingly:

- In LD 86, if the SBOC (Step Back On Congestion) prompt is set to NRR (No Reroute) or RRO (Reroute Originator), then it would be sufficient that the VNS originating node be configured with either RRO (Reroute Originator) or RRA (Reroute All).
- In LD 86, if the SBOC (Step Back On Congestion) prompt is set to RRA (Reroute All) for a transit node, then the different alternative routes at this node must be configured with VNS and must be configured as VNS Bearers.

Hybrid Networks

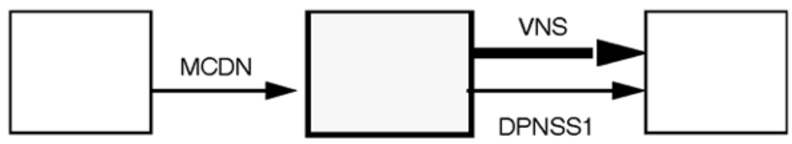

Figure 124: MCDN/VNS with DPNSS1 node

- If a congestion is encountered inside the VNS portion of the path, the node behaves as an MCDN/MCDN tandem. The ISDN Drop Back Busy (IDBB) and ISDN Off-Hook Queuing (IOHQ) are transmitted, so that they can be applied further along the VNS portion of the path, or at the tandem node.
- If a congestion is encountered within the DPNSS1 network, the VNS portion of the call is cleared and the disconnection is propagated back to the originating side of the MCDN path. Neither Drop Back Busy nor Off-Hook Queuing is activated at the tandem node, even if IDBB or IOHQ are activated.

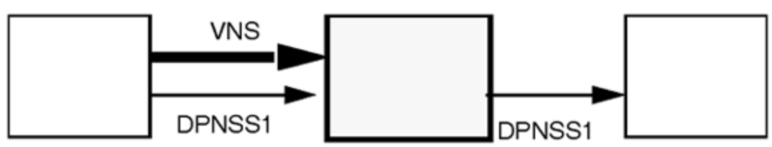

Figure 125: VNS with DPNSS1/DPNSS1 node

This scenario is considered an MCDN/DPNSS1 gateway.

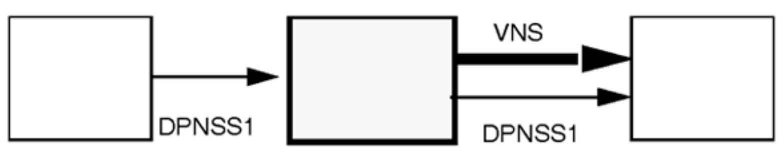

Figure 126: DPNSS1/VNS with DPNSS1 node

- If a congestion is encountered inside the VNS portion of the path, the VNS portion of the call is cleared and the disconnection is propagated back to the originating DPNSS1 side. The Step Back on Congestion feature is invoked, if it is configured.
- If a congestion is encountered the within the DPNSS1 portion of the path, with the DPNSS1 trunk being used as a VNS Bearer, the VNS portion of the call is cleared and a normal disconnection is propagated back to the originating DPNSS1 side. The Step Back on Congestion feature is not invoked, even if it is configured.
- Refer to Figure 127: Network Attendant Service (NAS) on page 508 for information on the interaction with NAS in a similar scenario.

DPNSS1 Executive Intrusion

DPNSS1 Extension Three-Party Service is not supported over VNS Bearer trunks. Attendant Break-in can be provided instead, if NAS is configured over the VNS Bearer trunks.

Figure 127: Network Attendant Service (NAS)

NAS calls being routed over the DPNSS1 network used as VNS Bearer will get dropped if there is congestion in the bearer call setup. NAS DBK (drop back) will not occur even if it is configured.

Stand-alone Meridian Mail

Stand-alone Meridian Mail is not supported over VNS Bearer trunks. A mailbox user can access Meridian Mail, if the ISDN Network Message Services is configured.

DPNSS1 Enhancements for ISDN Interworking

Enhancements allow DPNSS1 to interwork with QSIG and EuroISDN. At an ISDN gateway, ISDN information can be carried into some DPNSS1 messages, if DPNSS_189I package 284 is equipped.

DPNSS1/DASS2 to ISDN PRI Gateway

A VNS call over a DPNSS1 or DASS2 Bearer trunk of an DPNSS1/DASS2 to ISDN PRI Gateway acts as the ISDN leg of the Gateway.

Electronic Switched Network (ESN)

The following ESN features are supported on VNS routes:

- ESN Basic Automatic Route Selection
- ESN Coordinated Dialing Plan Routing Enhancement
- ESN Coordinated Dialing Plan
- ESN (999 Loc.)

- ESN Flexible Numbering Plan
- ESN Free Calling Area Screening
- ESN Incoming Trunk Group Exclusion
- ESN Network Authorization Code
- ESN Network Automatic Route Selection
- ESN Network Routing Controls (Time-of-day Scheduling)
- ESN Network Speed Call
- ESN Tone Detection
- ESN Off-Hook Queuing

EuroISDN Continuation

A EuroISDN link can be used as a B-Channel for the Virtual Network Services feature.

EuroISDN Trunk - Network Side

Virtual Network Services is supported on a EuroISDN Trunk - Network Side connectivity, meaning that a EuroISDN Trunk - Network Side trunk can be used as a VNS bearer trunk.

Incoming Digit Conversion

Since VNS Virtual DNs must be received on the incoming VNS Bearer (DID) trunks, as they are defined at the terminating node, the VNS feature is not supported for routes that perform digit conversion on the digits used for VNS Virtual DNs.

ISDN Call Connection Limitation (ICCL) Checks

The VNS trunk from the external network looks exactly like an ISDN TIE trunk and accordingly is subject to ICCL checks and call restrictions applied thereon.

ISDN PRI/BRI system to Asia Pacific Connectivity

It is not possible to configure an Asia Pacific D-channel as a VNS D-channel. However, the voice connection through the Public Exchange of a VNS call can use a PRI/BRI COT or DID as a virtual TIE trunk.

ISDN QSIG Basic Call

A QSIG link can be used as a B-channel for the Virtual Network Service (VNS) over a private network. All VNS services are supported as normal. QSIG is only used as a speech bearer.

Intercept Treatment

Intercept treatment applied to VNS calls is configured as for TIE trunks.

Network ACD

Network ACD (NACD) is supported by VNS. When a call queued at a source node receives notification that an agent is free and reserved at the target node, a VNS call is made to the target node. At that time, the call is removed from the queue at the source node. The call will continue to receive ringback (or Recorded Announcement (RAN) if configured) while it is waiting for the VNS call to be completed. When an alerting message is received from the target node, the ringback or RAN is removed and the speechpath with the Bearer is connected. The user will thus hear ringback tone (given either by the PSTN or the system at the target node, depending on the Bearer type), until the agent answers the call.

If for some reason the ALERTING message is not received, the user is requeued (at the top of the queue at the source node). Since ringback or RAN were not removed in the first place, the user is unaware that an attempt to reach a remote agent has been made and has failed.

Since PSTN Bearer trunk call establishment can take longer than PRI2 TIE trunk call establishment, it is necessary to allow more time for the call to arrive at the agent's phone than provided by the regular NACD feature. The Agent Reservation Timer should be configured to accommodate a longer interval.

If an agent is reserved at the target node, but the call fails to reach that node (e.g., all trunks are busy), the agent will stay reserved until NACD Target Reservation Timer (RAGT) expires (the target node has no indication that the call has encountered a busy condition). This is more critical when NACD is used with VNS, because (RAGT) must be set to a greater value.

NACD allows up to 20 remote target nodes to be defined in the routing tables. Since the maximum number of VNS Virtual DNs for each customer is 100, it is not realistic to configure 20 target nodes using VNS routing: this would only allow five Virtual DNs for each target node and thus a maximum of five simultaneous calls.

Set the RAGT to a minimum of 6, but ideally, it should be set to 12. Set the CRQS and FCTH according to the D-Channel speed. Below 28800 the settings should be a minimum. For example, 11 for CRQS and 10 for FCTH. For 28800 and greater, use 10 for FCTH and 20 for CRQS.

Note:
These settings are critical for proper network operation.

Network Call Party Name Display

Network Call Party Name Display is supported on VNS routes. All display information is taken from messages on the VNS D-channel. The VNS Bearer does not drive the display of such information.

Network Distinctive Ringing

For an incoming DID call (without VNS) that tandems to another node using VNS, the feature will be supported as it would have been if an ISDN TIE trunk had been used for the VNS call.

Overlap Sending and Overlap Receiving

Call establishment over the VNS D-channel will not use overlap sending/receiving even if configured. Enbloc sending will always be used on the VNS D-channel. Overlap sending/receiving will be supported on the Bearer trunks if that capability already exists.

Periodic Pulse Metering

Periodic Pulse Metering is supported on the VNS Bearer trunks only.

R2 Multifrequency Compelled Signaling to DPNSS1 Gateway

If the call on the DPNSS1 (or R2MFC) trunk is tandeming to the R2MFC or (DPNSS1) trunk on a Virtual Network Services (VNS) call, the R2MFC to DPNSS1 Gateway feature does not apply. If a DPNSS1/R2MFC tandem is encountered during the routing of a VNS call, the R2MFC to DPNSS1 Gateway feature applies. The following figure illustrates how the R2MFC-DPNSS1 gateway can apply to a VNS call.

Three Wire Analog Trunk - Commonwealth of Independent States (CIS)

Virtual Network Services is not supported on CIS trunks.

Trunk Barring

Three cases apply for Trunk Barring:

1. When the second trunk involved in the call is used by VNS, no trunk barring is applied regardless of the configuration of the first trunk. The call is always allowed to get through.

   Note:
   This implementation completely overrides the Trunk Barring feature.
2. When the first trunk involved in the call uses VNS, and the second one is not used by VNS, trunk barring is performed according to the content of the default Access Restriction Table (ART) for the TIE trunk.
3. When neither the first trunk nor the second trunk is involved in a VNS call, the usual rules for Trunk Barring apply.

Vacant Number Routing

Calls rerouted by the Vacant Number Routing feature are not allowed to have digit manipulation performed on the DN dialed. Thus, for non VNS calls, no Digit Manipulation Index (DMI) can be associated in the Route List Index (RLI) used by Vacant Number Routing. For VNS calls (in LD 86, the entries on this RLI are defined with the prompt VNS = YES), it is not allowed to associate any manipulation on the digits included in the messages exchanged over the VNS D-channel. In these cases, the prompt VMDI is not displayed, but the prompt DMI is still displayed.

Advice of Charge for Euro ISDN

For a Virtual Network Service (VNS) simple call connectivity, received charging information is stored against the Message Registration meter of the calling party's phone.

On an outgoing trunk call on VNS connectivity, charging information is processed based on the Trunk to Trunk Connection feature.

Feature packaging

The Virtual Network Services (VNS) package is 183.

The following software packages are also required for VNS:

- Network Alternate Route Selection (NARS) package 58, which is dependent on Basic Routing (BRTE) package 14 and Network Class of Service (NCOS) package 32
- Integrated Services Digital Network (ISDN) package 145
- ISDN Signaling Link (ISL) package 147
- Advanced Network Services (NTWK) package 148
- Primary Rate Access (PRI) package 146, or 2.0 Mbit PRI (PRI2) package 154 is required if VNS uses the D-Channel of a PRI or PRI2 trunk for its signaling (USR = SHAV)
- Integrated Services Digital Network Supplementary (ISDNS) package 161

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

Table 201: LD 17: Configure Virtual Network Services.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	ADAN aaa xx	Action device and number.
...		

Prompt	Response	Description
- USR	VNS	To define a D-channel used for Virtual Network Services (or ISLD).
	SHAV	To define a D-channel shared between PRI and VNS (and ISLD).
- VNSM	0-100	Define the maximum number of VNS channels over the D-channel.
- VNSC	xx	Virtual Network Services Customer number.
- VNSP	0-32700	Private Network Identifier (PNI) of the far end customer.
- VNCA	YES	Network Call Party Name Display is available over this D-channel for VNS.
- VCRD	YES	Network Call Redirection is available over this D-channel for VNS.
- VTRO	YES	Trunk Route Optimization before answer is available over this D-channel for VNS. This prompt is optional and is not a prerequisite for VNS.

Table 202: LD 79: Add or create a new single VDN or a block of contiguous VDNs.

Prompt	Response	Description
REQ	NEW	Add or create a new single VDN or a block of contiguous VDNs. **Note:** The CHG command is not supported; you must use the NEW command to enter information.
TYPE	VNS	Virtual Network Services.
CUST		Customer number
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
VNDN	xx...x 1-4000 xx...x	Individual VDN to be added. 1-4000 = number of contiguous VDN to be added xx...x = first VDN to be added.
	<CR>	You can add another single VDN or a block of contiguous VDNs by entering <CR> after the VNDN entry. VNDN is prompted until <CR> is entered. In this case, the REQ prompt will appear again. **Note:** For the above entries, the VDNs must be part of the customer's numbering plan.

Table 203: LD 79: Remove a single VDN or a block of contiguous VDNs, or remove all existing VDN data blocks.

Prompt	Response	Description
REQ	OUT	Remove a single VDN or a block of contiguous VDNs, or remove all existing VDN data blocks. **Note:** You cannot remove only certain VDNs from a block; you have to remove the entire block.
TYPE	VNS	Virtual Network Services.
CUST		Customer number **Note:** At least one D-Channel must be configured with USR = VNS or USR = SHAV and having VNS = customer number.
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
VNDN	XALLVDNS xx...x	Remove all VNS data blocks. Remove an individual VDN, or the first VDN of a block of contiguous VDNs.
	<CR>	You can remove another single VDN, or a block of contiguous VDNs, by entering <CR> after the VNDN entry. VNDN is prompted until <CR> is entered. In this case, the REQ prompt will appear again. If XALLVDNS is entered, the message REMOVE ALL VDN BLOCKS? is then output, followed by the CONF prompt.
CONF	YES	To confirm the removal of all VDN blocks.

Table 204: LD 79: Disable or enable single VDN, or a block of contiguous VDNs.

Prompt	Response	Description
REQ	DIS	Disable a single VDN or a block of contiguous VDNs
	ENL	Enable a single VDN or a block of contiguous VDNs
TYPE	VNS	Virtual Network Services.
CUST		Customer number **Note:** At least one D-Channel must be configured with USR = VNS or USR = SHAV and having VNS = customer number.
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
VNDN	xx....x	Individual VDN, or first VDN of a block of contiguous VDNs to be disabled or enabled.

Prompt	Response	Description
	<CR>	You can enable or disable another single VDN, or a block of contiguous VDNs, by entering <CR> after the VNDN entry. VNDN is prompted until <CR> is entered. In this case, the REQ prompt will appear again.

Note:

The information is output after the customer number is entered in response to the CUST prompt.

Table 205: LD 79: Print VNS information for a customer.

Prompt	Response	Description
REQ	PRT	Print VDN information.
TYPE	VNS	Virtual Network Services.
CUST		Customer number **Note:** At least one D-Channel must be configured with USR = VNS or USR = SHAV and having VNS = customer number.
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
		The VNS information is output for the customer. For a range of VDNs, the first VDN is displayed, followed by "—" and the last VDN of the block. On the same line, the number of VDNs in the block is displayed in brackets. For a single VDN, the VDN is displayed followed by "(1)". If a block is disabled, the above indication is followed by the number of VNS calls still using a VDN in the block. These calls have to be cleared before the VDN block can be removed. At the end, the total number of VDNs configured for the customer is output.
		A sample output could be: 7676 (1) 8100—8199 (100) TOTAL NUMBER OF VDN FOR CUST 2: 101 If the VDN block 8100-8199, containing 100 VDNs, is disabled, the output would be: 7676 (1) 8100—8199 (100) *DISABLED - VDN USED: 2* TOTAL NUMBER OF VDN FOR CUST 2: 101 In this case, the VDN block is disabled and two VNS calls are still using two VDNs. These two calls must first be cleared before the VDN block 8100-8199 can be removed.

Table 206: LD 86: Assign D-channel number and VNS digit manipulation index to be used when signaling on the Bearer trunk and on the D-channel.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
...		
ENTR	0-63	Entry number for NARS/BARS Route List.
ROUT		Route number **Note:** This is the route number associated with the VNS Bearer channel.
	0-511	Range for Large System , Media Gateway 1000B, and CS 1000E system.
VNS	YES	Virtual Network Services.
VDCH	0-63	The D-channel used for these VNS calls (must be configured in LD 17).
VDMI	xxx	The Digit Manipulation Table to be used on the VNS D-channel.
	(0)	No digit manipulation required.
	1-31	For Coordinated Dialing Plan feature.
	1-255	For NARS/BARS.
VTRK	1-(20)-100	Number of VNS trunks allowed on the route.
DMI	xxx (0) 1-31 1-255	The Digit Manipulation table to be used on the VNS Bearer. No digit manipulation required. For Coordinated Dialing Plan feature. For NARS/BARS.

Table 207: LD 16: Configure VNS trunk route options.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
TYPE	RDB	Route Data Block.
CUST		Customer number
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
ROUT		Route number

Prompt	Response	Description
		Note: This is the route number associated with the incoming VNS Bearer channel.
	0-511	Range for Large System , Media Gateway 1000B, and CS 1000E system.
CNTL	YES	Change control of timers.
- TIMR	VSS (0)	VNS Set Speechpath Timer 0 = Do not answer the bearer channel until the terminating party answers.
	1 2-1023	1 = Answer the Bearer channel immediately on arrival. 2-1023 = Answer the Bearer channel after specified seconds (rounded down to two-second multiples) if the terminating party has not already answered.
- TIMR	VGD 0-(6)-31	VNS Guard Timer The time allowed for the Bearer trunk call to disconnect, in seconds. This is a guard timer on the associated VNS DN.
...		
VRAT	(NO) YES	VNS Return Attendant Tones Option Do (not) answer an attendant extended call over VNS immediately on the incoming Bearer trunk.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 54: Virtual Network Services Virtual Directory Number Expansion

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Feature description

Virtual Network Services (VNS) provides ISDN features to customers when no ISDN Primary Rate Interface (PRI) or ISDN Signaling Link (ISL) Bearer Channels are available between two system switches. (Refer to the VNS feature description module in this technical document for detailed information on VNS).

You must configure VNS DNs (VDNs) as part of the numbering plan. The VNS VDN expansion feature sets a new limit on the number of VDNs at 4000. VDNs are configured on LD 79.

The VDNs are defined in sets of blocks. Each block can contain any number of contiguous VDNs, as long as the total number does not exceed 4000. Within a block, it is possible to define a range of VDNs as well as individual VDNs.

For example, a customer can define the following VDNs (In this example, the customer is defining a total of 164 VDNs.)

- 7200-7299
- 7320-7325
- 7355
- 7400-7455
- 7676

A customer can remove a block of contiguous VDNs, as long as there is no VNS call using a VDN in the block. To remove a block of contiguous VDNs, the block has to be first disabled in LD 79 (by entering DIS against the REQ prompt), to prevent new VNS calls from using any of the VDNs in the block. Once the block has been disabled, the system administrator has to wait until all the VNS calls, using any of the VDNs in the block, are cleared.

After disabling the block, the system administrator can determine the number of VDNs used by VNS calls by printing VNS information (by using the PRT command in response to REQ in LD 79). Once all of the VDNs are free, the block can be removed by using the OUT command.

Operating parameters

There are no operating parameters associated with this feature.

Feature interactions

There are no feature interactions associated with this feature.

Feature packaging

The VNS VDN expansion feature requires the following packages:

Virtual Network Services (VNS) package 183

The following software packages are also required:

- Network Alternate Route Selection (NARS) package 58, dependent on:
    - Basic Routing (BRTE) package 14

- Network Class of Service (NCOS) package 32
- Integrated Services Digital Network (ISDN) package 145
- ISDN Signaling Link (ISL) package 147
- Advanced Network Services (NTWK) package 148
- Integrated Services Digital Network Supplementary (ISDN INTL SUP) package 161
- Primary Rate Access (PRI) package 146, or 2.0 Mbit PRI (PRI2) package 154, is required if VNS uses the D-Channel of a PRI or PRI2 trunk for its signaling (USR = SHAV)

Feature implementation

Task summary list

The following is a summary of the tasks in this section:

1. Table 208: LD 17: Define the maximum number of VNS channels supported by a D-Channel. on page 521
2. Table 209: LD 79: Add or create a new single VDN or a block of contiguous VDNs. on page 522
3. Table 210: LD 79: Remove a single VDN or a block of contiguous VDNs, or remove all existing VDN data blocks. on page 523
4. Table 211: LD 79: Disable or enable single VDN, or a block of contiguous VDNs. on page 523
5. Table 213: LD 86: Define the maximum number of VNS trunks allowed on the route list entry. on page 525

Table 208: LD 17: Define the maximum number of VNS channels supported by a D-Channel.

Prompt	Response	Description
REQ	CHG	Change existing data.
	END	Exit LD 17.
TYPE	ADAN	Action Device and Number.
- ADAN	CHG DCH 0-63	For Large Systems
...		
- USR	VNS SHAV	VNS = dedicated VNS D-Channel SHAV = shared VNS D-Channel

Prompt	Response	Description
...		
- - VNSM	1-300	Maximum number of VNS channels supported by the D-channel. **Note:** This is the potential VNS capability for the D-channel and is not associated with other restrictions placed on VNS capability, such as the number of VDNs.

Table 209: LD 79: Add or create a new single VDN or a block of contiguous VDNs.

Prompt	Response	Description
REQ	NEW	Add, or create a new single VDN or a block of contiguous VDNs. **Note:** The CHG command is not supported; you must use the NEW command to enter information.
TYPE	VNS	Virtual Network Services.
CUST		Customer number **Note:** At least one D-Channel must be configured with USR = VNS or USR = SHAV and having VNS = Customer number.
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
VNDN	xx...x 1-4000 xx...x	Individual VDN to be added. 1-4000 = number of contiguous VDN to be added xx...x = first VDN to be added.
	<CR>	You can add another single VDN or a block of contiguous VDNs by entering <cr> after the VNDN entry (VNDN is prompted until <cr> is entered.) In this case, the REQ prompt will appear again. **Note:** For the above entries, the VDNs must be part of the customer's numbering plan.

Table 210: LD 79: Remove a single VDN or a block of contiguous VDNs, or remove all existing VDN data blocks.

Prompt	Response	Description
REQ	OUT	Remove a single VDN or a block of contiguous VDNs, or remove all existing VDN data blocks. **Note:** You cannot remove only certain VDNs from a block; you must remove the entire block.
TYPE	VNS	Virtual Network Services.
CUST		Customer number **Note:** At least one D-Channel must be configured with USR = VNS or USR = SHAV and having VNS = Customer number.
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
VNDN	XALLVDNS xx...x	Remove all VNS data blocks. Remove an individual VDN, or the first VDN of a block of contiguous VDNs.
	<CR>	You can remove another single VDN, or a block of contiguous VDNs, by entering <cr> after the VNDN entry (VNDN is prompted until <cr> is entered.) In this case, the REQ prompt will appear again. If XALLVDNS is entered, the message REMOVE ALL VDN BLOCKS? is then output, followed by the CONF prompt.
CONF	YES	To confirm the removal of all VDN blocks.

Table 211: LD 79: Disable or enable single VDN, or a block of contiguous VDNs.

Prompt	Response	Description
REQ	DIS	Disable a single VDN or a block of contiguous VDNs
	ENL	Enable a single VDN or a block of contiguous VDNs
TYPE	VNS	Virtual Network Services.
CUST		Customer number **Note:** At least one D-Channel must be configured with USR = VNS or USR = SHAV and having VNS = Customer number.
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
VNDN	xx....x	Individual VDN, or first VDN of a block of contiguous VDNs to be disabled or enabled.

Prompt	Response	Description
	<CR>	You can enable or disable another single VDN or a block of contiguous VDNs, by entering <CR> after the VNDN entry (VNDN is prompted until <CR> is entered.) In this case, the REQ prompt will appear again.

Note:

The information is output after the customer number is entered in response to the CUST prompt.

Table 212: LD 79: Print VNS information for a customer.

Prompt	Response	Description
REQ	PRT	Print VDN information.
TYPE	VNS	Virtual Network Services.
CUST		Customer number **Note:** At least one D-Channel must be configured with USR = VNS or USR = SHAV and having VNS = Customer number.
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
		The VNS information is output for the customer. For a range of VDNs, the first VDN is displayed, followed by "—" and the last VDN of the block. On the same line, the number of VDNs in the block is displayed in brackets. For a single VDN, the VDN is displayed followed by "(1)". If a block is disabled, the above indication is followed by the number of VNS calls still using a VDN in the block. These calls have to be cleared before the VDN block can be removed. At the end, the total number of VDNs configured for the customer is output. A sample output could be: 7676 (1) 8100—8199 (100) TOTAL NUMBER OF VDN FOR CUST 2: 101 If the VDN block 8100-8199, containing 100 VDNs, is disabled, the output would be: 7676 (1) 8100—8199 (100) *DISABLED - VDN USED: 2* TOTAL NUMBER OF VDN FOR CUST 2: 101 In this case, the VDN block is disabled and two VNS calls are still using two VDNs. These two calls must first be cleared before the VDN block 8100-8199 can be removed.

Table 213: LD 86: Define the maximum number of VNS trunks allowed on the route list entry.

Prompt	Response	Description
REQ	NEW	Add new data.
	CHG	Change existing data.
CUST		Customer number
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
FEAT	RLB	Route list data block feature.
RLI	0-MXRL	The Route List Index to be associated with the VNS Bearer Channel.
ENTR	0-63	The entry within the Route List Index to be associated with the VNS Bearer Channel.
ROUT		Route number **Note:** This is the route number associated with the incoming VNS Bearer channel.
	0-511	Range for Large System , Media Gateway 1000B, and CS 1000E system.
VNS	YES	Virtual Network Services.
...		
VTRK	1-(20)-254	Number of VNS Trunks allowed on the route.

Feature operation

No specific operating procedures are required to use this feature.

Chapter 55: Zone Based Dialing

Contents

This section contains the following topic:

Feature description

Use the Zone Based Dialing (ZBD) feature to replace a nodal PBX network with one or more high-capacity soft switches and branch gateways for Public Switched Telephone Network (PSTN) access. New customers, who plan to setup a private network in multiple locations, can deploy ZBD.

For more information about ZBD, see *Avaya Dialing Plans Fundamentals, NN43001-283*.

Chapter 56: Engineering and configuration guidelines

Contents

This section contains information on the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Description

This section contains the ISDN guidelines for compatible system software and hardware configurations. This includes:

- system compatibility information
- configuration parameters
- transmission characteristics
- software package requirements
- hardware requirements
- disk-drive upgrade requirements
- cable information
- data characteristics
- loss and level plan information

For detailed instructions on hardware installation, refer to *Avaya ISDN Primary Rate Interface Installation and Commissioning, NN43001-301*.

System compatibility

The ISDN software supports the Large Systems

Inter-system compatibility

PRI Transmission characteristics

There are five characteristics of transmission necessary for ISDN PRI compatibility. These are:

- carrier-system compatibility
- synchronization
- signaling

- trunk-type support
- voice and data transmission compatibility

Carrier system compatibility

PRI is compatible with carrier systems which:

- use CEPT G.703 framing on repeater cables;
- use the CEPT G.703 interface (such as fiber optic, microwave, copper, satellite, and infrared transport);
- meet CCITT Q.921 and Q.931 recommendations; and
- use HDB3 line coding at 75-ohm coaxial or 120-ohm twisted-pair interfaces.

Synchronization

PRI is Stratum 3 compatible (accuracy, jitter, pull-in range).

Signaling

ISDN D-channel signaling is used for Primary Rate Access.

Trunk type support

PRI supports the following trunk types:

- Tie (2-wire E&M, 4-wire E&M)
- Foreign Exchange (FX)
- WATS
- PBX-to-Public Exchange trunks; also known as Central Office (CO) trunks
- Direct Inward Dial (DID or DDI) trunks

Voice connections

Voice transmission meets the CCITT standard for flexible loss-and-level plan.

Data connections

PRI supports the following Transmission modes:

- asynchronous 50 bit/s to 19.2 Kbit/s
- synchronous 1200 bit/s to 64 Kbit/s
- half or full duplex

Primary Rate Interface (PRI) hardware requirements

The following hardware is required to equip ISDN PRI on Meridian 1 Large Systems:

- NT6D11(AB/AE/AF) D-Channel Interface (DCH) card (for 2.0 Mbit PRI)
- QPC757 D-channel Interface (DCH) for (1.5 Mbit PRI)
- NT6D80 Multipurpose Serial Data Link (MSDL) card
- NTBK51 Downloadable D-Channel Daughterboard (DDCH), used as an option to the NT6D80 MSDL, the NT5D97 dual-port DTI2/PRI2 card, or the NT5D12 dual-port 1.5 Mbit DTI/PRI card
- NT8D72 (AB/BA) PRI2 card
- NT5D97 dual-port DTI2/PRI2 card
- QPC720 1.5 Mbit PRI card
- NT5D12 dual-port 1.5 DTI/PRI card
- QPC471 or NTRB53 Clock Controller

Note:

The QPC471 and NTRB53 Clock Controllers cannot be mixed in one system. Vintages A through G of the QPC471 Clock Controller can be used in one system; vintage H of QPC471 Clock Controllers cannot be mixed with Clock Controllers of other vintages.

Additional hardware is also required for PRI capability and applications. Installation instructions are given in other Avaya publications, or supplied by the manufacturer. This additional hardware includes:

- QPC414 Network card
- Channel Service Unit (CSU)
- Echo canceller

Note:

Meridian 1 PBX 81Cor CS 1000M MGrequirements are fulfilled by the NT6D66 Call Processor (CP) card.

- QMT8 Asynchronous Data Module (ADM)

ISDN Signaling Link (ISL) hardware

The following hardware is required for ISDN Signaling Link (ISL) capability and applications.

Equipment required for shared mode capability:

- NT6D11(AB/AE/AF) D-Channel (DCH) card (for 2.0 Mbit PRI)
- QPC757 D-channel (DCH) for (1.5 Mbit PRI)
- NT6D80 Multipurpose Serial Data Link (MSDL) card
- NTBK51 Downloadable D-Channel Daughterboard (DDCH), used as an option to the NT6D80 MSDL, the NT5D97 dual-port DTI2/PRI2 card, or the NT5D12 dual-port 1.5 Mbit DTI/PRI card
- NT8D72 (AB/BA) PRI2 card
- NT5D97 dual-port DTI2/PRI2 card
- QPC720 1.5 Mbit PRI card
- NT5D12 dual-port 1.5 DTI/PRI card
- QPC471 or QPC775 Clock Controller

Equipment required for dedicated mode using leased lines:

- NT6D11(AB/AE/AF) D-Channel (DCH) card (for 2.0 Mbit PRI)
- QPC757 D-channel (DCH) for (1.5 Mbit PRI)
- NT6D80 Multipurpose Serial Data Link (MSDL) card
- NTBK51 Downloadable D-Channel Daughterboard (DDCH), used as an option to the NT6D80 MSDL
- modem set in synchronous mode

Equipment required for dedicated mode using a dial-up modem:

- NT6D11(AB/AE/AF) D-Channel (DCH) card (for 2.0 Mbit PRI)
- QPC757 D-channel (DCH) for (1.5 Mbit PRI)
- NT6D80 Multipurpose Serial Data Link (MSDL) card
- NTBK51 Downloadable D-Channel Daughterboard (DDCH), used as an option to the NT6D80 MSDL

- modem with auto-dial capability

Note:
This configuration is the least reliable due to lockup problems inherent in Smart Modems from power spikes and noisy lines. To increase the reliability on this configuration, use a constant power source when powering the modems. Also, verify that TIE lines meet data grade specifications. Avaya takes no responsibility for ISL D-Channel outages due to modem lockup.

- 500 set line card

Equipment required for dedicated mode using a DTI/DTI2 trunk:

- NT6D11(AB/AE/AF) D-Channel (DCH) card (for 2.0 Mbit PRI)
- QPC757 D-channel (DCH) for (1.5 Mbit PRI)
- NT6D80 Multipurpose Serial Data Link (MSDL) card
- NTBK51 Downloadable D-Channel Daughterboard (DDCH), used as an option to the NT6D80 MSDL
- NT5D97 dual-port DTI2/PRI2 card
- QPC472 1.5 Mbit DTI card or NT5D12 dual-port 1.5 DTI/PRI card
- QMT8 Asynchronous Data Module (ADM), QMT11 Asynchronous/Synchronous Interface Module (ASIM) or QMT21 High Speed Data Module (HSDM)
- Data line card

Cable and channel information

The following sections contain cable and channel information.

Cable distance

The cable type used is a 2-pair twisted wire. Maximum cable distances are:

- 200 m (655 ft) from the system to cross-connect point (using ARAM or ABAM equivalent cable)
- 229 m (750 ft) from the system to Office Repeater Bay

Configuration parameters

There are two types of configuration parameters:

- line rate
- T1 and E1 compatibility

The line rate is 1.544 Mbit for T1 and 2.048 Mbit for E1.

The integrated voice and data can use a single medium to transmit speech and data between locations.

There are three advantages to T1 or E1 compatibility:

- E-link or T-link version 2 supports system to system, system to SL-100, and system to Custom DMS-100 for 56 or 64 Kbit/s data, and system to Central Office connectivity.
- includes capability to be configured as a standard T1 DS-1 link
- eliminates need for channel bank equipment when using digital network facilities

Data characteristics

PRI utilizes Avaya T-link Data Rate Adaptation protocol. There are three transmission modes:

- asynchronous 50 bit/s to 19.2 Kbit/s
- synchronous 1200 bit/s to 64 Kbit/s
- half or full duplex

Transmission characteristics

There are five types of transmission necessary for ISDN compatibility:

- carrier system compatibility
- synchronization
- signaling
- trunk types supported
- voice transmission

These transmission types are described in the lists that follow.

Carrier system compatibility:

- compatible with D2, D3, D4, B8ZS, and Extended superframe format (ESF) framing on T1 repeater cables
- compatible with systems that use a DS-1 interface, such as fiber optics, microwave, copper, satellite, and infrared
- meets CCITT Q.921 and Q.931 recommendations
- complies with T1D1 minimal subset

Synchronization: stratum 3 compatible (accuracy, jitter, pull-in range)

Signaling:

- in PRI mode: ISDN D-channel signaling
- in DTI mode: loop start, ground start, E&M, DTMF, and dial pulse
- in ITA mode: PRI trunks use PRI mode and DTI trunks use DTI mode

Trunk types supported:

CO, FX, WATS, DID, TIE (2-wire E&M, 4-wire E&M)

Voice transmission:

meets EIA Digital PBX Draft Standard PN-1429 requirements such as loss and level, distortion, and delay

Note:
ISDN meets the Radio Frequency Interference (RFI) requirements.

Loss and level plan

The loss plan for PRI has been added to the existing system loss matrix (the EIA loss plan).

PRI loss and level plan shows the connections on a port-to-port basis and the corresponding loss values (in dB) for both directions of transmission.

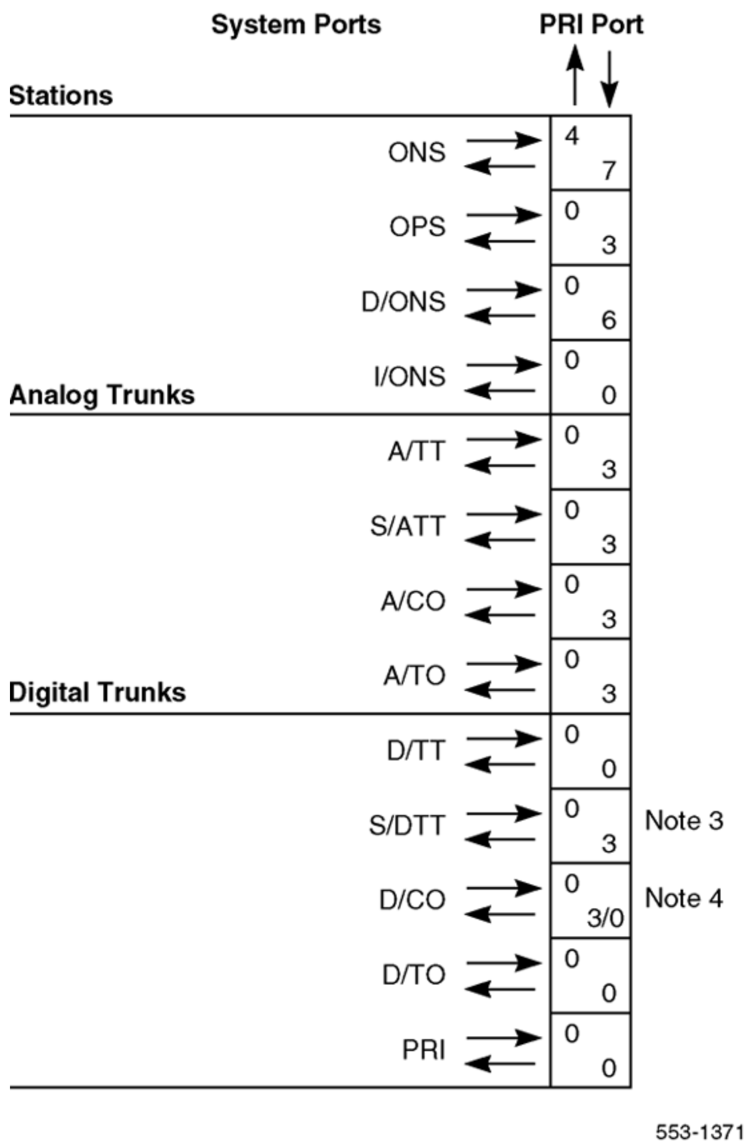

Figure 128: PRI loss and level plan

Note:

The loss is bidirectional. For example, the A/TT coordinate indicates a nominal port-to-port loss of: 0 dB from the A/TT interface to the Primary Rate Interface (PRI) 3 dB loss from the Primary Rate Interface (PRI) to the A/TT interface

Note:

The table column is shown; the loss table has a corresponding row.

Note:

For echo control reasons, this connection cannot be loss-less.

Note:

The value of 0 dB in the PRI-D/CO direction is the long-term objective. The value of 3 dB is to be used for connections to D/COs that have not been programmed for inserting receive-side loss on PRI to local loop connections.

Legend:

ONS	Line interface/on premise line
OPS	Line interface/off premise line
D/ONS	Digital line interface/on premise line
I/ONS	ISDN terminal (on premise)
A/TT	Analog trunk interface/analog TIE trunk
S/ATT	Analog trunk interface/analog satellite PBX TIE trunk
A/CO	Analog trunk interface/analog CO trunk
A/TO	Analog trunk interface/analog toll office trunk
D/TT	Digital trunk interface/digital or combination TIE trunk
S/DTT	Digital trunk interface/digital satellite PBX TIE trunk
D/CO	Digital trunk interface/digital or combination CO trunk
D/TO	Digital trunk interface/digital or combination toll office trunk
PRI	Primary Rate Interface

Call connection limitations

Call connection restrictions limit user access to networks and features by allowing users to set the following limits:

- number of tandem connections
- number of call redirections
- number of PSTNs; can be one or unlimited
- number of ?/A-law conversions
- number of satellite delays

These restrictions apply only within an ISDN environment. Limitations also prevent trunk lockup by allowing only one trunk without disconnect supervision to participate in a call connection. (Trunks providing disconnect supervision include CO/FX/WATS, CO, DID, TIE, CCSA, 2MB DTI trunks, and ISDN.) If multiple call transfers, conferences, or other situations cause two or more unsupervised trunks to be connected, call connection restrictions might not be effective.

Call connection restrictions override the Satellite Link Control feature. If the two features conflict (for example, Satellite Link Control limits satellite hops to one and call connection restrictions permit five hops), call connection restrictions prevail.

Prompts in LD 15 permit configuration of Call Connection Restrictions.

Table 214: LD 15: Configure Call Connection Restriction.

Prompt	Response	Description
REQ	CHG	Change existing data.
TYPE	NET	Networking Data.
CUST		Customer number
	0-99	Range for Large System , Media Gateway 1000B, and CS 1000E system.
ISDN	YES	ISDN option; must be set to YES to see following call connection restriction prompts.
...		
- RCNT	0–(1)–5	Number of call redirections allowed in a call connection.
- PSTN	YES (NO)	YES limits the number of PSTNs allowed in a call connection to 1. NO permits unlimited PSTNs.
- - TNDM	0–(15)–31	Number of tandem connections allowed in a call connection.
- - PCMC	0–(15)–31	Number of PCM (μ/A-law) conversions permitted in a network connection.
- - SATD	0–(1)–5	Number of satellite delays allowed in a network connection.

Software packages

The following tables list the software features and their corresponding packages.

Note:

To upgrade current ISDN software, see *Avaya Communication Server 1000M and Meridian 1 Large System Upgrades Overview, NN43021-458*.

Note:

Package 19 is required for receiving CLID or NCPND.

Note:

Package 75, PBX interface, is not required for ISL (package 147), unless ISL is over DTI. For ISL over analog trunks, ESN # 2 or 3 signaling is required. ESN # 5 signaling can be used if package 75 is installed.

Note:

CDP (package 59) requires packages 28 and 61. Packages 28 and 61 are not required for NARS (package 58).

Note:

If the user dials a Location code, package 58 must be equipped at the originating and the receiving system. If CDP is used, package 59 needs to be equipped at both sites.

Note:

Package 117 is also required in ISA configurations.

Note:

Multi-purpose Serial Data Link (MSDL) cards (NT6D80) require package 222 for D-channel (and Application Module Link) operations.

Table 215: Software packages

Features	Package dependencies
64 Kbit/s Clear Data Transport	75, 145, 146
Attendant Blocking of Directory Number (ABDN)	14, 28, 32, 58, 75, 127, 145, 146 or 147, 159
Attendant and Network Wide Remote Call Forward	1, 18, 58, 59, 73, 139, 145
Backup D-channel	75, 145, 146 or 147
Basic Call Service	75, 145, 146 or 147
Call Forward, Break-In, Hunt Internal or External Network Wide	159, 263
Call Page Network Wide	307
Call Park Network Wide	306, 159, 33
Calling Line Identification (CLID)	19, 75, 145, 146 or 147
CLID in CDR record	4, 5, or 6, 118, 75, 145, 146 or 147

Features	Package dependencies
AT&T 4ESS	75, 145, 146
Custom AT&T 5ESS	75, 145, 146, 149
Custom DMS100	75, 145, 146
Data Packet Network (DPN) access	75, 145, 146
Display of Calling Party Denied	95, 145, 159
DTI Backwards Compatibility	75
DTI with Extended Superframe (ESF)	75, 145, 146
E.164/ESN Numbering Plan Expansion	19, 57, 58, 145, 146, 147, 160, 203, 216, 222, 235, 263
ESN over ISL or Primary Rate Interface	14, 32, 37, 39, 58 or 59, 75, 145, 146
Integrated Services Access (ISA)	75, 117, 145, 146
Integrated Trunk Access (ITA)	75, 145, 146
ISDN CLID Enhancements	145
ISDN Signaling Link (ISL)	75, 145, 147
Local trunk queuing over PRI/ISL (offhook or call back queuing)	14, 28, 32, 37, 58 or 59, 62, 75, 145, 146 or 147
Meridian Mail Trunk Restriction	46
Multi-purpose Serial Data Link (MSDL)	222
NCOS over ISDN Signaling Link (ISL)	14, 32, 37, 39, 58 or 59, 75, 145, 147
NCOS over Primary Rate Interface to Custom DMS-100	14, 32, 37, 39, 58 or 59, 75, 145, 146
National ISDN-2 (NI-2)	145, 146, 222, 291
Network Attendant Service (NAS)	14, 28, 32, 58, 59, 61, 75, 127, 145, 146 or 147, 148, 159, 161, 192
Network Call Forwarding	14, 32, 58 or 59, 75, 145, 146 or 147
Network Call Party Name Display (NCPND)	19, 75, 95, 145, 146 or 147
Network Call Redirection (NCRD)	145, 146 or 147
Network Message Services (NMS)	14, 32, 58 or 59, 75, 77, 145, 146 or 147, 148, 175
Network Ring Again (NRAG)	14, 32, 58 or 59, 75, 145, 146 or 147,148
Network Wide Listed Directory Numbers	14, 32, 58, 75, 76, 145, 146 or 147, 159
Non-Associated Signaling (nB +D)	75, 145, 146 or 147
PRI to DMS-250 or AT&T 4ESS	75, 145, 146, 149

Features	Package dependencies
Private Network Hopoff and Overflow	14, 28, 32, 58 or 59, 61, 75, 145, 146 or 147
QSIG Basic Call	263, 19, 145, 146, 222
QSIG Call Completion	263, 305, 316
QSIG GF Transport	263, 305
QSIG Name Display	19, 95, 139, 263, 305
Remote Virtual Queuing	192
T-1 Frame Slippage Auto-recovery	75, 145, 146
Trunk Anti-Tromboning	312, 145, 146 or 147, 148, 222
Trunk Optimization (TRO)	145, 146 or 147, 148
VNS VDN Expansion	14, 32, 58, 145, 146, 147, 148, 161, 183

Software and hardware compatibility

The different configurations within an ISDN environment are supported by different sets of features and services. As ISDN evolves, more and varied configurations are supported. These different configurations have their own software and hardware dependencies, as listed in the following tables.

The tables in this section describe the following configurations:

- System software and hardware compatibility
- System connectivity to SL-100, Custom DMS-100, and DMS-250, with software and hardware compatibility
- System connectivity to AT&T 4ESS and Custom AT&T 5ESS software and hardware compatibility
- System connectivity to National ISDN-2 (NI-2) software and hardware compatibility

Conventions within the following tables are:

- LF = limited functionality (the two items do interact, but call functions are somewhat limited compared to a different configuration)
- N = no, or "not supported"
- - = not applicable, or it does not apply to this configuration
- NR = not recommended for this configuration
- Y = yes, it is supported

Table 216: System software and hardware compatibility

Features	720 A	720 B	720 C/ E*	720 F**	757 A	757 B	757 C	757 D	757 E	NT 6D80A A***	NT 6D 80 AB ***	NT 5D 12 DD P****
* The QPC720D was not introduced in North America (it is only used in Hong Kong.) ** The QPC720F has been introduced to handle NI-2, and R22 and higher software features. *** The NT6D80AA MSDL supports R18 - R20 inclusive. The NT6D80AB supports R21 and higher. *** Includes the NTBK51AA/NTBK51CA Downloadable D-Channel Daughterboard.												
Attendant Blocking of DN	N	N	Y	Y	N	N	N	N	N	N	Y	Y
Attendant Netwide RCFW	N	N	Y	Y	N	N	N	N	N	Y	Y	Y
Att/Net RCFW	N	N	Y	Y	N	N	N	N	N	Y	Y	Y
Backup D-channel	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
Basic Call Service	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CFW, Break-In, Hunt Internal, External Netwide	N	N	Y	Y	N	N	N	N	N	N	Y	Y
CFW/Hunt Override FFC	N	N	Y	Y	N	N	Y	Y	Y	N	Y	Y
Call Page Netwide	N	N	Y	Y	N	N	N	Y	Y	N	Y	Y
Call Park Netwide	N	N	Y	Y	N	N	N	N	N	N	Y	Y
Call Pickup Network Wide	N	N	Y	Y	N	N	N	N	N	N	Y	Y
Calling Line ID	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Calling Party Privacy	N	N	Y	Y	N	N	Y	N	N	N	Y	Y
CLID in CDR	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
DCH Error Report and Monitoring	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y
DTI, ESF, CRC	Y	Y	Y	Y	-	-	-	-	-	-	-	-
Display of Calling Party Denied	N	N	Y	Y	N	N	N	N	Y	N	Y	Y
DTI Compatibility	Y	Y	Y	Y	-	-	-	-	-	-	-	Y

Features	720 A	720 B	720 C/E*	720 F**	757 A	757 B	757 C	757 D	757 E	NT 6D80AA***	NT 6D80AB***	NT 5D12DDP****
Electronic Lock Net/ Private Line	N	N	Y	Y	N	N	N	N	Y	N	Y	Y
E.164/ESN Numb Plan Expansion	N	N	Y	Y	N	N	N	N	Y	N	Y	Y
ESN over PRI	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Incoming Trunk Program. CLID	N	N	Y	Y	N	N	N	N	N	N	Y	Y
ISDN CLID Enhancements	N	N	Y	Y	N	N	N	N	Y	N	Y	Y
ISL*	Y	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y
ISL (Conventional)*	N	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y
ITA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Meridian Mail Trunk Restriction	N	N	Y	Y	N	N	N	N	N	N	Y	Y
NACD	N	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y
NAS	N	N	Y	Y	N	N	N	N	Y	Y	Y	Y
National ISDN 2 TR-1268 PRI	N	N	N	Y	N	N	N	N	N	N	Y	Y
* Features must be compatible with the transport.												
nB + D	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NCPND	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NND	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y
NCRD												Y
— NCFAC	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
— NCFB	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
— NCFNA	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
— NHNT	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
NWLDN	N	N	Y	Y	N	N	Y	Y	Y	Y	Y	Y
— NXFER	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
Network Call Trace	N	Y	Y	Y	N	N	N	N	Y	Y	Y	Y

Features	720 A	720 B	720 C/E*	720 F**	757 A	757 B	757 C	757 D	757 E	NT 6D80AA***	NT 6D80AB***	NT 5D12DDP****
Network Intercom	N	N	Y	Y	N	N	N	N	N	N	Y	Y
B8ZS	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NMS-MC	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
NMS-MM	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
NRAG	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
QSIG Basic Call	N	N	N	Y	N	N	N	N	N	N	Y	Y
QSIG Call Completion	N	N	N	Y	N	N	N	N	N	N	Y	Y
QSIG GF Transport	N	N	N	Y	N	N	N	N	N	N	Y	Y
QSIG Name Display	N	N	N	Y	N	N	N	N	N	N	Y	Y
64 K Clear Data	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Remote Virtual Queuing	N	N	Y	Y	N	N	N	N	Y	Y	Y	Y
Trunk Anti- Tromboning	N	N	Y	Y	N	N	N	N	N	N	Y	Y
TRO	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
T1 Frame Slip Auto-recovery*	N	Y	Y	Y	-	-	N	N	-	-	-	Y*
T309 Timer	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Virtual Network Services	N	N	Y	Y	N	N	N	N	Y	N	Y	Y
VNS VDN Expansion	N	N	Y	Y	N	N	N	N	Y	N	Y	Y
* Without the NTBK51AA/NTBK51CA.												

Table 217: System compatibility with connectivity to SL-100, Custom DMS-100, DMS-250

Features	720 A	720 B	720 C/E*	720 F**	757 A	757 B	757 C	757 D	757 E	NT 6D80AA***	NT 6D80AB***	NT 5D12DDP****
* The QPC720D was not introduced in North America (it is only used in Hong Kong.) ** The QPC720F has been introduced to handle NI-2, and R22 and higher software features.												

Features	720 A	720 B	720 C/E*	720 F**	757 A	757 B	757 C	757 D	757 E	NT6D80AA ***	NT6D80AB ***	NT5D12DDP****
*** The NT6D80AA MSDL supports R18 - R20 inclusive. The NT6D80AB supports R21 and higher. *** Includes the NTBK51AA/NTBK51CA Downloadable D-Channel Daughterboard.												
Backup D-channel	N	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y
nB+D	N	N	Y	Y	N	N	N	N	Y	Y	Y	Y
Basic Call Service	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Calling Line ID	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
CLID in CDR	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
DPN access	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
DTI, ESF, CRC	Y	Y	Y	Y	-	-	-	-	-	-	-	-
DTI Compatibility	Y	Y	Y	Y	-	-	-	-	-	-	-	Y
ESN over PRI	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ISA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NND	Y	Y	Y	Y	N	N	N	N	Y	Y	Y	Y
NCRD												Y
— NCFAC	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
— NCFB	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
— NCFNA	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
— NHNT	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
NRAG (TIE)	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
B8ZS	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NRAG	N	Y	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
64 K Clear Data	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Private Network Hopoff	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
T1 Frame Slip Auto-recovery*	N	Y	Y	Y	-	-	-	-	-	-	-	Y*
* Without the NTBK51AA/NTBK51CA.												

Table 218: System software and hardware compatibility with connectivity to AT and T 4ESS

Features	720 A	720 B	720 C/E*	720 F**	757 A	757 B	757 C	757 D	757 E	NT6D80AA***	NT6D80AB***	NT5D12DDP****
* The QPC720D was not introduced in North America (it is only used in Hong Kong.) ** The QPC720F has been introduced to handle NI-2, and R22 and higher software features. *** The NT6D80AA MSDL supports R18 - R20 inclusive. The NT6D80AB supports R21 and higher. *** Includes the NTBK51AA/NTBK51CA Downloadable D-Channel Daughterboard.												
ANI in CDR	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ANI Station ID	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Backup D-channel	N	N	Y	Y	N	Y	Y	Y	Y	Y	Y	Y
Basic Call Service	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ISA/CBC	N	Y	Y	Y	N	N	N	Y	Y	Y	Y	Y
DTI, ESF, CRC	Y	Y	Y	Y	-	-	-	-	-	-	-	-
nB+D	N	N	Y	Y	N	Y	Y	Y	Y	Y	Y	Y

Table 219: System software and hardware compatibility with connectivity to Custom AT and T 5ESS

Features	720 A	720 B	720 C/E*	720 F**	757 A	757 B	757 C	757 D	757 E	NT6D80AA***	NT6D80AB***	NT5D12DDP****
* The QPC720D was not introduced in North America (it is only used in Hong Kong.) ** The QPC720F has been introduced to handle NI-2, and R22 and higher software features. *** The NT6D80AA MSDL supports R18 - R20 inclusive. The NT6D80AB supports R21 and higher. *** Includes the NTBK51AA/NTBK51CA Downloadable D-Channel Daughterboard.												
ANI Station ID	N	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y
Basic Call Service	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
ISA/CBC	N	Y	Y	Y	N	N	N	N	Y	Y	Y	Y

Table 220: System software and hardware compatibility with NI-2

Features	720 A	720 B	720 C/ E*	720 F**	757 A	757 B	757 C	757 D	757 E	NT 6D 80 AA ***	NT 6D 80 AB ***	NT 5D 12 DD P** **
* The QPC720D was not introduced in North America (it is only used in Hong Kong.) ** The QPC720F has been introduced to handle NI-2, and R22 and higher software features. *** The NT6D80AA MSDL supports R18 - R20 inclusive. The NT6D80AB supports R21 and higher. *** Includes the NTBK51AA/NTBK51CA Downloadable D-Channel Daughterboard.												
Bearer capability	N	N	N	Y	N	N	N	N	N	N	Y	Y
Basic Call Service	N	N	N	Y	N	N	N	N	N	N	Y	Y
Calling Party Number	N	N	N	Y	N	N	N	N	N	N	Y	Y
nB+D	N	N	N	Y	N	N	N	N	N	N	Y	Y
Backup D-channel	N	N	N	Y	N	N	N	N	N	N	Y	Y

Table 221: System software and hardware compatibility

Services	720A	720B	720C	757A	757B	757C	757D	757E	MSDL
QPC720A	Y	LF	LF	Y	Y	LF	LF	LF	N
QPC720B	LF	Y	LF	N	LF	Y	Y	Y	N
QPC720C/E	LF	LF	Y	N	LF	Y	Y	Y	Y
QPC720F	LF	LF	Y	N	LF	Y	Y	Y	Y
QPC757A	Y	N	N	Y	LF	LF	LF	LF	LF
QPC757B	Y	LF	LF	LF	Y	LF	LF	LF	LF
QPC757C	LF	Y	Y	LF	LF	Y	LF	LF	LF
QPC757D	LF	Y	Y	LF	LF	LF	Y	LF	LF
QPC757E	LF	Y	Y	LF	LF	LF	LF	Y	LF
NT6D80 (MSDL)	N	N	Y	N	N	N	Y	Y	Y
NT5D12/w NTBK51AA/ NTBK51CA	LF	LF	Y	N	LF	Y	Y	Y	Y
Y = (supported); N = not supported; NR = not recommended; LF = limited functionality (items interact, but call functions could be limited)									

System connectivity

ISDN signaling connectivity is supported between the system and the following products:

- Meridian 1and CS 1000M
- SL-100
- Custom DMS-100 and DMS-250
- AT&T 4ESS
- Custom AT&T 5ESS

Central Office connectivity:

- Asia Pacific, consisting of:
    - Australia (private or alternative carrier)
    - China
    - Hong Kong
    - India
    - Indonesia
    - Japan
    - Malaysia
    - New Zealand
    - Philippines
    - Singapore
    - Taiwan
    - Thailand
- Australia ETSI
- AXE-10 Australia (non-Asia Pacific ISDN Connectivity)
- AXE-10 (Sweden)
- EuroISDN
- Japan D70 (non-Asia Pacific ISDN Connectivity)
- NEAX-61 (New Zealand) (non-Asia Pacific ISDN Connectivity)
- Numeris VN3 (France)
- SwissNet (Switzerland)

- SYS-12 (Norway)
- 1TR6 (Germany)

Table 222: E1 and T1 Supported Interfaces on CS 1000

ISDN Interface	E1 (30B+D)	T1 (23B+D)
Australia ETSI	Y	N
AXE-10 (Sweden and Australia)	Y	N
Swiss Net (Switzerland)	Y	N
NEAX-61 (New Zealand) (non-Asia Pacific ISDN Connectivity)	Y	N
SYS-12 (Norway)	Y	N
Numeris VN3 (France)	Y	N
1TR6 (Germany)	Y	N
Japan D70 (non-Asia Pacific ISDN Connectivity)	N	Y
Euro ISDN ETS 300-102 basic protocol	Y	N
Austria	Y	N
Denmark	Y	N
Finland	Y	N
Germany	Y	N
Italy	Y	N
Norway	Y	N
Portugal	Y	N
Sweden	Y	N
Ireland	Y	N
Holland	Y	N
Switzerland	Y	N
Belgium	Y	N
Spain	Y	N
United Kingdom	Y	N
France	Y	N
Commonwealth of Independent States (Russia and the Ukraine)	Y	N
Asia Pacific	Y	N

ISDN Interface	E1 (30B+D)	T1 (23B+D)
Australia	Y	N
China	Y	N
Hong Kong	N	Y
India	Y	N
Indonesia	Y	N
Japan	N	Y
Malaysia	Y	N
Philippines	Y	N
Singapore	Y	N
Taiwan	Y	N
New Zealand	Y	N
Thailand	Y	N
QSIG	Y	Y
JTTC (Japan QSIG)	N	Y
SL-1	Y	Y
D100	N	Y
D250	N	Y
SL100	N	Y
National ISDN 2 (NI-2)	N	Y
ESS4	N	Y
ESS5	N	Y
DPNSS/DASS	Y	N

Cable information

The following list contains cable and channel information. The cable type used is a 2-pair twisted wire.

- 655 ft (200 m) maximum distance from the system to DSX-1 cross-connect point (using ARAM or ABAM equivalent shielded cable)
- 750 ft (229 m) maximum distance from the system to Office Repeater Bay

Specific cables are detailed in *Avaya ISDN Primary Rate Interface Installation and Commissioning, NN43001-301*.

Chapter 57: Service verification

Contents

This section contains information on the following topics:

Testing PRI

There are four tests used to test the Primary Rate Interface:

1. PRI local loop back test
2. PRI self-test performed manually

3. PRI automatic loop test
4. PRI remote loop-back test (must run in conjunction with a link diagnostic test at the far end)

PRI local loop back test

This test checks the communication path between the QPC414 Network card and the PRI card. It also checks the leads for the J4. It is often performed when the PRI cannot be enabled. The PRI card must be installed, and a cable connecting its J3 connector to a QPC414 Network card.

1. Disable the D-channel.

   ```
   LD 96
   DIS DCH x
   ```

2. Disable the PRI loop:

   ```
   LD 60
   DISL loop
   ```

3. Disconnect the cable connector from the PRI J4 (if attached). Several LEDs will light on the faceplate.
4. Attach a female 15 pin connector loopback plug to J4. The loopback plug must have pins 1 and 3, and pins 9 and 11 shorted together.
5. Enable the PRI loop:

   ```
   LD 60
   ENLL loop
   ```

   The green ACT LED will light in a few seconds. If so, the test passed. Continue with the following steps.

   If the green ACT light does not come on, retest. Unseat the PRI card between steps 2 and 3.

   If the light still does not turn on, try replacing your QPC414 or PRI cards, or the connecting cable.

6. Remove the loopback plug from the J4 connector.
7. Replace cable connector to the PRI J4 (removed in step 3).
8. Enable the loop:

   ```
   LD 60
   ENLL loop
   ```

9. Enable the DCH:

```
LD 96
ENL DCH x
```

PRI self-test

The self-test checks speech path continuity, zero code suppression, remote alarm detection, and A&B bit signaling. This test is performed manually, for each channel or for each frame (24 channels).

The DCH and PRI must be disabled before performing the self-test or call processing is disrupted. To perform the self-test on a specific loop:

1. Disable DCH:

   ```
   LD 96
   DIS DCH x
   ```

2. Disable the PRI loop and run the self-test:

   ```
   LD60
   DISL  loop
   SLFT  loop
   ```

   When the system returns OK, it indicates that the hardware is operable.

3. Re-enable the PRI loop:

   ```
   LD 60
   ENLL  loop
   ```

   The D-channel will re-enable automatically.

PRI automatic loop test

The automatic loop test checks the same functions as the self-test. Unlike the self-test, it can be run automatically, as part of the midnight routines.

With the ATLP command set to one:

If all 23 channels are idle at midnight, the system disables the card and performs a self-test on all channels.

If any of the 23 channels are busy at midnight, the system disables one idle channel, chosen at random, and checks it while the card is enabled.

With the ATLP command set to zero, only one channel is tested. The channel tested is randomly selected by software; it cannot be specified.

To perform the remote loop-back test, use the following:

```
LD 60 ATLP 1 or 0
```

When ATLP 1 is entered, the TTY prints out AUTO TEST ENBL. When ATLP 0 is entered, the TTY prints out AUTO TEST DSBL.

Link diagnostic and remote loop-back tests

The remote loop-back test and the link diagnostic test are performed manually for each channel or for each frame (23 channels).

Link diagnostic test

The link diagnostic test, also called the far end loop-back test, does not test the system PRI. It puts the PRI in loop-back mode at the far end so a remote loop-back test can be performed on far end equipment. The PRI channel, loop, or frame tested must be disabled.

Remote loop-back test

The remote loop-back test, also called the near end loop back test, checks the integrity of the PRI from the system to the far end. The far end must be put into loop-back mode before this test can be performed. The PRI channel, loop, or frame tested must be disabled.

Coordinating the tests

When a technician at the far end asks for loop-back mode on the system, perform the following steps.

1. Disable the D-channel.

   ```
   LD 96
   DIS DCH x
   ```

2. Disable the PRI loop and activate loop-back mode.

   ```
   LD 60
   DISL  loop
   RLBK  loop
   ```

   The QPC720 LBK LED lights.

When a technician at the far end asks for loop-back mode on the system to be disabled, perform this step.

Disable loopback mode.

```
LD 60
DLBK loop
```

The LBK LED turns off.

When a technician at the far end asks for PRI and DCH to be re-enabled, perform this step.

Enable the PRI loop.

```
LD 60
ENLL loop
```

OK will print out. The D-channel re-enables automatically.

To run the remote loop-back test on the system, call a technician at the far end and ask for loop-back mode at that facility.

When loop-back mode at the far end is confirmed, the technician at the far end follows these steps.

1. Disable the D-channel.

   ```
   LD 96
   DIS DCH N
   ```

2. Disable the PRI loop and run the loop-back test using.

   ```
   LD 60
   DISL  L
   RMST  L
   ```

   SLFT OK prints out to indicate a successful test.

3. Call the far end technician to disable the loopback test, and to re-enable the PRI and DCH. The far end technician enables the PRI.

   ```
   LD 60
   ENLL L
   ```

   OK prints out, and the D-channel re-enables automatically.

PRI remote loop-back and link diagnostic tests shows the relationship between the remote loop-back test and the link diagnostic test.

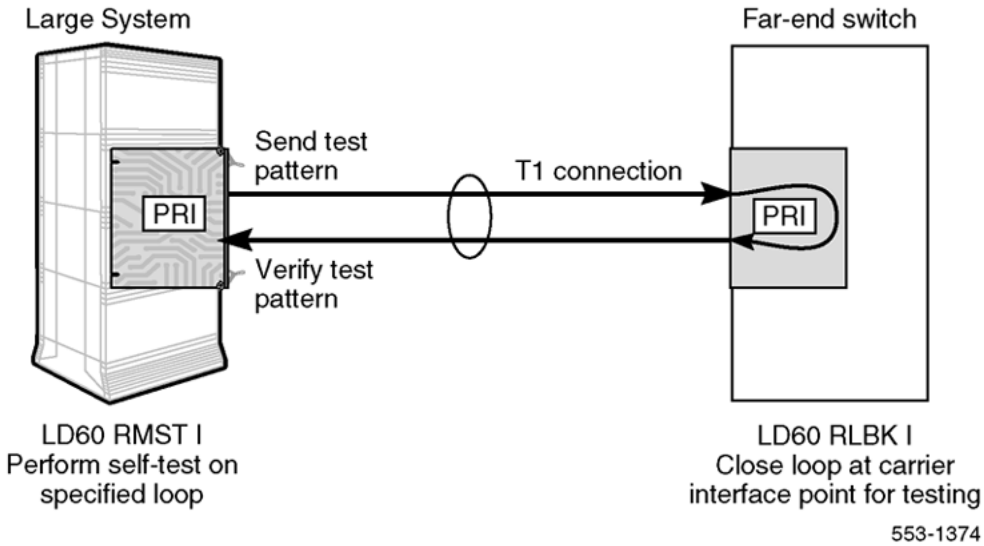

Figure 129: PRI remote loop-back and link diagnostic tests

Testing DCH

This chapter describes the following DCH tests. These tests are supported on the QPC757, NT6D11AB, NT6D11AD DCHI cards. MSDL card (NT6D80) tests are shown later in this chapter.

- Test 100: Interrupt generation
- Test 101: Loop-back mode
- Test 200: Interrupt handler
- Test 201: Interrupt handler-to-link interface

DCH tests 100 and 101

DCH tests 100 and 101 are isolated hardware tests. Test 100 checks interrupt generation on the DCHI card. Test 101 checks the DCHI loop-back capability. If either test fails, either a faulty DCHI or a contention problem is indicated. A test failure initiates DCH error messages. See Figure 130: DCH tests 100 and 101 on page 560.

Tests 100 and 101 must be run in sequential order (tests 200 and 201 can follow). Established calls stay up, but new calls cannot be placed.

The DCH link must be in the reset state when these tests are run. Reset can be accomplished when the status of the D-channel is established (EST) or released (RLS).

To reset:

```
LD 96
STAT
DCH xRST (responds either EST or RLS)
DCH x
```

If the DCHI is disabled, it must be enabled before reset can be established.

To enable the DCHI:

```
LD 96
STAT DCH x (responds RST)
ENL DCH x (if a problem caused the disabled state, RLS occurs; if the
disabled state is cleared, status is EST)
```

To run Test 100 and Test 101 after verifying that the DCH is reset:

```
TEST 100 x
TEST 101 x
```

OK appears when test passes successfully.

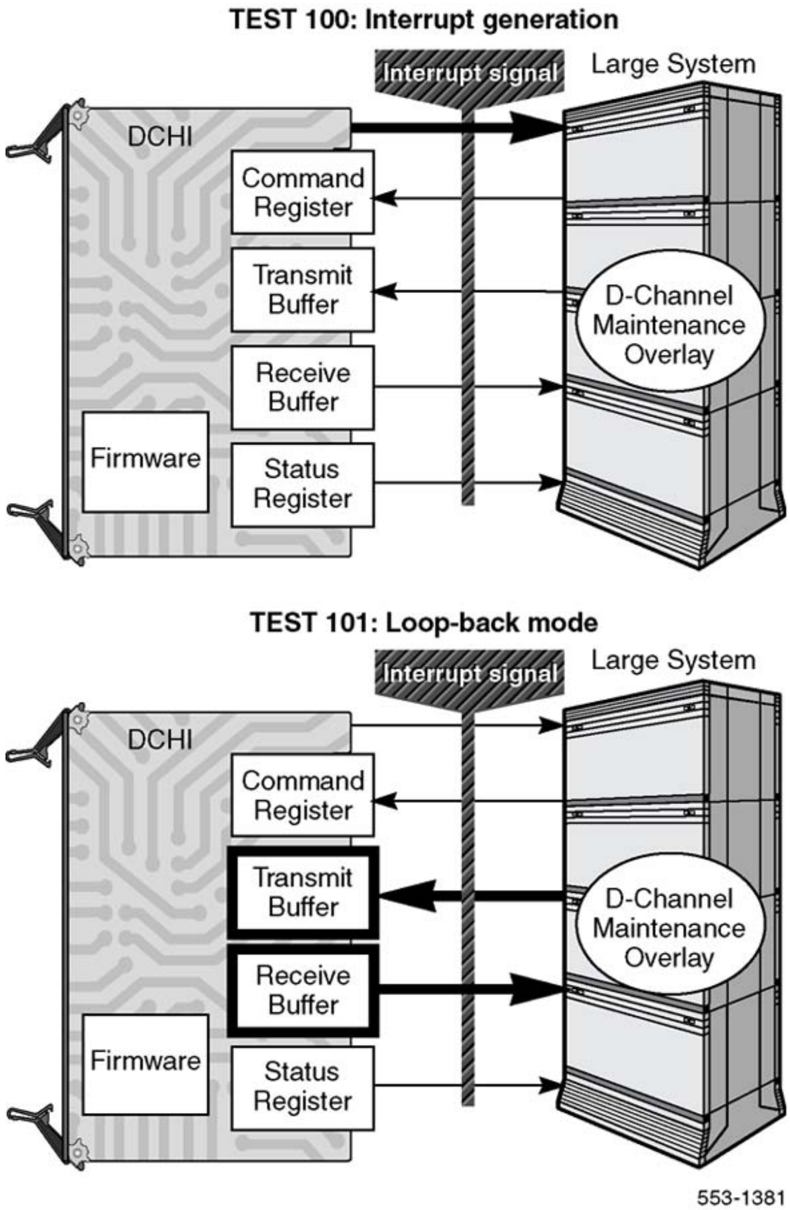

Figure 130: DCH tests 100 and 101

DCH tests 200 and 201

DCH tests 200 and 201 are software tests. See Figure 131: DCH tests 200 and 201 on page 562. Test 200 monitors the DCHI interrupt handler. Test 201 checks the interrupt handler-to-link interface path. A failure of either test indicates software problems. A test failure initiates DCH error messages.

Tests 200 and 201 must be run sequentially after tests 100 and 101. Established calls stay up, but new calls cannot be placed.

The DCH link must be in the reset state when these tests are run. Reset can be established when the status of the D-channel is established (EST) or released (RLS).

To reset:

```
LD 96
STAT DCH x (responds either EST or RLS)
RST DCH x
```

If the DCHI is disabled, it must be enabled before reset can be established.

To enable the DCHI:

```
LD 96
STAT DCH x (responds RST)
ENL DCH x (if a problem caused the disabled state, RLS occurs; if the
disabled state is cleared, status is EST)RST DCH x
```

To run Test 200 and Test 201 after verifying that the DCH is reset:

```
TEST 200 x
TEST 201 x
```

OK appears when test passes successfully.

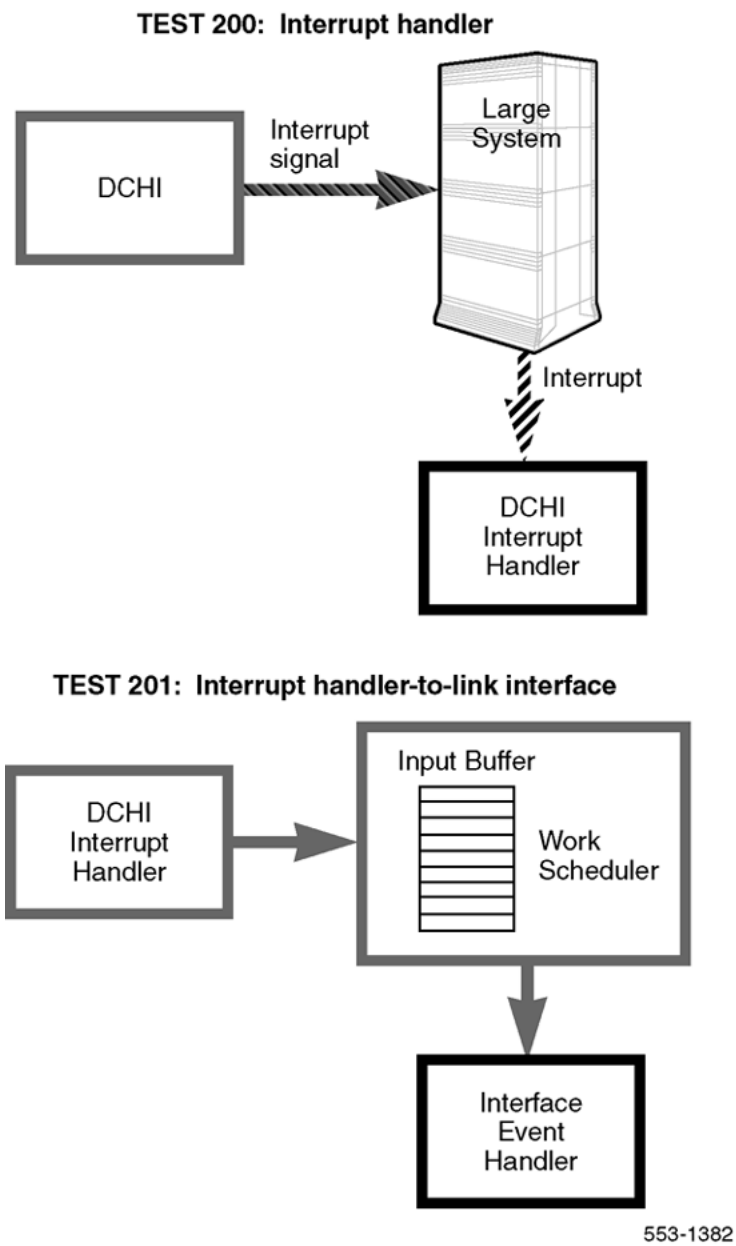

Figure 131: DCH tests 200 and 201

MSDL local loopback test (NT6D80)

To start the local loopback test on the MSDL card, use the following steps. The test checks both MSDL expedited and normal (ring) interfaces.

1. Place MSDL in Test state. Enter `ENL TEST DCH x` x = the D-channel logical address
2. Place the MSDL in local loopback mode. Enter `ENL LLB DCH x` x = the D-channel logical address
3. Perform the test. Enter `TEST LLB DCH x` x = the D-channel logical address

The response for the expedited interface that carries urgent signaling and maintenance messages between the system CPU and the MSDL MPU follows.

```
DCH : X XDU TEST CONFIRM TIME : <time of day>
TEST : PASS (or FAIL)
```

X is the D-channel logical address XDU is the expedient message sent around the loop.

The response for the ring interface that transmits operation data between the system CPU and the MSDL MPU follows.

```
DCH : X DU TEST CONFIRM TIME : <time of day>
TEST : PASS (or FAIL)
```

1. If the test fails, check the status of the MSDL card, used by this DCH link, with the `STAT MSDL x FULL` command.
2. If the MSDL card is faulty, disable the card and perform self-test. `DIS MSDL x` x = the MSDL device number SLFT MSDL xx = the MSDL device number
3. If the card passed the test, the problem might lie in incompatible software.

Refer to *Avaya Circuit Card Reference, NN43001-311*.

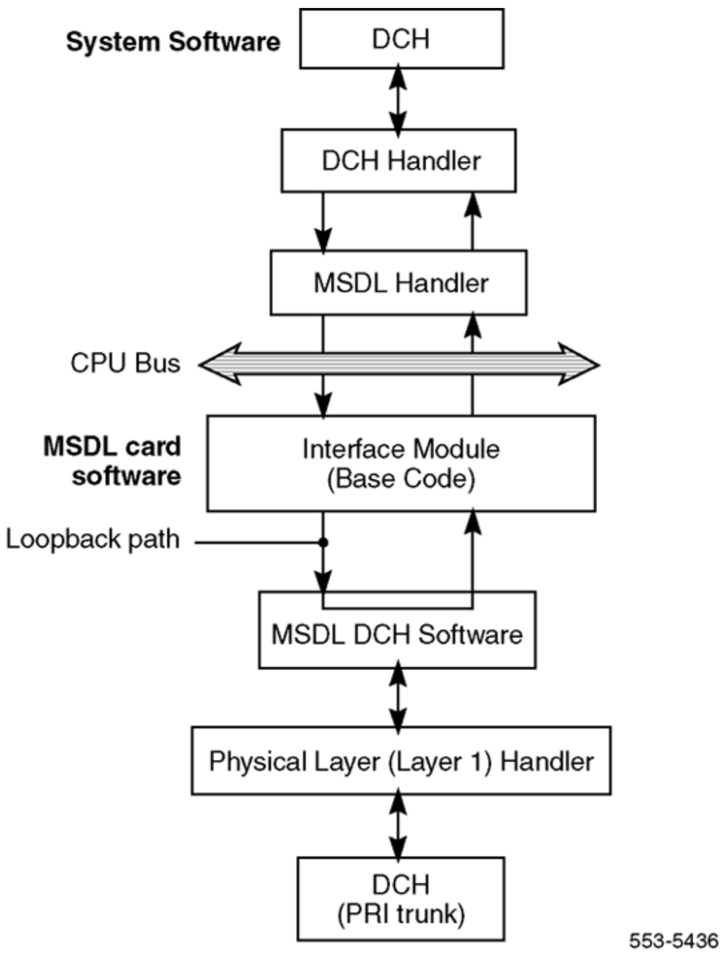

Figure 132: Local loopback test (NT6D80)

MSDL remote loopback tests (NT6D80)

Before beginning this test, verify the following.

- D-channels on both switches are configured on MSDL cards
- DCH links on both switches are set to TEST mode
- DCH at Switch B is in remote loopback mode (RLB)
- remote capability (RCAP) is MSDL

To place DCH links on both systems in TEST mode, enter **ENL TEST DCH x** on Switch A and **ENL TEST DCH y** on Switch B for the same DCH link (**x** is the logical address for the DCH link in Switch A and **y** is the corresponding DCH link in Switch B). The DCH link on both switches are automatically placed in idle state (IDLE).

1. Place the Switch B DCH link in remote loopback state (RLB) with **`ENL RLB DCH x`**. The DCH link in Switch A must stay in idle.
2. Perform the loopback test **`TESTRLB x`** from Switch A.

   The result of the remote loopback test is displayed on Switch A's console in the following format.

   DCH : X RLB TEST CONFIRM TIME : <time of day> TEST : PASS TEST : FAIL - NO DATA RCV FAR END TEST : FAIL - CORPT DATA RCV FAR END TEST : FAIL - REASON UNKNOWN

   TEST : FAIL can indicate a problem in the physical link between the two switches, or faulty equipment in either switch. Check the connections, and verify the status of the MSDL and PRI trunk cards used for this link. Refer to *Avaya ISDN Primary Rate Interface Maintenance, NN43001-717* for detailed troubleshooting procedures.
3. Place the Switch B DCH link back to the idle state, with the **`DIS RLB y`** command.
4. If you think the MSDL card used in either switch has failed, check the status of the DCH link and the status of the MSDL card by entering **`STAT MSDL x FULL`**.
5. If the MSDL card is faulty, disable the card and perform self-test. **`DIS MSDL x`** **`SLFT MSDL x`**
6. If the card passed the test, the problem might lie in incompatible software. Refer to *Avaya Circuit Card Reference, NN43001-311*.

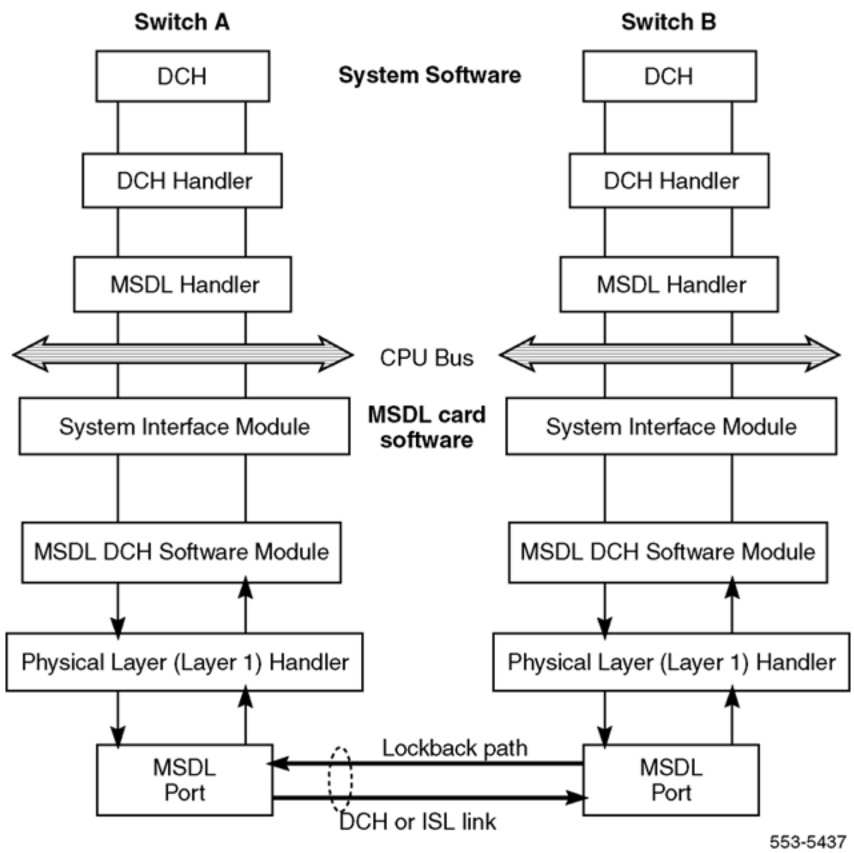

Figure 133: Remote loopback tests (NT6D80)

Testing applications

Calling Line Identification

To verify Calling Line Identification (CLID), do the following:

1. Place a call from the system over a PRI trunk to a terminal with a digit display at the far-end facility.
2. Verify that the call is terminated correctly.
3. Verify that the CLID number displayed on the far-end phone is correct.
4. Have the far end place a call to a system device with a digit display.
5. Verify that the number displayed is the correct CLID number.
6. Verify that the call can be released properly from either end.

Network Call Redirection (system to system connection only)

To verify Network Call Redirection (NCRD), do the following:

1. Place a call from the system over a PRI trunk to a digit display phone at a far-end facility. This far-end facility must be on a different network.
2. To ensure that network redirection takes place, the first dialed number must be in an NCFNA or NCFU condition.
3. Verify that the call is terminated correctly.
4. Verify that the CLID display of the calling party contains the following:
    - Originally called party DN (or redirecting DN)
    - Connected Party DN
    - Reason for redirection
    - Connected Party Name
5. Verify that the CLID display of the connected party contains the following information:
    - Calling party DN
    - Originally called party DN (or redirecting DN)
    - Reason for redirection
    - Calling Party Name
6. Verify that the call can be released properly from either end.
7. Have the far end place a call that is redirected. Then repeat steps 4 and 5.

Network Ring Again (system to system connection only)

To verify Network Ring Again (NRAG), do the following:

1. Coordinate with far-end personnel. Place a call to a busy station at the far end over a PRI trunk.
2. Verify that the calling terminal can activate NRAG and that any ring again indicator lamps are lit.
3. When the far-end call disconnects, verify that the calling terminal is notified.
4. Verify that the far-end number can be dialed through NRAG access.
5. Test the timeout period with far-end personnel.
6. Verify that NRAG can be manually deactivated by the calling terminal.

ISDN Signaling Link (system to system connection only)

To verify the ISDN Signaling Link, do the following:

1. Coordinate with far-end personnel. Place a call over a system switch.
2. As you are dialing, the dialed DN appears on your phone.
3. When the far-end phone is ringing, the CLID of your phone is displayed on the far-end phone.
4. Both phones continue to display the CLIDs when the far end goes off hook.

Appendix A: Call scenarios for name display

Public protocol does not update name display during call transfer

Figure 134: Display updating for call transfer on page 569 shows an example scenario for name display updating for a call transfer.

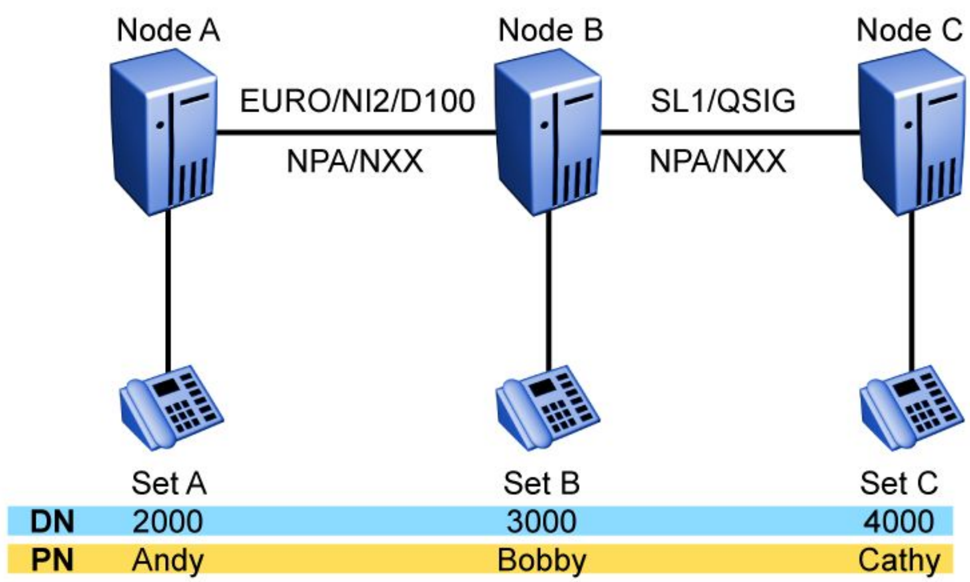

Figure 134: Display updating for call transfer

Call flow scenarios

Call flow scenario 1:

- Set A makes a public call (E164/NXX) to set B.
- Set B answers the call.
- Set B originates the call transfer to set C using the public dialing plan (E164/NXX).

- Set C answers the call from set B.
- Set B transfers the call.

Call flow scenario 2:

- Set C make a public call (E164/NXX) to set B.
- Set B answers the call.
- Set B originates the call transfer to set A using the public dialing plan (E164/NXX).
- Set A answers the call from set B.
- Set B transfers the call.

The following tables show examples of call flow scenarios for public protocol for updating name display during call transfers.

Table 223: Call flow scenario 1

A calls B. B does supervised transfer to C.	SL1		QSIG	
	Display on set A	Display on set C	Display on set A	Display on set C
EURO	NPA NXX (DN of Cathy)	Andy (DN of Andy)	NPA NXX (DN of Cathy)	(DN of Andy)
NI2	Bobby AC1 NPA NXX (DN of Bobby)	Andy (DN of Andy)	Bobby AC1 NPA NXX (DN of Bobby)	(DN of Andy)
D100	Cathy (DN of Cathy)	Andy (DN of Andy)	Cathy (DN of Cathy)	Andy (DN of Andy)

Table 224: Call flow scenario 2

C calls B. B does supervised transfer to A.	EURO		NI2		D100	
	Display on set A	Display on set C	Display on set A	Display on set C	Display on set A	Display on set C
SL1	(DN of Cathy)	Andy (DN of Andy)	Bobby (DN of Bobby)	ACOD	Cathy (DN of Cathy)	Andy (DN of Andy)
QSIG	(DN of Cathy)	NPA NXX (DN of Andy)	Bobby (DN of Bobby)	NPA NXX (DN of Andy)	Cathy (DN of Cathy)	Andy (DN of Andy)

Name display for call forward no answer over public-private network using EURO interface

Figure 135: Name display for CFNA over public-private network with EURO interface on page 571 shows an example scenario for name display for Call Forward No Answer (CFNA) over a public-private network using the EURO interface.

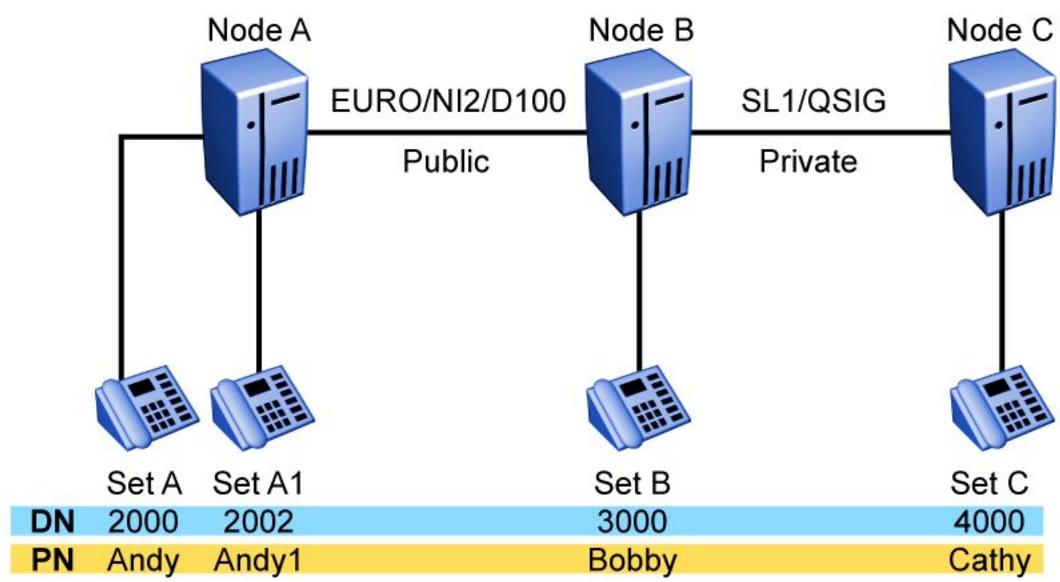

Figure 135: Name display for CFNA over public-private network with EURO interface

Call flow scenarios

Call flow scenario 1:

- Set A calls Set B over a public network (NPA/NXX dialing).
- Set B CFNAs to Set C over a private network (CDP dialing).
- Set C answers the call.

Call flow scenario 2:

- Set C calls set B over a public network (NPA/NXX dialing).
- Set B CFNAs to set A over a private network (CDP dialing).
- Set A answers the call.

Call flow scenario 3:

- Set A calls set B over a public network (NPA/NXX dialing).
- Set B CFNAs to set A1 over a private network (CDP dialing).
- Set A1 answers the call.

The following tables show examples of call flow scenarios for name display for CFNA over a public-private network with EURO interface.

Table 225: Call flow scenario 1

A calls B. B CFNAs to C.	SL1		QSIG	
	Display on set A	Display on set C	Display on set A	Display on set C
EURO	Bobby (DN of Cathy) Cathy (DN of Cathy)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)	Bobby (DN of Cathy) Cathy (DN of Cathy)	Ringing Andy (DN of Andy) (DN of Bobby) AnswerAndy (DN of Andy) (DN of Bobby)
NI2	Bobby AC1 NPA NXX (DN of Bobby) Cathy AC1 NPA NXX (DN of Bobby)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)	Bobby AC1 NPA NXX (DN of Bobby) Cathy AC1 NPA NXX (DN of Bobby)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)
D100	Cathy AC1 NPA NXX (DN of Bobby) (DN of Cathy) Cathy AC1 NPA NXX (DN of Bobby) (DN of Cathy)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)	Bobby AC1 NPA NXX (DN of Bobby) Cathy (DN of Cathy)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Table 226: Call flow scenario 2

C calls B. B CFNAs to A.	EURO		NI2		D100	
	Display on set C	Display on set A	Display on set C	Display on set A	Display on set C	Display on set A
SL1	Bobby AC1 NPA NXX (DN of Bobby) Andy AC1 NPA NXX	Ringing Cathy (DN of Cathy) Answer Cathy (DN of Cathy)	Bobby AC1 NPA NXX (DN of Bobby) Andy (DN of Andy)	Ringing Cathy (DN of Cathy) (DN of Bobby) Answer Cathy (DN	ANDY AC1 NPA NXX (DN of Bobby) (DN of Andy)	Ringing Cathy (DN of Cathy) (DN of Bobby) Answer Cathy (DN

	(DN of Bobby)			of Cathy) (DN of Bobby)	ANDY AC1 NPA NXX (DN of Bobby) (DN of Andy)	of Cathy) (DN of Bobby)
QSIG	Bobby AC1 NPA NXX (DN of Bobby) Andy AC1 NPA NXX (DN of Bobby)	Ringing Cathy (DN of Cathy) Answer Cathy (DN of Cathy)	Bobby AC1 NPA NXX (DN of Bobby) Andy AC1 NPA NXX (DN of Bobby) (DN OF Andy)	Ringing Cathy (DN of Cathy) (DN of Bobby) Answer Cathy (DN of Cathy) (DN of Bobby)	Bobby AC1 NPA NXX (DN of Bobby) Andy AC1 NPA NXX (DN of Bobby) (DN of Andy)	Ringing Cathy (DN of Cathy) (DN of Bobby) Answer Cathy (DN of Cathy) (DN of Bobby)

Table 227: Call flow scenario 3 for EURO

A calls B. B CFNAs to A1.	EURO	
	Display on set A	Display on set A1
EURO	Bobby AC1 NPA NXX (DN of Bobby) Andy 1 (DN of Andy 1)	Ringing Andy (DN of Andy) Answer Andy (DN of Andy)

Table 228: Call flow scenario 3 for NI2

A calls B. B CFNAs to A1.	NI2	
	Display on set A	Display on set A1
NI2	Bobby AC1 NPA NXX (DN of Bobby) AC1 NPA NXX (DN of Bobby)	Ringing Andy (DN of Andy)) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Table 229: Call flow scenario 3 for D100

A calls B. B CFNAs to A1.	D100	
	Display on set A	Display on set A1
D100	Andy1 AC1 NPA NXX (DN Bobby) (DN of Andy1) Andy1 AC1 NPA NXX (DN of Bobby) (DN of Andy1)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Table 230: Call flow scenario 3 for SL1

A calls B. B CFNAs to A1.	SL1	
	Display on set A	Display on set A1
SL1	Andy1 AC1 NPA NXX (DN Bobby) (DN of Andy1) Andy1 AC1 NPA NXX (DN of Bobby) (DN of Andy1)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Table 231: Call flow scenario 3 for QSIG

A calls B. B CFNAs to A1	QSIG	
	Display on set A	Display on set A1
QSIG	Andy1 AC1 NPA NXX (DN Bobby) (DN of Andy1) Andy1 AC1 NPA NXX (DN of Bobby) (DN of Andy1)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Private name displayed for call originates locally and CFNA/ CFW in public network

Figure 136: Private name display on page 575 shows an example scenario for private name display for a call that originates locally and CFNA Call Forward (CFW) in a public network.

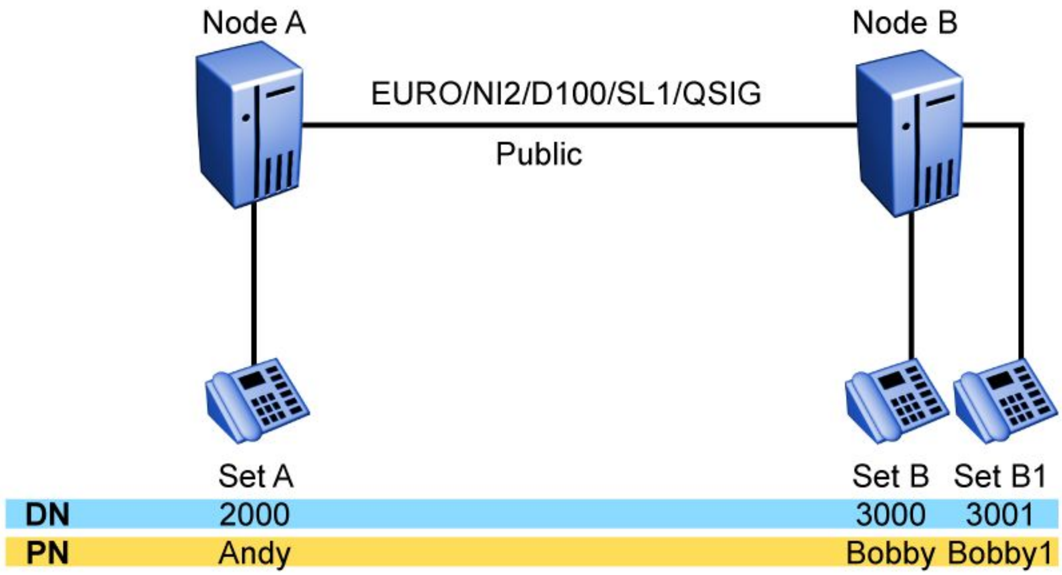

Figure 136: Private name display

Call flow scenario

Call flow:

- Set A calls set B using NPA/NXX dialing.
- Set B CFNAs to Set B1.
- Set B1 answers the call.

The following tables show examples of call flow scenarios for private name displayed for calls that originate locally and for CFNA/CFW in a public network.

Table 232: Call flow scenario for SL1

Set A calls B. B CFNAs to B1.	SL1	
	Display on set A	Display on set B1
SL1	Bobby1 AC1 NPA NXX (DN of Bobby) (DN of Bobby1) Bobby1 AC1 NPA NXX (DN of Bobby) (DN of Bobby1)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Table 233: Call flow scenario for QSIG

Set A calls B. B CFNAs to B1.	QSIG	
	Display on set A	Display on set B1

QSIG	Bobby1 AC1 NPA NXX (DN of Bobby) (DN of Bobby1) Bobby1 AC1 NPA NXX (DN of Bobby) (DN of Bobby1)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Table 234: Call flow scenario for EURO

Set A calls B. B CFNAs to B1.	EURO	
	Display on set A	Display on set B1
EURO	Bobby (DN of Bobby1) Bobby1 (DN of Bobby1)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Table 235: Call flow scenario for NI2

Set A calls B. B CFNAs to B1.	NI2	
	Display on set A	Display on set B1
NI2	Bobby AC1 NPA NXX (DN of Bobby) Bobby1 AC1 NPA NXX (DN of Bobby)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Table 236: Call flow scenario for D100

Set A calls B. B CFNAs to B1.	D100	
	Display on set A	Display on set B1
D100	Bobby1 AC1 NPA NXX (DN of Bobby) (DN of Bobby1) Bobby1 AC1 NPA NXX (DN of Bobby) (DN of Bobby1)	Ringing Andy (DN of Andy) (DN of Bobby) Answer Andy (DN of Andy) (DN of Bobby)

Access code is displayed for a call transfer through QSIG/NI2 IFC from a local call

The Access Code (ACOD) is displayed instead of the Calling Line Identification (CLID) on the originating set for the following call flow scenarios:

- ka local call that is blind transferred across EuroISDN
- a local call that is transferred across NI2

Index

C

D

F

I

L

M

N

R

S

T

V

W